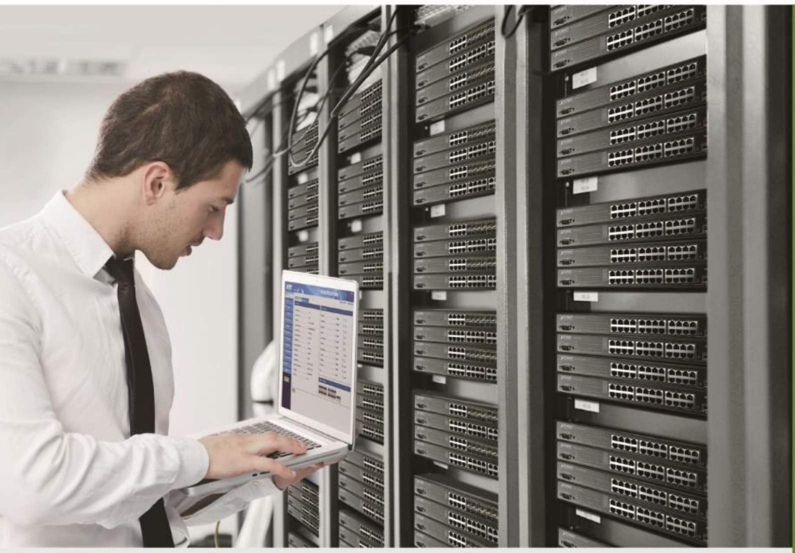
PLANET
Networking & Communication

User's Manual

► DCS-7342-32C2X
► DCS-7342-48Y8C

PLANET Layer 3 32-Port 100G/40G QSFP28 + 2-Port 10G SFP+ / 48-Port 25G SFP28 + 8-Port 100G/40G QSFP28 Managed Data Center Switch



www.PLANET.com.tw

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.

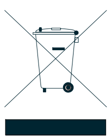
FCC Warning

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 device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

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

User's Manual of PLANET Layer 3 32-Port 100G/40G QSFP28 +2-Port 10G SFP+/48-Port 25G SFP28 +8-Port 100G/40G QSFP28 Managed Data Center Switch

Models:DCS-7342-32C2X and DCS-7342-48Y8C
Revision: 1.0
Part No: EM-DCS-7342 Series Configuration Guide_v1.0

Contents

Chapter 1 INTRODUCTION

Thank you for purchasing PLANET Layer 3 24-/48-Port 10G SFP+ plus 4-Port 100G QSFP28 Managed Switch. The descriptions of these models are shown below:

DCS-7342-32C2X	Layer 3 24-Port 10G SFP+ + 4-Port 100G/40G QSFP28 Managed Switch
DCS-7342-48Y8C	Layer 3 48-Port 10G SFP+ + 2-Port 100G/40G QSFP28 Managed Switch

1.1 Packet Contents

Unless specified, "**Managed Switch**" mentioned in this users manual refers to theDCS-7342-32C2X/DCS-7342-48Y8C.

Open the box of the Managed Switch and carefully unpack it. The box should contain the following items:

	DCS-7342-32C2X	DCS-7342-48Y8C
Quick Installation Guide	■	■
DB9 to RJ45 Interface RS232 Console Cable	■	■
Rack Mount Accessory Kit	■	■
AC Power Cord	■	■
SFP Dust Cap	34	56

If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Description

Meeting Complex Demands of Today's Data Centers

PLANET DCS-7342 Managed Data Center Switch Series, tailored to meet the complex demands and high-performance standards of modern data centers, offers high performance and flexibility. It excels in providing comprehensive Layer 2, Layer 3, and Layer 4 functionalities. The DCS-7342-48Y8C features up to 48 25G and 8 100G/40G QSFP28 ports while the DCS-7342-32C2X comes with up to 32 100G/40G QSFP28 ports and 2 10G SFP+ ports. PLANET data center switch series is equipped with robust Layer 3 routing protocols including OSPF, and BGP, addressing the complexities of network architectures. This ensures seamless data transmission and high bandwidth, making it ideal for cloud computing environments, large enterprise data centers, high-frequency trading, and large-scale content delivery networks (CDN).

Scalable Networks with Robust Performance

Designed for scalability and robust performance, PLANET data center switch series features powerful Layer 3 routing capabilities and supports 100G/40G interfaces. It is built into a durable chassis, allowing administrators to select suitable QSFP transceivers for efficient network expansion and coverage. The series securely handles large data volumes, making it perfect for data center backbone networks and high-capacity servers. It excels in supporting critical applications like VoIP, video streaming, and multicast, ensuring reliable network performance.

Enhanced Reliability with MLAG

PLANET data center switch series is integrated with MLAG (Multi-chassis Link Aggregation Group) technology to enhance network reliability in critical environments. MLAG allows multiple switches to function as a unified entity, ensuring seamless failover and increased bandwidth utilization. This technology synchronizes configurations and state information between paired switches, minimizing downtime and optimizing network resilience. Ideal for high-demand applications like enterprise data centers and cloud environments, PLANET data center switch series with MLAG supports uninterrupted connectivity and scalability without compromising performance.

VXLAN Application and Scalability

Support for VXLAN technology, including Layer 2 and Layer 3 switching functionalities and EVPN VXLAN support, It extends IPv6 application capabilities over IPv4 infrastructure. With stacking design, administrators can virtualize multiple switches into a single logical device, simplifying network management and expansion. Stacking enhances network reliability and availability by sharing ports and enables intelligent management functions, thereby optimizing resource utilization and facilitating flexible network configurations. This makes PLANET data center switch series an ideal choice for handling large-scale network requirements, meeting enterprises' needs for high performance and scalability.

High Availability, Advanced Security and Energy Efficiency

Ensuring high availability, the switch features redundant power supplies and smart fans. Built-in CLI management tools enhance configuration and monitoring convenience, ensuring reliability in various environments. Advanced Security features
and an energy-efficient design enhance operational efficiency and environmental sustainability. Layer 4 functionalities refine network management, improving the overall efficiency and responsiveness.

High-density Port Configuration and Advanced QoS Data Security

The switch supports high-density port configurations such as 10G, 40G and 100G ports, facilitating large-scale data transmission and high-bandwidth applications. Advanced Quality of Service (QoS) support ensures efficient transmission of critical business data through intelligent traffic management and prioritization. Advanced security features including ACLs, port security, and data encryption protect against unauthorized access and malicious attacks.

Energy-efficient Design

Optimizing energy utilization efficiency, the switch reduces energy consumption and meets environmental standards. Smart fans adjust speed based on temperature and workload, ensuring efficient cooling with minimal power usage and noise.

VLAN, Q-in-Q and Traffic Management

Extensive VLAN support with up to 4,000 VLAN IDs and support for flexible Q-in-Q functionalities enable dynamic network segmentation and secure isolation. Support for IGMP and MLD Snooping optimizes multicast traffic management, ensuring efficient network operations and resource utilization. Integrated features make the data center switch an ideal choice for handling large-scale data and complex network environments, providing robust support for network architecture and future expansions.

1.3 Product Features

DCS-7342-48Y8C

- 48-Port 25G SFP28
- 8-Port 100G/40G QSFP28
- RJ45 to DB9 console interface for switch basic management and setup

DCS-7342-32C2X

- 32-Port 100G/40G QSFP28
- 2-Port 10GBASE-SR/LR SFP+
- RJ45 to DB9 console interface for switch basic management and setup

➢ **Stacking Features**

- Hardware Stacking
  - Virtualized multiple PLANET data center switches stacked into one logical device
  - Connects with stack member via 100G/40G QSFP28 and 10G SFP+ interfaces
  - Single IP address stack management, supporting up to 2 hardware units stacked together
  - Stacking architecture supports redundant ring mode

➢ **IP Routing Features**

- IPv4 static routing
- IPv4 dynamic routing protocols such as OSPFv2, IS-IS and BGP
- IPv6 dynamic routing protocols such as OSPFv3, RIPng, BGP4 and BGP4+
- DHCP/DHCPv6 snooping VLAN-based
- GRE tunneling
- Equal-cost routing
- Policy-based routing
- Neighbor Discovery (ND)
- Path MTU Discovery (PMTU)
- IPv6 Ping and IPv6 Telnet
- ACL based on source IPv6 address, destination IPv6 address, Layer 4 port, and protocol type
- Dual-stack for IPv4 and IPv6
- Multiple tunneling techniques
- BFD session binding static routes, VRRP, OSPF, IS-IS, and BGP

➢ **Multicast Routing Features**

- Supports PIM-DM (Protocol Independent Multicast – Dense Mode)
- Supports IGMP v1/v2/v3

➢ **Layer 2 Features**

- Supports VXLAN Layer 2 Switching, Routing Switching, and Layer 3 Gateway
- Supports EVPN VXLAN
- Supports IPv6 VXLAN over IPv4
- Supports Link Aggregation
  - 802.3ad Link Aggregation Control Protocol (LACP)
- Multi-Chassis Link Aggregation (MLAG)
  - Static configuration and dynamic MAC learning
  - MAC browsing and removal
  - Configurable aging time of the MAC address
  - Limited number of learnable MAC addresses
  - MAC filtration
  - Black-hole MAC list
  - IEEE 802.1AE MacSec
- Supports up to 4K VLANs
  - 1:1 and N:1 VLAN Mapping based on 802.1p
  - Q-in-Q and enhanced flexible Q-in-Q

- Supports 802.1d STP, 802.1w RSTP and 802.1s MSTP
  - BPDU Protection
  - Root Protection
  - Loop Protection
- Supports IGMP v1/v2c/v3
  - IGMP Snooping
  - MLD snooping
- Supports L2-L4 packet filtering
  - Filters based on MAC, IP, port, protocol, IP ToS, 802.1p priority, VLAN ID, SVLAN ID, VLAN range, etc.
- Supports cross-device link aggregation
- Supports port mirroring and flow mirroring
- Link Layer Discovery Protocol (LLDP)

➢ **Quality of Service**

- L2-L4 packet filtering with filters based on MAC, IP, port, protocol, IP ToS, 802.1p priority, VLAN ID, SVLAN ID, VLAN range, etc.
- ACL based on time periods
- DLF (Destination Lookup Failure) storm suppression, multicast storm suppression, and broadcast storm suppression
- Port-based bandwidth limiting
- Flow/VLAN-based bandwidth limiting (single-rate two-color, single-rate three-color, dual-rate three-color)
- Priority-based scheduling and priority mapping for flows
- SP/PQ (Strict Priority/Priority Queuing), DRR (Deficit Round Robin), and SP/PQ+DRR scheduling algorithms
- Queue management policies such as tail drop and WRED (Weighted Random Early Detection)
- 8 hardware priority queues per port
- 802.1p, DSCP/ToS priority marking

➢ **Multicast**

- Supports IPv4 IGMP snooping v1, v2 and v3
- Supports IPv6 MLD snooping v1 and v2
- MVR (Multicast VLAN Registration)

➢ **Security**

- User permission classification management and command line classification protection
- Authentication support for 802.1x, RADIUS, and TACACS+
- User level quantity limitation
- User binding (port, source MAC, source IP address access control)
- SNMP login terminal restriction
- SSH v2.0 support
- DDoS attack prevention
- IP Source Guard support
- MAC black hole support
- MAC address quantity limitation
- Static ARP, Gratuitous ARP, ARP inspection

➢ **Management**

- Supports Console, Telnet and SSH terminal services (5 simultaneous Telnet / SSH sessions at least)
- Supports SNMPv1/v2/v3 network management protocols and standard MIB for general features
- Supports NETCONF network management protocol
- Supports file upload and download via FTP and TFTP methods, unified management of logs, alarms and debug information
- Supports user operation logs and RMON (remote monitoring)
- Supports port mirroring and flow mirroring
- Supports BootROM upgrade, remote online upgrade and hot patch
- Supports fan temperature control for automatic adjustment
- Supports temperature and fan monitoring with alerts
- SNMP trap for interface Link Up and Link Down notification

- Network Time Protocol (NTP), RSPAN
- DHCP Functions
  - DHCP Client/Relay/Server
  - DHCP Option 43/60/82
  - DHCP Relay per VLAN
  - DHCPv6 Relay/Server

- **Redundant Power System**
  - Supports dual power redundancy and redundant backup for two sets of fans (Include 2 power DCS-PWR800AC)
  - Hot-swappable power modules and fans

1.4 Product Specifications

Product	DCS-7342-48Y8C	DCS-7342-32C2X
Hardware Specifications		
Switching Capacity	4Tbps	6.4Tbps
Forwarding Rate	2000Mpps	2000Mpps
Power supply	2 (DCS-PWR800AC)	
Power Supply Slot	2 Supports 1+1 backup and hot swapping	
10G Ports	-	2-port 10GBASE-SR/LR SFP+ interface
25G Ports	48-port 25G SFP28 Backward compatible with 10GBASE-X SFP+	-
100G Ports	8-port 100G QSFP28 Backward compatible with 40G QSFP+	32-port 100G QSFP28 Backward compatible with 40G QSFP+ transceiver
Console	1 x RJ45-to-RS232 serial port (115200, 8, N, 1)	
Management Port	1 x 10/100/1000BASE-T RJ45 port	
USB	1 x USB 2.0 Type A for USB storage device use (Configuration backup and restore)	
Fan	2 hot-pluggable fan modules	
Dimensions (W x D x H)	440 x 420 x 44 mm	
Weight	8.1 kg with dual modular power supplies	8.25 kg with dual modular power supplies
Power Supply	AC: 100-240V, 50Hz±10%	
Power Consumption	Maximum 207W/706.3 BTU(full loading)	Maximum 275W/938.3 BTU (full loading)
Switching Specifications		
Switch Architecture	Store-and-forward	
Switch Fabric	4.0Tbps/non-blocking	6.4Tbps/non-blocking
Switch Throughput	4.0Tbps@64bytes	6.44Tbps@64bytes
Address Table	96K MAC address table with auto learning function	
ARP Table	100K	
IP Interfaces	Max. 4K VLAN interfaces	
Routing Table	IPv4 128K entries IPv6 64K entries	
Multicast Table	IGMP snooping: 4k IGMP: 2K	
ACL Table	L2ACL in: 768 L2ACL Out: 512	

	IPv4ACL in: 2000 IPv4ACL Our: 512
Shared Data Buffer	10MB
Jumbo Frame	9KB
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex
Layer 3 Functions	
Routing Protocols	IPv4 static routing IPv4 dynamic routing protocols: - OSPFv2 (Open Shortest Path First) - IS-IS (Intermediate System to Intermediate System) - BGP (Border Gateway Protocol) IPv6 static routing IPv6 dynamic routing protocols: - OSPFv3 (Open Shortest Path First) - BGP4 - BGP4+ - RIPng Equal-cost routing Policy-based routing Neighbor Discovery (ND) Path MTU Discovery (PMTU) IPv6 Ping and IPv6 Telnet
Multicast Routing Protocol	PIM-DM
Layer 2 Functions	
Port Configuration	Supports port configuration and management Monitors and manages port status Provides port mirroring functionality Port loopback detect
Port Status	Monitors and displays the operational status of each port Provides real-time information on port link status (up/down) Reports port-specific statistics such as traffic throughput, error rates, and packet counts Supports detection and notification of port-related events and alarms
Port Mirroring	Supports port mirroring functionality Allows the replication of traffic from a source port or VLAN to a destination port for monitoring and analysis purposes
VLAN	IEEE 802.1Q tag-based VLAN IEEE 802.1ad Q-in-Q and enhanced flexible Q-in-Q capabilities Supports up to 4K VLANs Multicast VLAN Register (MVR)
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)

	Features BPDU protection, root protection, loop protection, and BPDU tunneling
IPv4 IGMP Snooping	IPv4 IGMP v1/v2/v3 snooping IGMP Fast Leave IPv4 Querier
IPv6 MLD Snooping	IPv6 MLD v1/v2 snooping
Multicast	Supports IGMP v1/v2c/v3 Implements IPv4 IGMP v1/v2/v3 Snooping Implements IPv6 MLD v1/v2 Snooping
Link Aggregation	Supports cross-device link aggregation (LACP) Implements Multi-Chassis Link Aggregation (MLAG)
Storm Control	Implements DLF (Destination Lookup Failure) storm suppression Supports multicast storm suppression Supports broadcast storm suppression
Bandwidth Control	Port-based bandwidth limitation Supports flow/VLAN-based bandwidth limiting (single-rate two-color, single-rate three-color, dual-rate three-color) Implements priority-based scheduling and priority mapping for flows
QoS	8 priority queues on all switch ports Traffic Supervision and Traffic Shaping Scheduling for priority queues - Weighted Round Robin (WRR) - Strict priority (SP) - SP+WRR Traffic classification: - IEEE 802.1p CoS - DSCP - DiffServ - Precedence - TOS - VLAN ID - IP ACL - MAC ACL Policy-based ingress and egress QoS 802.1p and DSCP priority remark Supports queue management policies such as tail drop and WRED (Weighted Random Early Detection)
Security Functions	
Access Control List	ACL support based on source IPv6 address, destination IPv6 address, Layer 4 port, and protocol type ACL support based on time periods Supports L2-L4 packet filtering with filters based on MAC, IP, port, protocol, IP ToS, 802.1p priority, VLAN ID, SVLAN ID, VLAN range, etc. DLF (Destination Lookup Failure) storm suppression, multicast storm suppression, and broadcast storm suppression
Security	DDoS attack prevention

	IP Source Guard support MAC black hole support MAC address quantity limitation Port isolation DHCP snooping, DHCP Option 43/60/82 Defend against DOS attacks Port security
AAA	Supports 802.1x, RADIUS, and TACACS+ authentication User level quantity limitation User binding (port, source MAC and source IP address access control)
Network Access Control	SNMP login terminal restriction SSH v2.0 support
Switch Management Functions	
System Configuration	Supports Console and Telnet terminal services Supports SNMPv1/v2c network management protocols and standard MIB for general features
Secure Management Interfaces	Supports SSH v2.0 and SNMPv3 User permission classification management and command line classification protection SNMP login terminal restriction Authentication support for 802.1x, RADIUS, and TACACS+
System Management	Supports file upload and download via FTP and TFTP methods and unified management of logs, alarms and debug information Supports BootROM upgrade, remote online upgrade and hot patch Supports NETCONF network management protocol Supports user operation logs Supports temperature and fan monitoring with alerts Supports MIB and TRAP Supports Ping / traceroute Supports Syslog Supports transceiver DDM
Event Management	Supports port mirroring and flow mirroring Supports RMON (remote monitoring) Supports DDoS attack prevention Supports MAC black hole support
Hardware Stacking	Supports hardware stacking Virtualizes multiple physical devices into a logical device Stacking virtualization technology improves reliability
Hardware Stacking Compatibility List	Supports 2 units for virtual stacking Supports 20Gbps/200Gbps stacking bandwidth
SNMP MIBs	RFC 1066 TCP/IP-based MIB RFC 1213, 1157 SNMPv2c/v3 MIB RFC1493 bridge MIB RFC 2674 bridge MIB extension

	RFC1643 ethernet MIB RFC1757 RMON group 1,2,3,9 RFC 2925 Remote Management MIB RFC 2233 (rfc2233) - SMIv2 MIB
Standard Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 25G, 40G, 100G Ethernet standards IEEE 802.1Q VLAN standard IEEE 802.1D STP, 802.1w RSTP, 802.1s MSTP standards IEEE 802.1X Network Authentication standard RFC standards, such as RFC 768 (UDP), RFC 791 (IPv4), RFC 2460 (IPv6), etc. IEEE 802.1ab LLDP
Environments	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -40 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

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 2-1-1 and 2-1-2, show the front panel of the Managed Switches.

DCS-7342-32C2X Front Panel

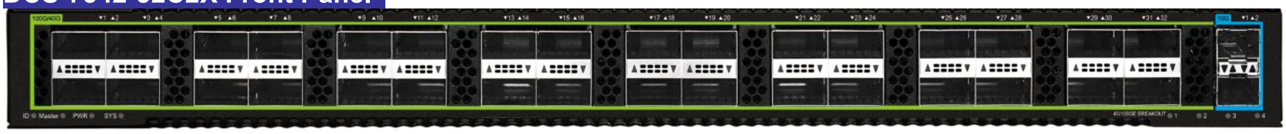


Figure 2-1-1DCS-7342-32C2X front panel

DCS-7342-48Y8C Front Panel

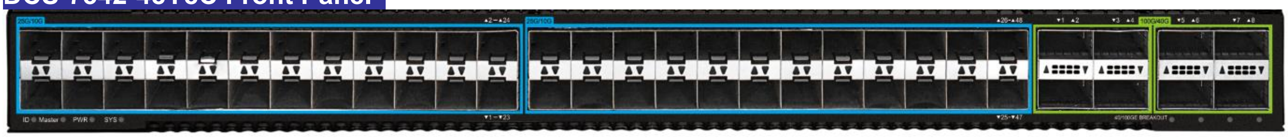


Figure 2-1-2 DCS-7342-48Y8C front panel

- **SFP+/SFP28 slots**

  SFP+/SFP28 mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters (Multi-mode fiber) to 10/30/50/70/120 kilometers (Single-mode fiber).

  The console port is an RJ45 type, RS232 male serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached RS232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

- **QSFP28 slots**

  QSFP28 slot, QSFP (Quad Small Form-factor Pluggable) transceiver module: Supports transmission distances ranging from 0.5/2/100 meters (Multi-mode fiber) to 10 kilometers (Single-mode fiber).

- **USB Interface**

  The USB port is a USB2.0 type; it is an interface for uploading/restoring the configuration/firmware.

- **MGMT Port**

  The MGMT port is an RJ45 type, an independent interface for Telnet or SSH.

2.1.2 Switch Rear panel

The unit rear panel provides a simple interface monitoring the switch. Figure 2-1-3 and 2-1-4, show the front panel of the Managed Switches.

DCS-7342-32C2X Rear Panel

Figure 2-1-3 DCS-7342-32C2X rear panel

DCS-7342-48Y8C Rear Panel

Figure 2-1-4 DCS-7342-48Y8C rear panel

- **USB Interface**

  The USB port is a USB2.0 type; it is an interface for uploading/restoring the configuration/firmware.

- **MGMT Port**

  The MGMT port is an RJ45 type, an independent interface for Telnet or SSH.

- **Console Port**

  The console port is an RJ45 type, RS232 male serial port connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP address setting, factory reset, port management, link status and system setting. Users can use the attached RS232 cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

2.1.3 LED Indications

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

DCS-7342-32C2X

Figure 2-1-5 DCS-7342-32C2X front panel

- **LED Definition**

LED	Color	Function
ID	Green	Off: ID light not activated default state
		On: Used for on-site locating, controlled by maintenance personnel to turn on and off ID light
Master	Green	Off: Device is not the stack master
		On: Device is the stack master or not stacked
PWR	Green	Off: Device is not powered on
		On: Device power is working normally
SYS	Green	Off: Device is not running
		Fast Blinking: Device initialization in progress. Slow Blinking: Device running normally
100/40GE BREAKOUT	Green	Note: For 100GE interface, supports non-rate-splitting and rate-splitting. Non-rate-splitting mode: Off: 100GE interface operates in 100GE mode, not split into 4x25GE interfaces. On: One of the 100GE interfaces operates in 25GE mode, split into 4x25GE interfaces. Sequence lights 1/2/3/4 on, each indicates the status of the corresponding 25GE interface. Rate-splitting mode to 40GE: Off: 40GE interface operates in 40GE mode, not split into 4x10GE interfaces. On: One of the 40GE interfaces operates in 10GE mode, split into 4x10GE interfaces. Sequence lights 1/2/3/4 on, each indicates the status of the

		corresponding 10GE interface.
ACT	**Green**	Off: Fan not running. On: Fan running normally.
ALM	**Red**	On: Fan alarm. Blinking: Main control unable to control fan, fan adjusts speed according to environmental temperature.
ACT	**Green**	Off: USB boot not enabled, default mode. On: USB boot completed. Blinking: USB data reading.
L/A	**Green**	Off: Link not connected. On: Link connected. Blinking: Interface transmitting and receiving data.

2.1.3.1 DCS-7342-48Y8C

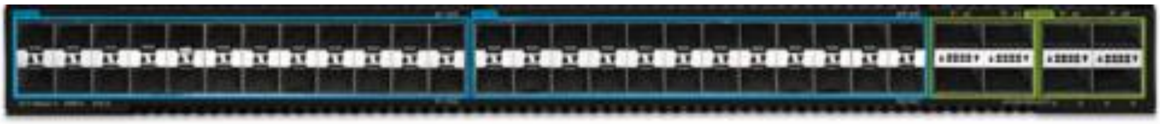


Figure 2-1-6 DCS-7342-48Y8C front panel

- **LED Definition**

LED	Color	Function
ID	Green	Off: ID light not activated default state
		On: Used for on-site locating, controlled by maintenance personnel to turn on and off ID light
Master	Green	Off: Device is not the stack master
		On: Device is the stack master or not stacked
PWR	Green	Off: Device is not powered on
		On: Device power is working normally
SYS	Green	Off: Device is not running
		Fast Blinking: Device initialization in progress. Slow Blinking: Device running normally
100/40GE BREAKOUT	Green	Note: For 100GE interface, supports non-rate-splitting and rate-splitting. Non-rate-splitting mode: Off: 100GE interface operates in 100GE mode, not split into 4x25GE interfaces. On: One of the 100GE interfaces operates in 25GE mode, split into 4x25GE interfaces. Sequence lights 1/2/3/4 on, each indicates the status of the corresponding 25GE interface. Rate-splitting mode to 40GE: Off: 40GE interface operates in 40GE mode, not split into 4x10GE interfaces. On: One of the 40GE interfaces operates in 10GE mode, split into 4x10GE interfaces. Sequence lights 1/2/3/4 on, each indicates the status of the corresponding 10GE interface.
ACT	Green	Off: Fan not running. On: Fan running normally.
ALM	Red	On: Fan alarm.

		Blinking: Main control unable to control fan, fan adjusts speed according to environmental temperature.
ACT	**Green**	Off: USB boot not enabled, default mode. On: USB boot completed. Blinking: USB data reading.
L/A	**Green**	Off: Link not connected. On: Link connected. Blinking: Interface transmitting and receiving data.
25GE Left light(Link)	**Green**	Off: Port is not connected or disabled. On: Port is connected.
25GE Right light(ACT)	**Orange**	Off: No data transmission on the port. On: Blinking Port is transmitting data.

2.2 Switch Installation

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 follow these steps:

Step 1: Attach the rubber feet to the recessed areas on the bottom of the Managed Switch.

Step 2: Place the Managed Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-2-1.

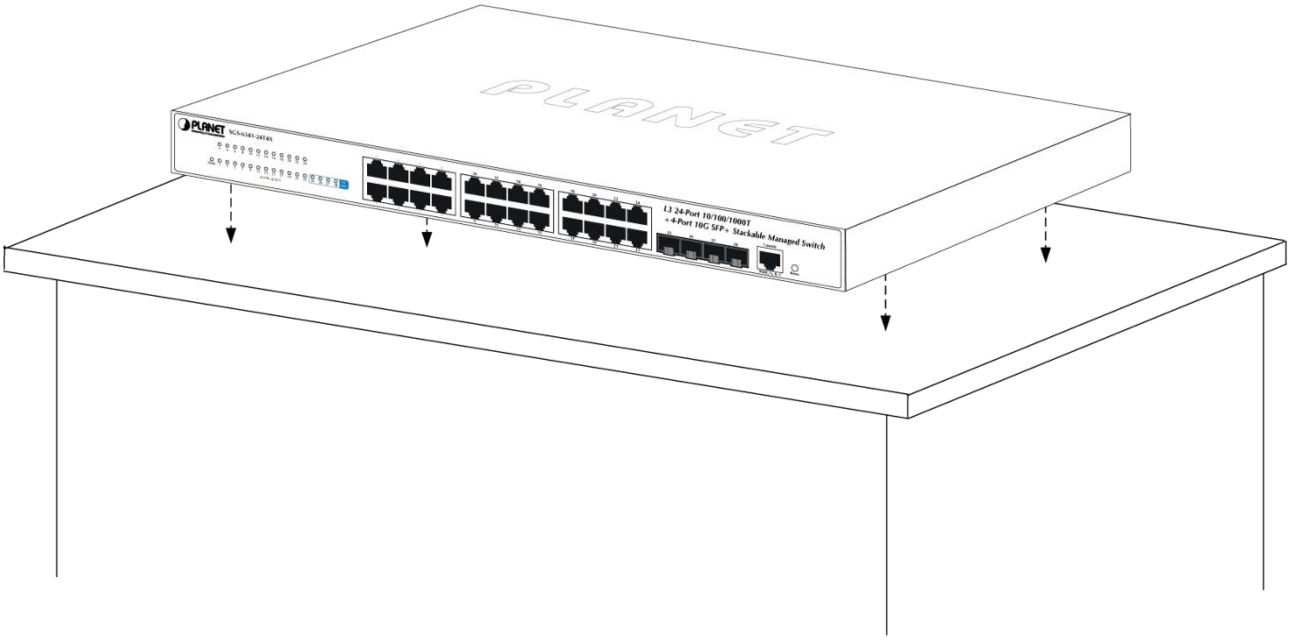


Figure 2-2-1 Place the Managed Switch on the desktop

Step 3: 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 under **Specifications**.

Step 4: Connect the Managed Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed Switch and connect the other end of the cable to the network devices such as printer servers, workstations or routers, etc.

Connection to the Managed Switch requires UTP Category 5 network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

Step 5: 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 follow the instructions described below:

Step 1: Place the Managed Switch on a hard flat surface, with the front panel positioned towards the front side.

Step 2: Attach the rack-mount bracket to each side of the Managed Switch with supplied screws attached to the package.

Figure 2-2-2 shows how to attach brackets to one side of the Managed Switch.

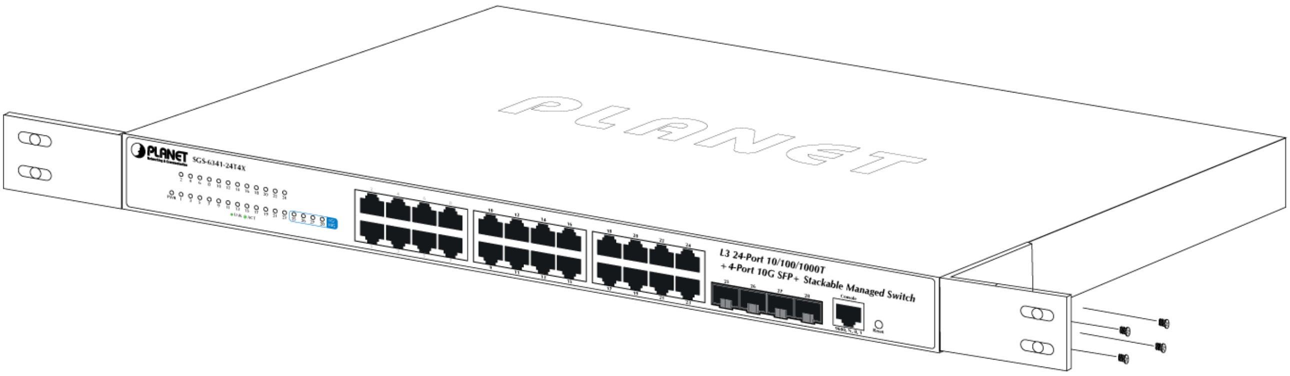


Figure 2-2-2 Attach brackets to the Managed Switch.

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

Step 3: Secure the brackets tightly.

Step 4: Follow the same steps to attach the second bracket to the opposite side.

Step 5: After the brackets are attached to the Managed Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-2-3.

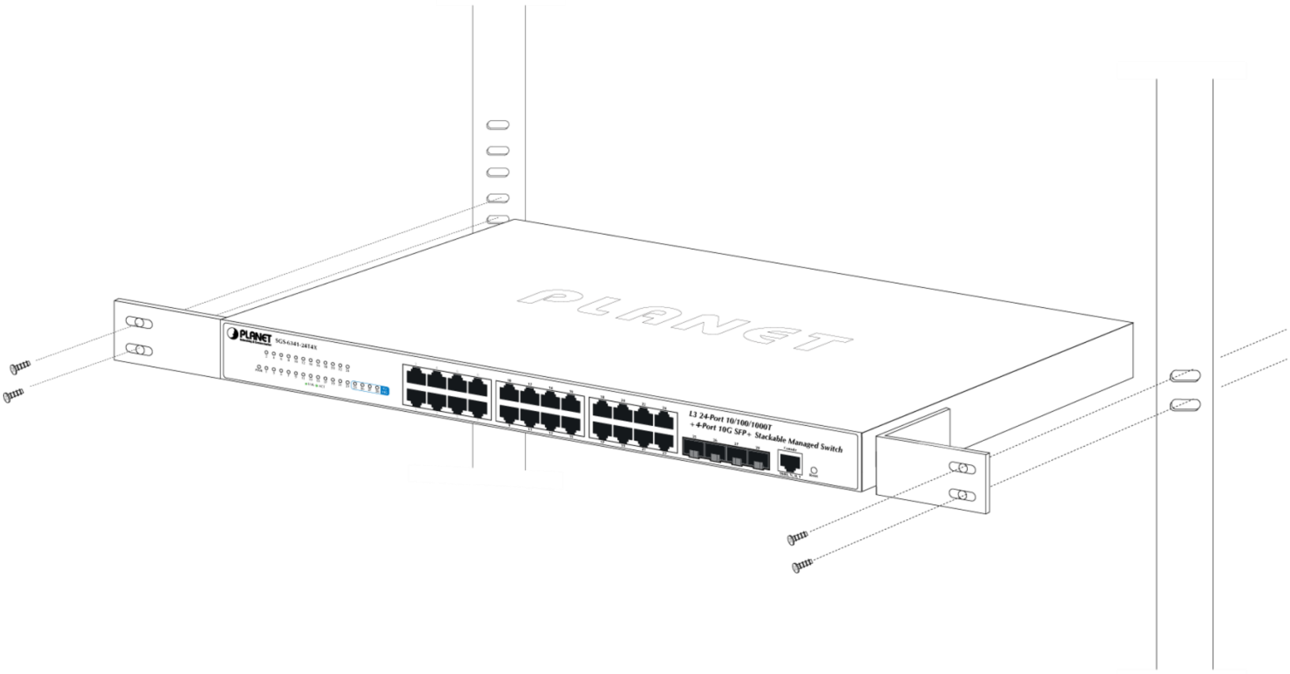


Figure 2-2-3 Mounting Managed Switch in a Rack

Step 6: Proceed with Steps 4 and 5 of Session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed Switch.

■ **AC Power Receptacle**

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

Plug the female end of the power cord firmly into the receptacle on the rear panel of the Managed Switch. Plug the other end of the power cord into an electrical outlet and then the power will be ready.

Chapter 3 Configuration Preparation

The chapter mainly describes the following preparatory works before you configure the switch at the first time:

- Port number of the switch
- Preparation before switch startup
- How to get help
- Command mode
- Cancelling a command
- Saving configuration

3.1 Port Number of the Switch

The physical port of the switch is numbered in the **<type><slot>/<port>** form. The type-to-name table is shown as follows:

Interface Type	Name
10G Ethernet interface	xgigaethernet
10G Ethernet	10gigaethernet
25G Ethernet	25gigaethernet
40G Ethernet	40gigaethernet
100G Ethernet	100gigaethernet

The expansion slot number to mark and set ports must be the number **0**. Other expansion slots are numbered from left to right, starting from **1**.

The ports in the same expansion slot are numbered according to the order from top to bottom and the order from left to right, starting from **1**. If only one port exists, the port number is **1**.

Note:

Ports in each kind of modulars must be numbered sequently from top to bottom and from left to right.

3.2 Preparation Before Switch Startup

Do the following preparatory works before the switch is configured:

(1) Set the switch's hardware according to the requirements of the manual.

(2) Configure a PC terminal simulation program.

(3) Determine the IP address layout for the IP network protocols.

3.3 Acquiring Help

Use the question mark (?) and the direction mark to help you enter commands:

- Enter a question mark. The currently available command list is displayed.

  Switch> ?

- Enter several familiar characters and press the space key. The available command list starting with the entered familiar characters is displayed.

  Switch> s?

- Enter a command, press the space key and enter the question mark. The command parameter list is displayed.

  Switch> show ?

- Press the "up" key and the commands entered before can be displayed. Continue to press the "up" key and more commands are to be displayed. After that, press the "down" key and the next command to be entered is displayed under the current command.

3.4 Command Modes

The command line interfaces for the switch can be classified into several modes. Each command mode enables you to configure different groupware. The command that can be used currently is up to the command mode where you are. You can enter the question mark in different command modes to obtain the available command list. Common command modes are listed in the following table:

Command View	Function	Prompt	Entry Command	Exit Command
Privileged user view	Checks all running status and statistical information on the switch, and manages files and the system.	Switch#	You will enter this view as soon as a connection is set up with the switch.	Run **exit** to log out. You need to enter the user name and password again upon the next login.

Command View	Function	Prompt	Entry Command	Exit Command
Global configuration view	Configures global parameters of the switch.	Switch (config)#	Run **config** in the privileged user view.	Run **exit** to return to the privileged user view.
Common user view	Debugs some functions of the switch, upgrades the system software, and checks the running status and statistics of the switch.	Switch>	Run **disable** in the privileged user view.	Run **enable** to return to the privileged user view.
Terminal configuration view	Configures a terminal.	Switch (config-line)#	Run **line vty <1-32>** in the global configuration view.	Run **exit** to return to the global configuration view.
Interface configuration view	Configures interface parameters on the switch. (N: interface number) You can configure individual Ethernet interfaces or trunk interfaces.	Switch(config-xge1/0/1)# Switch(config-eth-trunkN)#	Run **interface xgigaethernet 1/0/1** or **interface eth-trunk- N** in the global configuration view.	Run **exit** to return to the global configuration view.
Interface group configuration view	Configures interface parameters on the switch.	Switch(config-xge1/0/1->xge1/0/12)# Switch(config-if-group)#	Run **Switch(config)#interface xgigaethernet 1/0/1 to xgigaethernet 1/0/12** or **Switch(config)#interface group 1/0/1,1/0/12-1/0/20** in the global configuration view.	Run **exit** to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
VLAN configuration view	Configures Layer 2 VLANs on the switch.	Switch(vlan-N1)#	Run **vlan** *N1* in the global configuration view.	Run **exit** to return to the global configuration view.
VLANIF configuration view	Configures Layer 3 VLAN interfaces on the switch. (N: VLAN ID)	Switch (config-vlanif-N)#	Run **interface vlan N** in the global configuration view.	Run **exit** to return to the global configuration view.
STP configuration view	Configures the Spanning Tree Protocol (STP) on the switch.	Switch (config-stp)#	Run **stp** in the global configuration view.	Run **exit** to return to the global configuration view.
AAA configuration view	Configures the Remote Authentication Dial In User Service (RADIUS) on the switch.	Switch(config-aaa)#	Run **aaa** in the global configuration view.	Run **exit** to return to the global configuration view.
OSPFv2 configuration view	Configures the Open Shortest Path First (OSPF) on the switch.	Switch(config-ospf-1)#	Run **router ospf** in the global configuration view.	Run **exit** to return to the global configuration view.
Line configuration view	Line view configuration for user terminals, including the console terminal and virtual terminal	Switch (config-line)#	Run **line console/vty** in the global configuration view.	Run **exit** to return to the global configuration view.
Schedule-profile configuration view	Configures schedule-profile parameters.	Switch(config-schedule-profile-#)#	Run **schedule-profile #** in the global configuration view.	Run **exit** to return to the global configuration view.
Time-range configuration view	Configures the time-range on the switch.	Switch(config-timerange1)#	Run **time-range list number** in the global	Run **exit** to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
			configuration view.	
MPLS remote-peer configuration view	Configures the remote-peer on the switch.	Switch(config-mplsldp-remote1)#	Run **mpls ldp remote-peer index** in the global configuration view.	Run **exit** to return to the global configuration view.
BGP configuration view	Configures the BGP on the switch.	Switch(config-bgp)#	Run **router bgp AS -number** in the global configuration view.	Run **exit** to return to the global configuration view.
Route-policy configuration view	Configure the route policy on the switch.	Switch(config-route-policy)#	Run **route-policy** *name* **permit/deny node Index** in the global configuration view.	Run **exit** to return to the global configuration view.
Rlink configuration view	Configures the Rlink function on the switch.	Switch(config-rlink1)#	Run **rlink group rlink-group-number** in the global configuration view.	Run **exit** to return to the global configuration view.
Mlink configuration view	Configures mlink on the switch.	Switch(config-mlink1)#	Run **mlink group mlink-group number** in the global configuration view.	Run **exit** to return to the global configuration view.
NTP configuration view	Configures the Network Time Protocol (NTP) on the switch.	Switch(config-ntp)#	Run **ntp** in the global configuration view.	Run **exit** to return to the global configuration view.
Filter configuration view	Configures filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run **filter filter list number** in the global configuration	Run **exit** to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
			view. List numbers 1001-2000 specify IPv4 ACLs.	
Filter configuration view (IPv6)	Configures the Filtev6r on the switch.	Switch(configure-filter-filter type- filter list number)#	Run **filter filter list number** in the global configuration view. List numbers <3001-4000> specify IPv6 ACLs.	Run **exit** to return to the global configuration view.
Filter-hybrid configuration view	Configures hybrid filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run **filter filter list number** in the global configuration view. List numbers 2001-3000 specify hybrid ACLs.	Run **exit** to return to the global configuration view.
Layer-2 filter configuration view	Configures Layer-2 filters on the switch.	Switch(configure-filter-filter type- filter list number)#	Run **filter filter list number** in the global configuration view. List numbers 1-1000 specify Layer-2 ACLs.	Run **exit** to return to the global configuration view.
DHCP pool configuration view	Configures the DHCP address pool on the switch.	Switch(config-dhcp-pool-N1)#	Run **dhcp pool N1** in the global configuration view.	Run **exit** to return to the global configuration view.
VPN configuration view	Configures the L3VPNP on the switch.	Switch(config-vpn-instance-name)#	Run **ip vpn-instance name** in the global configuration view.	Run **exit** to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
Y1731 configuration view	Configures the Y1731 on the switch.	Switch(config-y1731)#	Run **y1731** in the global configuration view.	Run **exit** to return to the global configuration view.
Address family configuration view	Configures the address family on the switch.	Switch(config-bgp-af-ipv4)#	Run **ipv4-family unicast** in the BGP view.	Run **exit** to return to the global configuration view.
MA configuration view	Configures the MA on the switch.	Switch(config-md-*mdname*-ma-*maname*)#	Run **ma name *ma-name* vlan *vlan-id*** in the MD view.	Run **exit** to return to the global configuration view.
Meg configuration view	Configures the meg on the switch.	Switch(config-meg-*icc string-umc string*)#	Run **meg vlan *vlan-id* level *level* icc *icc-string* umc *umc-string*** in the Y1731 configuration view.	Run **exit** to return to the global configuration view.
Loopback interface configuration view	Configures the loopback interface on the switch.	Switch(config-loopback-loopbacknumber)#	Run **interface loopback number** in the global configuration view.	Run **exit** to return to the global configuration view.
Tunnel interface configuration view	Configures the tunnel interface on the switch.	Switch(config-tunnel- Tunnel interface number)#	Run **interface tunnel Tunnel interface number** in the global configuration view.	Run **exit** to return to the global configuration view.
MVLAN configuration view	Configures IGMP snooping on the switch.	Switch(config-igmpsnoop-mvlan4000)#	Run **igmp-snooping mvlan** *vlan-id* in the global configuration view.	Run **exit** to return to the global configuration view.

Command View	Function	Prompt	Entry Command	Exit Command
MPLS LDP configuration view	Configures the MPLS VPN on the switch.	Switch(config-mpls-ldp-1)	Run **mpls ldp vpn-instance name** in the global configuration view.	Run **exit** to return to the global configuration view.
BD view	Configures bridge domains on the switch.	Switch(config)#bridge-domain 1	Run **bridge-domain** *bd-id* in the global configuration view.	Run **exit** to return to the global configuration view.

Each command mode is unsuitable to subsets of some commands. If problem occurs when you enter commands, check the prompt and enter the question mark to obtain the available command list. Problem may occur when you run in incorrect command mode or you misspelled the command.

Pay attention to the changes of the interface prompt and the relative command mode in the following case:

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

3.5 Canceling a Command

To cancel a command or resume its default properties, add the keyword “no” before most commands. An example is given as follows:

no ip routing

3.6 Saving Configuration

You need to save configuration in case the system is restarted or the power is suddenly off. Saving configuration can quickly recover the original configuration. You can run write to save configuration in management mode or office configuration mode.

Chapter 4 Initial Setup

4.1 Basic Configuration

4.1.1 Device Management Configuration

Device management configuration tasks display the switch's board status, CPU utilization, and memory utilization.

Device management configuration tasks include:

- Resetting the switch
- Updating system or configuration files
- Running log configuration commands
- Configuring access control lists

4.1.1.1 Resetting the Switch

Purpose

To restart a faulty switch, you can run the **reboot** command. This command provides the same function as a cold restart. Using this command, you can reboot the switch remotely, without the need to go to the equipment room. Do not use this command unless necessary, because it will cause a temporary interruption of the network. In addition, it is recommended that you determine whether to save the configuration file before rebooting. To save the configuration file, run the **write file** command and then run the **y** command in the user view.

Procedure

Purpose	Procedure
Reset the switch	1. In the privileged user view, run the **reboot** command. 2. Run the **y** command.

4.1.1.2 Updating System or Configuration Files

Purpose

Run the **upgrade (os|config)** command to upgrade system or configuration files. Before running this command, run the **ftp get** command to download all the files to be upgraded to the device. Use this command under the instructions of technical support personnel.

Procedure

The procedure for updating system or configuration files is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Upgrade system or configuration files	1. Access the global configuration view. 2. Run the **upgrade** { **os** | **config** } command.

4.1.1.3 Configuring Access Control Lists

Purpose

This section describes how to configure access control lists (ACLs).

Procedure

The procedure for configuring ACLs is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or configure an ACL	1. Access the global configuration view. 2. Run the following commands: ● **management acl** { **enable | disable** } ● **management acl** *ipv4-address* ● **management acl** *ipv4-address1 ipv4-address2* **{ telnet | snmp | ssh | tftp | ftp | all }**
Disable or delete a configured ACL	1. Access the global configuration view. 2 Run the **no management acl** *ipv4-address/M* command.

4.1.2 Configuring Basic System Environment

System basic configuration and management include:

- Setting the switch name.
- Setting the system clock.

4.1.2.1 Configuring the Switch Hostname

Purpose

This section describes how to configure the switch hostname.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the switch hostname	1. Access the global configuration view. 2. Run the **hostname** *host-name* command.
Restore the switch hostname to the default value	1. Access the global configuration view. 2. Run the **no hostname** command.

4.1.2.2 Setting the System Clock

Purpose

This section describes how to configure the switch system clock.

Procedure

The procedure for setting the system clock is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the system clock	1. Access the global configuration view. 2. Run the following commands: ● **clock set** *HH:MM:SS YYYY/MM/DD* ● **clock set** *HH:MM:SS DD MM YYYY*

4.1.2.3 Setting the DST

Purpose

This section describes how to set the name, start time, and end time of daylight-saving time (DST) and cancel the settings.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the DST	1. Access the global configuration view. 2. Run the following commands: ● **clock summer-time** *summer-time-name* **date** *start-hour:start-minutes start-day start-month start-year end-hour:end-minutes end-day end-month end-year* ● **clock summer-time** *summer-time-name* **date** *start-hour:start-minutes start-year/start-month/start-day end-hour:end-minutes end-year/end-month /end-day* ● **clock summer-time** *summer-time-name* **recurring** { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *start-hour:start-minutes* { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *end-hour:end-minutes*
Cancel the DST	1. Access the global configuration view. 2. Run the **no clock summer-time** command.

4.1.2.4 Setting the Local Time Zone

Purpose

This section describes how to set the local time zone.

Procedure

The procedure for setting the local time zone is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the local time zone	1. Access the global configuration view. 2. Run the **clock timezone** *time-zone-name* { **add** | **minus** } *offset* command.

4.1.3 Displaying Basic System Information

4.1.3.1 Displaying Device Management and Running Information

Purpose

Run the **show** command in any view to display the operation condition of the configured device. You can verify the configuration by viewing the displayed information.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the system configuration parameters that are effective currently	1. Access the privileged user view, global configuration view, or common user view. 2. Run the following commands: ● **show running-config** ● **show running-config include-default**

4.1.3.2 Displaying All Available Commands in the Current Configuration View

Purpose

This section describes how to view all available commands in the current configuration view.

Procedure

The following is the procedure for viewing all available commands in the current configuration view.

Purpose	Procedure
View all available commands in the current configuration view	1. Access the current configuration view. 2. Run the **list** command.

4.1.3.3 Displaying Commands That Have Been Used by Users

Purpose

This section describes how to display commands that have been used by users.

Procedure

The following is the procedure for displaying commands that have been used by users.

Purpose	Procedure
Display commands that have been used by users	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show history** command.

4.1.3.4 Displaying Software and Hardware Versions of the System

Purpose

This section describes how to display the information of the system, such as the software and hardware versions and the compiling time.

Procedure

The following is the procedure for displaying the information of the system, such as the software and hardware versions and the compiling time.

Purpose	Procedure
Display the information of the system, such as the software and hardware versions and the compiling time	1. Access the privileged user view or global configuration view. 2. Run the **show version** command.

4.1.3.5 Viewing the Number of Users That Have Logged in

Purpose

This section describes how to view the number of users that have logged in.

Procedure

The following is the procedure for viewing the number of users that have logged in.

Purpose	Procedure
Display the number of users that have logged in	1. Access the privileged user view or global configuration view. 2. Run the **show login-type count** command.

4.1.3.6 Viewing the Power Status of Switch

Purpose

This section describes how to view the power status of Switch.

Procedure

The following is the procedure for viewing the power status of Switch.

Purpose	Procedure
View the power status	1. Access the privileged user view, global configuration view, common user view, interface group configuration view, and interface configuration view. 2. Run the **show power** command.

4.1.3.7 Viewing MAC Addresses

Purpose

This section describes how to view the default MAC address of Switch and the MAC address in use.

Procedure

The following is the procedure for viewing the default MAC address of Switch and the MAC address in use.

Purpose	Procedure
View the ACL configuration	1. Access the privileged user view or global configuration view. 2. Run the **show system** command.

4.1.3.8 Viewing the ACL Configuration

Purpose

This section describes how to view the ACL configuration.

Procedure

The following is the procedure for viewing the ACL configuration.

Purpose	Procedure
View the default MAC address and the MAC address in use	1. Access the global configuration view. 2. Run the **show management acl** command.

4.1.4 Password Management Configuration

The Switch supports password management. Users must configure a system login password when logging into the Switch for the first time and input the configured password for each subsequent login. After the password is authenticated, users can log in to the switch and perform operations. If the password fails the authentication, users cannot log in to the switch. Users can use the default password or set a new password as follows:

- Log in as the Admin with the default username and password, and then create other usernames, permissions, and passwords. The system automatically adds these configured usernames, permissions, and passwords to the user list.
- When a user inputs a password for login, the system protects the password. The password input is not displayed in CLI. The password is not stored as clear text in the system configuration file or on the terminal. It is encrypted. The password input by a user is displayed as ****** on the terminal. When a user configures a password, the password is displayed in clear text in CLI but is encrypted in the configuration file.

4.1.4.1 Allocating User Permissions

Purpose

This section describes how to add usernames, permissions, and passwords after logging in to the Switch. Login users on the Switch are classified into four types, as described in Table 4-1. Only users that belong to the Administrators group have the permission to create a new user.

Table 4-1 User types supported by the Switch

User Type	Description
administrators	The administrators group has the highest level and can run any commands. Key operations greatly affecting the switch must have the administrator permission, such as commands for user management, FTP operations, history record clearing, terminal number reduction, image and configuration file upgrading, and FTP/Telnet enabling/disabling.
operators	The operators group has a lower level than the administrators group, and can run all commands except those related to key operations requiring the administrator permission.
users	The users group has a lower level than the operators group, and can run all commands except upgrade, TFTP, SNTP, SNMP, and SGM commands.
guests	The guests group has the lowest level and can run only information viewing commands and a few configuration commands, such as the **ping** command. Note that the guests group cannot view important information such as output

User Type	Description
	information of **show running-config**, **show snmp config**, **show startup-config**, and **show user config** commands.

Users can only run the commands of their levels or of lower levels. To keep confidentiality, the password is not displayed on the screen.

Operation

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Add a username and its permission and password	1. Access the global configuration view. 2. Run the command **username** *username* **group** { **administrators** | **operators | users | guests** } password *password*.
Delete a username and its permission and password	1. Access the global configuration view. 2. Run the **no username** *username* command.
Modify the password of the current login user	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **password** *password* command.

4.1.4.2 Example of User Permission Configuration

Network Requirements

A PC connects to a switch. You can either adopt the default settings or create a password.

Network Diagram

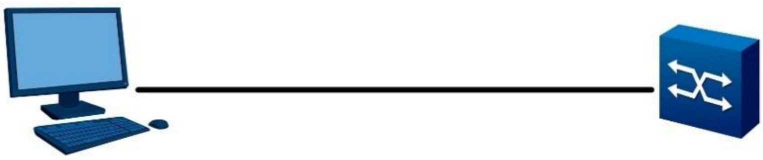


Figure 4-1 Example of user permission configuration

Configuration

Log in to the system by using the default username and password and access the global configuration view. Create an account with username **123**, password **Admin123456,** and permission **Administrators**. The steps are as follows:

```
Switch#config
Switch(config)#username 123 group Administrators password Admin123456
#Log out.
Switch(config)#quit
Switch#quit
# Use the configured username 123 and password 123 to log in to the system.
Username: 123
Password: ***********
Switch#
```

4.1.5 Configuring UIs

UI configurations include:

- Accessing or cancelling terminal configurations by users
- Configuring the number of lines displayed on a terminal
- Configuring the display color of a terminal
- Configuring the display language on a terminal
- Enabling a virtual terminal to receive debugging information or disabling the function
- Setting the login method for a virtual terminal
- Setting the timeout time of a virtual terminal

4.1.5.1 Enabling a Virtual Terminal to Receive Debugging Information or Disabling the Function

Purpose

This section describes how to enable a virtual terminal to receive debugging information or disable the function.

Procedure

The following is the procedure to enable a virtual terminal to receive debugging information or disable the function.

Purpose	Procedure
Enable a CLI terminal to receive debugging information	1. Access the line configuration view. 2. Run the **monitor** command.
Disable a CLI terminal from receiving debugging information	1. Access the line configuration view. 2. Run the **no monitor** command.

4.1.5.2 Accessing or Cancelling Terminal Configurations by Users

Purpose

This section describes how users can access or cancel terminal configurations.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enter the terminal configuration mode	1. Access the global configuration view and line configuration view. 2. Run the **line vty** *vty-number1 vty-number2* command.
Cancel terminal configurations.	1. Access the global configuration view and line configuration view. 2. Run the **no line vty** *vty-number* command.

4.1.5.3 Accessing the Console Terminal Configuration View

Purpose

This section describes how users can access the Console terminal configuration view.

Procedure

The procedure for accessing the Console terminal configuration view is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Access the Console terminal configuration view	1. Access the global configuration view and line configuration view. 2. Run the **line console** *number* command.

4.1.5.4 Closing a Virtual Terminal

Purpose

This section describes how to terminate the connection with a virtual terminal (Telnet or SSH terminal) and reset the terminal.

Virtual terminals are those connecting to the switch through Telnet or SSH.

The switch has five virtual terminals by default. That is, five users can log in to the switch through Telnet or SSH concurrently.

Procedure

The procedure for closing a virtual terminal is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Close a virtual terminal	1. Access the global configuration view. 2. Run the **kill vty** *vty-number* command.

4.1.5.5 Configuring Case Sensitivity of a CLI Terminal

Purpose

This section describes how to configure the case sensitivity of a CLI terminal.

Procedure

The following is the procedure for configuring the case sensitivity of the CLI terminal.

Purpose	Procedure
Configure the case sensitivity of a CLI terminal	1. Access the global configuration view. 2. Run the **case-sensitive** { **enable** | **disable** } command.

4.1.5.6 Configuring the Number of Lines Displayed on a Terminal

Purpose

This section describes how to configure the number of lines displayed on a terminal.
You can use this command to set the number of lines displayed on a screen when using the CLI. If the length is set to 0, the multi-screen display function is disabled.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the number of lines displayed on a terminal	1. Access the global configuration view. 2. Run the **terminal length** { **0** | *terminal-length* | **default** } command.
Restore the default value	1. Access the global configuration view. 2. Run the **no terminal length** command.
Configure the number of the lines that can be displayed on the terminal temporarily	1. Access the global configuration view. 2. Run the **terminal length** { **0** | *terminal-length* } **temporary** command.
Cancel the number of the lines that can be displayed on a terminal	1. Access the global configuration view. 2. Run the **no terminal length temporary** command.

4.1.5.7 Configuring the Display Color of a Terminal

Purpose

This section describes how to set the background color of a virtual terminal. The system supports the following colors: gray, red, green, yellow, blue, purple, water, and white.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the display color of a terminal	1. Access the global configuration view. 2. Run the command **terminal color { gray | red | green | yellow | blue | purple | water | white }.**

4.1.5.8 Configuring the Display Language of a Terminal

Purpose

This section describes how to configure the display language of a terminal.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the display language of a terminal	1. Access the global configuration view. 2. Run the command **line concole**, **line** vty *vty-number*, or **line vty** *vty-number1 vty-number2*. 3. Run the **language** { **chinese** | **english** } command.

4.1.5.9 Enabling a Virtual Terminal to Receive Debugging Information or Disabling the Function

Purpose

This section describes how to enable to display of debugging information on the screen or disable the function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable a virtual terminal to receive debugging information or disable the function	1. Access the global user view. 2. Run the **terminal monitor** command.
Restore the default value	1. Access the global user view. 2. Run the **no terminal monitor** command.

4.1.5.10 Setting the Timeout Time of a Virtual Terminal

Purpose

This section describes how to set the timeout time of a virtual terminal.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the timeout time of a virtual terminal	1. Access the global configuration view. 2. Run the **line concole** or **line vty** command. 3. Run the **timeout** *time* command.
Restore the default value	1. Access the global configuration view. 2. Run the **line concole** or **line vty** command. 3. Run the **no timeout** command.

4.1.5.11 Configuring the No-operation Timeout Time of a Virtual Terminal

Purpose

This section describes how to set the timeout time of a virtual terminal with no operation performed.

Procedure

The following is the procedure for setting and restoring the no-operation timeout time of a virtual terminal. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the no-operation timeout time of a virtual terminal	1. Access the global configuration view. 2. Run the **terminal timeout** *time* command.
Restore the default value	1. Access the global configuration view. 2. Run the **no terminal timeout** command.

4.1.5.12 Displaying Information of Online Users

Purpose

This section describes how to view the maximum number of concurrent online users allowed and the information on online users.

Procedure

The following is the procedure for displaying information of online users.

Purpose	Procedure
Display information of online users	1. Access the privileged user view, global configuration view, or common user view. 2. Run the **show lines** command.

4.1.6 Configuring User Permissions

This section describes how to manage users and distribute user permissions after logging in to the Switch.

4.1.6.1 Adding a User

Purpose

This section describes how to add a user after logging in to the Switch.

Login users on the Switch are classified into four types, as described in Table 4-2. Only users that belong to the Administrators group have the permission to create a new user.

Table 4-2 User types supported by the Switch

User Type	Description
administrators	The administration level has the permission to use all the commands relevant to the basic operation of the system. Commands relevant to the supportive modules are included as well. These commands provide support for services include file system, FTP, TFTP, download, user management, and level setting commands.
operators	System level: has the permission to use the service configuration commands, including the routing command and the command of each network layer. These commands are used to provide users with direct network service.
users	Monitoring level: for system maintenance and service fault diagnosis.
guests	Access level: has the permission to use the network diagnosis command (such as **ping**), user GUI language switching command (**language-mode**) and the telnet command. The command of this level cannot be used to save the configuration file.

Users can only run the commands of their levels or of lower levels. To keep confidentiality, the password is not displayed on the screen. If the password is correctly entered within three times, the user account is switched to a higher-level user; otherwise, it remains at the original level.

Procedure

The procedure for adding a user is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Add a user	1. Access the global configuration view. 2. Run the command **username** *username* **group { administrators | operators | users | guests }.**

4.1.6.2 Deleting a User

Purpose

This section describes how to delete a user after logging in to the Switch.

Only users that belong to the Administrators group have the permission to delete a user.

Procedure

The procedure for deleting a user is as follows. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Delete a user	1. Access the global configuration view. 2. Run the **no username** *username* command.

4.1.6.3 Viewing Attributes of a Created Local User

Purpose

This section describes how to view attributes of a created local user.

Procedure

The following is the procedure for viewing attributes or a created local user. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View Attributes of a Created Local User	1. Access the privileged user view or global configuration view. 2. Run the **show user config** command.

4.1.6.4 Configuring Different Domains to Manage User Login Permissions

Purpose

This section describes how to configure different domains to manage user login permissions.

Procedure

The following is the procedure for configuring different domains to manage user login permissions. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure different domains to manage user login permissions	1. Access the global configuration view. 2. Run the **username** *username* **domain** { **telnet** | **ssh** | **console** | **all** } command.

4.1.6.5 Elevating User Permissions

Purpose

This section describes how to elevate user permissions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Elevate user permissions	1. Access the global configuration view. 2. Run the **enable password level** *level-value* { **cipher** | **plain** } *password* command to configure a password for elevated permissions. 3. Access the line configuration view. 4. Run the **enable authentication local** command to enable the authentication function. 5. If users use permissions lower than the configured level for login, the system enters the privileged user view. 6. Run the **enable** *level-value* command. 7. Input the password set in Step 2. Then, the user permissions are elevated.

4.1.6.6 Setting the Complexity of a User Password

Purpose

This section describes how to set the complexity of a user password.

Procedure

The following is the procedure for setting the complexity of a user password. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the complexity of a user password	1. Access the global configuration view. 2. Run the following commands: ● **username** *word* **pwd-complex** *pwd-complex* ● **user pwd-complex** *pwd-complex*

4.1.6.7 Setting Password Length for a Specified User or All Users

Purpose

This section describes how to set the password length for a specified user or all users

Procedure

The following is the procedure for setting the password length for a specified user or all users. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the password length for a specified user or all users	1. Access the global configuration view. 2. Run the following commands: ● **username** *word* **pwd-length** *pwd-length* ● **user pwd-length** *pwd-length*

4.1.6.8 Setting the Maximum Number of Login Failures for a Specified User

Purpose

This section describes how to set the maximum number of login failures for a specified user.

Procedure

The following is the procedure for setting the maximum number of login failures for a specified user. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the maximum number of login failures for a specified user	1. Access the global configuration view. 2. Run the following commands: ● **user fail-count** *fail-count-time* ● **username** *word* **fail-count** *fail-count-time*

4.1.6.9 Setting a Reauthentication Interval

Purpose

This section describes how to set a reauthentication interval.

Procedure

The following is the procedure for setting the reauthentication interval. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the reauthentication interval	1. Access the global configuration view. 2. Run the following commands: ● **user reauth-interval** *reauth-interval-tim* ● **username** *word* **reauth-interval** *reauth-interval-time*

4.1.6.10 Setting a User FTP Path

Purpose

This section describes how to set a user FTP path.

Procedure

The following is the procedure for setting the user FTP path. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the user FTP path	1. Access the global configuration view. 2. Run the **username user-name ftp-directory { dir | default }** command.

4.1.6.11 Configuring Telnet, SSH, and FTP

Purpose

This section describes how to configure Telnet, SSH, and FTP.

Procedure

The following is the procedure for configuring Telnet, SSH, and FTP. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the maximum number of users that support Telnet, SSH, or FTP login	1. Access the global configuration view. 2. Run the **user** { **telnet** | **ssh** } **max-count** { *count-number* | **default** } command.
Enable or disable SSH debugging	1. Access the privileged user view. 2. Run the following commands: ● **debug ssh** ● **no debug ssh**
Enable or disable SSH file transmission protocol debugging	1. Access the privileged user view. 2. Run the following commands: ● **debug sftp** ● **no debug sftp**
Enable or disable the encryption algorithm supported by the SSH client	1. Access the global configuration view. 2. Run the following commands: ● **ssh { aes128-ctr | aes256-ctr | aes128-cbc | aes256-cbc | 3des-ctr | 3des-cbc } { enable | disable }** ● **ssh { hmac-sha1 | hmac-sha1-96 | hmac-sha2-256 | hmac-sha2-512 | 3 hmac-md5 } { enable | disable }**
Enable or disable the SSH file transmission protocol service	1. Access the global configuration view. 2. Run the **sftp-server** { **enable** | **disable** } command.
Enable the SSH function of the device	1. Access the global configuration view. 2. Run the following commands: ● **sshd** ● **no sshd**
Configure the SSHD authentication mode, password authentication and public key authentication	1. Access the global configuration view. 2. Run the following commands: ● **sshd auth { password | pubkey }** ● **no sshd auth { password | pubkey }**

Purpose	Procedure
Set the SSHD login grace time	1. Access the global configuration view. 2. Run the **sshd login-grace-time** { *login-grace-timer* | **default** } command.
Configure the key string	1. Access the global configuration view. 2. Run the following commands: ● **key { ssh-dss | ssh-rsa }** *key-string* ● **key** *key-string*
Create a public key	1. Access the global configuration view. 2. Run the following commands: ● **ssh keygen dsa** ● **ssh keygen rsa bits { 1024 | 2048 | 3072 }**
Configure an SSH user key	1. Access the global configuration view. 2. Run the **ssh user** *user-name* **key begin** command.
Show the SSH configuration	1. Access the common user view. 2. Run the **show ssh config** command.

4.1.6.12 Querying User Permissions

Purpose

This section describes how to query user permissions.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Query user permissions	1. Access the common user view or privileged user view. 2. Run the **show privilege** command.

4.2 System Configuration File Operation

The Switch provides the file system module for you to effectively manage storage devices such as flash memory. The file system provides the file and directory access management function, including creating, deleting, modifying, and renaming files and directories, and displaying file content. By default, the system gives a prompt for confirming the commands that may cause loss (such as deleting and overwriting files).

The file system operations can be classified into the following types according to different objects:

- Directory operation
- File operation

4.2.1 Directory Operation

Purpose

Operations can be performed to create or delete directories, and display the files under the current working directory, as well as the information under the directories. The following commands can be used for directory operations.

Procedure

The following is the procedure for directory operations. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a directory	In the privileged user view or global configuration view, run the **mkdir** *directory* command.
Delete a directory	In the privileged user view or global configuration view, run the **rmdir** *directory* command.
Check the current working directory	In the privileged user view, run the **pwd** command.
Change the current directory	Run the **cd** *directory* command in the privileged user view.
Update system or configuration files	In the global configuration view, run the **upgrade** { **os | config** } [*local-file-name*] command.
List the content in a directory or its subdirectories	In the privileged user view or global configuration view, run the **ls tree** *directory* command. In the privileged user view or global configuration view, run the **ls tree** *directory* **subtree** command.

4.2.2 File Operation

Purpose

Operations can be performed to delete files, display file content, rename files, copy files, and display the information of designated files. The following commands can be used for file operations.

Procedure

The following is the procedure for file operations. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Delete a file	In the privileged user view, run the **del** *file-name* command.
Delete a file permanently	In the privileged user view, run the **remove** *filename* command.
Rename a file	In the privileged user view, run the **rename** *old -filename new-filename* command.
Copy a folder	In the privileged user view, run the **xcopy** *srcfile destfile* command.
Copy a file	In the privileged user view, run the **cop**y *srcfile destfile* command.
Display the content of a designated binary text file	In the privileged user view, run the **type** *filename* { **binary** | **text** } command.
Clear the content of a specified file	In the privileged user view, run the **zero** *filename* command.

4.2.3 System Configuration File

This section describes operations on the system configuration file.

Switch Local Authentication Modes

Purpose

This section describes how to change the authentication mode to local configuration.

Procedure

The following is the procedure for changing the authentication mode to local configuration.

1. Access the global configuration view.
2. Run the **auth-degenerate** command.

4.2.3.1 Saving the Configuration File

Purpose

This section describes how to save the configuration in the current system to the startup configuration file.

Procedure

The following is the procedure for saving a configuration file.

1. Access the common user view or global configuration view.
2. Run the **write file** command.

4.2.3.2 Viewing and Deleting the OS Files

Purpose

This section describes how to view or delete OS files stored in the switch memory.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the OS files stored in the switch memory	1. Access the common user view. 2. Run the **show os-file** command.
Delete all OS files or OS files with the specified names stored in the switch memory	1. Access the global configuration view. 2. Run the following commands: ● **del os-file** ● **del os-file name**

4.3 Uploading and Downloading Device Files

4.3.1 FTP Configuration

The File Transfer Protocol (FTP) is a universal method of file transmission on the Internet and IP networks. The file transmission provided by FTP is to copy a complete file from a system to another. FTP supports limited file types (such as ASCII and binary) and file structures (byte-oriented stream or record). Most users prefer to use email and Web for file transmission. However, FTP is still widely used. The FTP protocol belongs to the application layer protocol in the TCP/IP protocol suite that is used for file transmission between remote server and local host.

The FTP services provided by the Switch include:

- FTP server service: Users can log in to the server and access the files on it by running the FTP client program (before users log in, the network administrator must configure the IP address of the FTP server in advance).
- FTP client service: After creating the connection between the PC and the Switch (FTP client) by using the terminal emulation program or Telnet program, users can run the command **ftp *X.X.X.X*** (*X.X.X.X* indicates the IP address of the remote FTP server) to create the connection between the Switch and the remote FTP server, and access the files on the remote FTP server.

The Switch supports the FTP function under IPv4 network address.

4.3.1.1 Enabling/Disabling the FTP Server

Purpose

This section describes how to enable and disable the FTP server.

Procedure

The following is the procedure for enabling or disabling the FTP server.

Purpose	Procedure
Enable the FTP server	1. Access the global configuration view. 2. Run the **ftpd** command.
Disable the FTP server	1. Access the global configuration view. 2. Run the **no ftpd** command.

4.3.1.2 Introduction to FTP Client

The FTP client is an auxiliary function provided by the Switch. It is an application module that needs no function configuration. In this case, the Switch serves as the FTP client to connect to the remote server. Users can run the commands of the FTP client for corresponding operations (such as creating or deleting directories).

4.3.1.3 FTP Server Configuration Example

Purpose

This section provides a configuration example to describe how to use the Switch as the FTP server to back up the configuration file and upgrade the software.

Device	Configuration
Switch	Enable the FTP server and set the username, password, and relevant parameters.
PC	Log in to the Switch by using the FTP client program.

Network Requirements

The Switch serves as the FTP server and the remote PC serves as the FTP client. The following configuration on the FTP server is complete: An FTP account with username **switch** and password **hello** is set and is authorized with the read/write permission on the root directory of the flash memory on the Switch. The in-band or out-of-band IP address of the Switch is set to **1.1.1.1** and the IP address of the PC is set to **1.1.1.2**; the route between the Switch and the PC is reachable. The application program **switch.z** of the Switch is saved to the PC. The **switch.z** is uploaded from the PC to the remote Switch via FTP and the configuration file **config** of the Switch is downloaded to the PC for backup.

Network Diagram

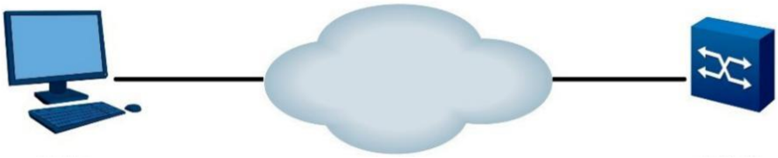


Figure 4-2 FTP configuration network diagram

Configuration

Configuration on the Switch

1) Log in to the Switch (via the Console port locally or via Telnet remotely) and enable the FTP service.

```
Switch#config
Switch(config)#ftpd
```

2) Run the FTP client program on the PC to set up an FTP connection to the Switch. Upload the application program **switch.z** of the Switch to the root directory of the flash memory, and download the configuration file **config** from the Switch. The FTP client application program is not offered.

```
C:\ftp 1.1.1.1
220 FHN(1.0)FTP Server ready
User (1.1.1.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>bin
200 Type set to I, binary mode
ftp> put switch.z
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: Send 3,069,212 bytes in 1.42 seconds, 2158.38 Kbytes/sec.
```

Obtain the switch configuration file.

```
ftp>ascii
200 Type is ASCII
ftp>get startcfg
150 Opening ASCII mode data connection
226 Transfer complete
ftp: Receive 14,251 bytes in 0.22 seconds, 65.07 Kbytes/sec.
```

Caution

If the flash memory of the Switch is not enough, delete the original application programs in the flash memory before uploading the new application program to the flash memory.

3) Perform upgrade on the Switch after uploading is completed.

You can run the **upgrade os** command as the application program for next startup, and then reboot the Switch to upgrade its application program.

```
Switch#config
Switch(config)#upgrade os
Switch(config)#quit
Switch#reboot
```

4.3.1.4 FTP Client Configuration Example

Purpose

This section provides a configuration example to describe how to use the Switch as the FTP client to perform configuration file backup and software upgrade.

<table>
<tr><th>Device</th><th>Configuration</th><th>Configuration Description</th></tr>
<tr><td>Switch</td><td>Log in to the remote FTP server by using the ftp command.</td><td rowspan="2">You must obtain the FTP username and password first and then log in to the remote FTP server to obtain the corresponding directory and file.
● ftp get ipv4-address user password remotefile [port-id]
● ftp get ipv4-address user password remotefile localfile filename [port-id]
● ftp put ipv4-address user password remotefile config
● ftp put ipv4-address user password remotefile localfile filename [port-id]</td></tr>
<tr><td>PC</td><td>Enable the FTP server and set parameters such as username, password, and user permission.</td></tr>
</table>

Network Requirements

The Switch serves as the FTP client and the remote PC serves as the FTP server. The following configuration on the FTP server is complete: An FTP account with username **123** and password **123** is set. The IP address of PC is set to **10.18.1.2.** Users can log in to the Switch remotely via Telnet; the application program of the Switch is downloaded from the FTP server to the flash memory of the Switch; the Switch is remotely upgraded by using command lines.

Network Diagram

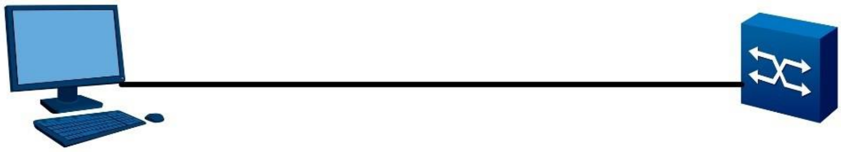


Figure 4-3 Network diagram of the Switch serving as the FTP client

Configuration

Access the global configuration view and use the following commands to perform the FTP connection. Input the correct username and password to log into the FTP server.

```
Switch#config
Switch(config)#ftp get 10.18.1.2 123 123 d:\upgrade.z
Local path is "Ram:/flash/download".
Getting data...
3069212 bytes downloaded
```

Download the upgrade program to the directory "Download" of the switch. Implement upgrade by using the command. Reboot the system to make the new image file effective.

```
Switch(config)#upgrade os
WARNING:System will upgrade! Continue?[y/n]
System now is upgrading,please wait.
%Local path is "Ram:/flash/download".
Switch(config)#reboot
```

Caution

When the PC serves as the FTP server, transmit the image file in bin mode, and transmit the configuration file in ASCII mode.

4.3.2 TFTP Configuration

The Trivial File Transfer Protocol (TFTP) was initially introduced for no-disk system booting (usually work station or X terminal). Compared with FTP, TFTP does not have complex interactive access interfaces or authority control and it is applicable in scenarios with no complex interaction between client and server. The TFTP protocol is usually implemented based on UDP.

The protocol transmission of TFTP is initiated by the client. When file downloading is required, the client sends a read request to the TFTP server, receives data from the server, and then sends a confirmation to the server. When file uploading is required, the client sends a write request to the TFTP server, sends data to the server, and receives a confirmation from the server. The file transmission of TFTP is in binary mode.

Before TFTP configuration, the network administrator needs to configure IP addresses of the TFTP client and server in advance, and make sure that the route between client and server is reachable.

The Switch supports the TFTP function under IPv4 network address.

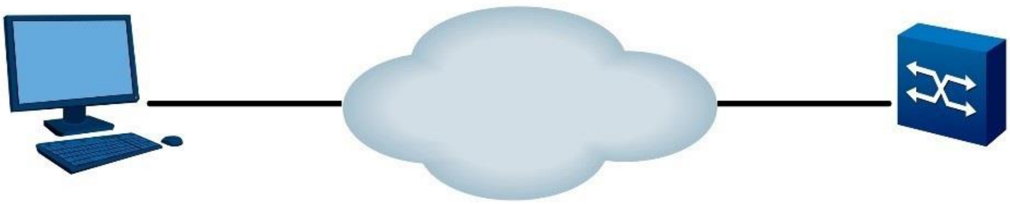


Figure 4-4 TFTP configuration network diagram

4.3.2.1 Configuring the TFTP Server Function

Purpose

This section describes how to enable or disable the TFTP server function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the TFTP server function	1. Access the global configuration view. 2. Run the **tftpd** command to enable the TFTP Server function of the device.
Disable the TFTP server function	1. Access the global configuration view. 2. Run the **no tftpd** command to disable the TFTP server function of the device.

4.3.2.2 Downloading Files via TFTP

Caution

It is recommended that you use this command under instruction of technical support personnel.

Purpose

To download files, the client sends a read request to the TFTP server, receives data from the server, and then sends a confirmation to the server. During switch running maintenance, you need to download the configuration file or operating system file from the host to the switch to configure or upgrade the operating system. This command is used to download such files to the switch.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Download a remote file via TFTP and save it locally. (This command applies to IPv4 networks.)	1. Access the global configuration view. 2. Run the **tftp get** *ipv4-address remotefile* **localfile** *filename* [*port-id*] command.

4.3.2.3 Uploading Files via TFTP

Caution

It is recommended that you use this command under instruction of technical support personnel.

Purpose

When the Switch needs to upload files to the TFTP server, the Switch serves as the client to send a write request to the TFTP server, sends data to the server, and then receives a confirmation from the server. The following commands can be used to upload files.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Upload the local file to the remote TFTP server (This command applies to IPv4 networks.)	1. Access the global configuration view. 2. Run the following commands: ● **tftp put** *ipv4-address remotefile* **config** ● **tftp put** *ipv4-address remotefile* **localfile** *filename [port-id]*
Enable the IPv4 Telnet server function for the switch	1. Access the global configuration view. 2. Run the **telnetd** command to enable the IPv4 Telnet server function for the switch.
Disable the IPv4 Telnet server function for the switch	1. Access the global configuration view. 2. Run the **no telnetd** command to disable the IPv4 Telnet server function for the switch.
Export content in the device default folder to a PC via TFTP	1. Access the global configuration view. 2. Run the **file export tftp** *ipv4-address remotedir localdir* command.

4.3.2.4 TFTP Client Configuration Example

Caution

It is recommended that you use this command under instruction of technical support personnel.

Purpose

This section provides a configuration example to describe how to use the Switch as the TFTP client to perform configuration file backup and software upgrade.

Device	Configuration	Configuration Description
Switch	Use the TFTP command directly to log in to the remote TFTP server to upload or download files.	TFTP is applicable for the environment with uncomplex interaction between client and server. Make sure that the route between switch and TFTP server is reachable.
PC	Enable the TFTP server. Configure the TFTP working directory.	-

Network Requirements

The Switch serves as the TFTP client and the PC serves as the TFTP server. The TFTP working path is configured on the TFTP server. The in-band IP address of the Switch is set to **1.1.1.1** (the port of the Switch connecting to the PC belongs to this VLAN) and the IP address of the PC is set to **1.1.1.2**. The application program **switch.z** of the Switch is saved to the PC. The Switch downloads **switch.z** from the TFTP server via TFTP, and uploads the configuration file to the working directory **vrpcfg.txt** of the TFTP server for backup.

Network Diagram

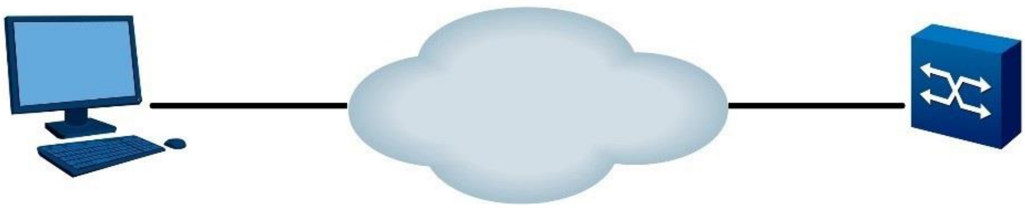


Figure 4-5 TFTP configuration network diagram

Configuration

1) Enable the TFTP server function on the PC and configure the working directory of the TFTP server.

2) Configure the switch.

Users log into the switch (via the Console port locally or via Telnet remotely) and access the global configuration view.

```
Switch#config
Switch(config)#tftp get 1.1.1.2    switch.z
Switch(config)#tftp put 1.1.1.2    vrpcfg.txt config
```

Chapter 5 L2 Ethernet Configuration

This chapter introduces the L2 Ethernet basic function configuration of the Switch.

5.1 Ethernet Interface Configuration

This section describes Ethernet interface configurations.

5.1.1 Configuring Basic Attributes of the Ethernet Interface

5.1.1.1 Accessing the Ethernet Port View

Background

You need to access the Ethernet port configuration view first and then configure the Ethernet port. This section describes how to access the Ethernet port view.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Access the Ethernet Port View	1. Access the global configuration view. 2. Run the following commands: ● **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **to { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **interface eth-trunk** *trunk-number*
Exit the Ethernet port view	1. Access the interface configuration view. 2. Run the **quit** command.
Enter the batch interface configuration view	1. Access the global configuration view. 2. Run the **interface group** *port-list* command.

5.1.1.2 Enabling/Disabling an Ethernet Interface

Background

After configuring the parameters and protocol of the interface, run the **no shutdown** command to enable the interface. You can also use the **shutdown** command to disable the interface so that it cannot forward data anymore. By default, the interface is enabled.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Disable an Ethernet interface. If an interface is idle (with no cable connected), run the **shutdown** command to shut down the interface. This prevents exceptions caused by interference.	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, batch interface configuration view, or VLANIF configuration view. 3. Run the **shutdown** command to shut down the current Ethernet interface.
Enable an Ethernet interface. When interface attributes are modified and new configuration has not taken effect, the **shutdown** and **no shutdown** commands can be used to disable and re-enable the interface to make the new configuration effective.	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, batch interface configuration view, or VLANIF configuration view. 3. Run the **no shutdown** command to start the current Ethernet interface.

5.1.1.3 Configuring the Ethernet Interface Rate

Background

You can use the following command to set the rate of the Ethernet interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the Ethernet interface rate	1. Access the global configuration view. 2. Run the **port mode** { **10xgi** | **25gi** } **interface** { **10gigaethernet** | **25gigaethernet** } *interface-number* command to set a rate for the interface. A 25G interface can be changed to a 10G port.

5.1.1.4 Configuring Ethernet Interface Flow Control

Background

After the local and peer switches are enabled with flow control, the local switch sends a message to the peer switch to instruct it to stop sending messages if congestion occurs on the local switch. The peer switch stops sending messages to the local switch once it receives the message, and vice versa. This mechanism avoids message loss. The following commands can be used to enable or disable flow control on the local Ethernet interface. Once flow control is disabled, the interface no longer sends flow control frames.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable Ethernet interface flow control	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **flow-control enable** command.
Disable Ethernet interface flow control	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **flow-control disable** command.

5.1.1.5 Configuring Broadcast/Multicast Message Suppression Function for the Ethernet Interface

Purpose

To prevent port blocking caused by flooding of broadcast/multicast messages, the switch provides the broadcast/multicast message suppression function. You can suppress broadcast, multicast, and unknown unicast messages by configuring bandwidth.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the Ethernet interface to perform storm control on broadcast, multicast, and	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the following commands:

Purpose	Procedure
unknown unicast messages	• **storm-control { broadcast | multicast | dlf } cir { gbps | kbps | mbps }** *value* • **storm-control { broadcast | multicast | dlf } percent** *value* (support only the Ethernet interface configuration view) • **storm-control { broadcast | multicast | dlf } pps** *control-value*
Cancel the storm control function	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **no storm-control { broadcast | multicast | dlf }** command.

5.1.1.6 Configuring Ethernet Interface Rate Suppression

Background

There are particular situations where the interface rate must be controlled to provide different bandwidths for different users. This can be achieved by rate suppression. The specific input/output bandwidth control granularity may vary depending on different interface types.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure rate suppression for the Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the **rate-limit out { gbps | kbps | mbps }** *rate-limit* command.
Configure the bandwidth alarm threshold and alarm recovery threshold	1. Access the global configuration view. 2. Access the Ethernet bridge interface configuration view or Ethernet routing interface configuration view. 3. Run the following commands: • **rate-limit out threshold {** *threshold-value* **| default }** • **rate-limit out threshold {** *threshold-value* **| default } resume-threshold { resume-***threshold-value* **| default** }
Cancel rate suppression configuration on the Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the **no rate-limit out** command.

5.1.1.7 Configuring the Interface Priority

Background

By configuring the priorities of different interfaces, you can ensure that important services are not delayed or discarded and guarantee the efficiency of network operation.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the Ethernet interface priority	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the **priority** *priority-level* command.

5.1.1.8 Configuring Maximum Transmission Unit (MTU) of the Ethernet Interface

Background

In high-throughput scenarios of data exchange such as file transmission, a long frame that exceeds the standard Ethernet frame length may occur. The following commands can be used to configure the size of frames allowed to pass.

The MTU of the Ethernet interface only affects the IP packet assembly or depacketization on the Ethernet interface. The MTU in Ethernet_II format is 1500. The MTU in Ethernet_SNAP frame format is 1492.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the maximum transmission unit (MTU) of the Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the **mtu** *mtu-value* command.

5.1.1.9 Clearing the Statistics of the Current Interface

Purpose

This section describes how to clear large volumes of information in an interface configuration view.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Clear the statistics of the current Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the **reset counter** command.

5.1.1.10 Clearing Statistics of a Specified Interface

Purpose

This command is used to clear statistics of a specified interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Clear statistics of a specified interface	1. Access the global configuration view. 2. Run the following commands to clear statistics of a specified interface: ● **reset counter interface eth-trunk** *trunk-number* ● **reset counter interface tunnel** *tunnel-number* ● **reset counter interface nve** *nve-id* ● **reset counter interface bridge-domain** *bd-id* ● **reset counter interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **reset counter interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **reset counter interface eth-trunk** *trunk-number.subinterface* ● **reset counter interface mgt-eth** *outband-number* ● **reset counter interface all**

5.1.1.11 Describing the Ethernet Interface

Purpose

This section describes how to configure descriptive strings by using the following commands to distinguish interfaces.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the descriptive string of the Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), or VLANIF configuration view. 3. Run the **alias** *description* command.
Delete the descriptive string of the Ethernet interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), or VLANIF configuration view. 3. Run the **no alias** command.

5.1.2 Configuring Advanced Attributes of the Ethernet Interface

5.1.2.1 Configuring Interface Loopback Detection

Purpose

This section describes how to enable interface loopback monitoring and configure the interval of periodic monitoring of external loopback. If one interface has loopback, the switch applies the configured measures to this interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Globally disable or automatically restore loopback detection	1. Access the interface group configuration view or interface configuration view. 2. Run the **loop-check action { block | shutdown | trap }** command. This command is used to configure the way of dealing with looped interface after a loop is found.
Globally enable/disable the trap alarm of interface loopback detection	1. Access the global configuration view. 2. Run the **loop-check tra**p { **enable** | **disable** } command.
Specify the VLAN in which loopback detection is performed on an interface of the switch	1. Access the interface configuration view (Ethernet or Trunk). 2. Run the **loop-check vlan** *vlan-list* command.
Enable/disable interface loopback detection	1. Access the interface configuration view (Ethernet or Trunk). 2. Run the **loop-check** { **enable** | **disable** } command.
Re-enable interface loopback detection	1. Access the interface configuration view (Ethernet or Trunk). 2. Run the **loop-check reset** command.
Debug interface loopback detection display	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show loop-check** command.
	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show loop-check** interface command.

5.1.2.2 Configuring CRC Detection for an Interface

Purpose

The following configuration task can enable a port to enter error down state when the number of received CRC error packets exceeds the threshold, or disable a port from going down in this case.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable a port to enter error down state when the number of received CRC error packets exceeds the threshold, or disable a port from going down in this case	1. Access the Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, or GRP routing interface configuration view. 2. Run the **port crc-error error-down { enable | disable }** command.
Configure the alarm interval for CRC error packets	1. Access the global configuration view. 2. Run the **crc-error protection interval** *interval* command.
Configure the CRC error packet alarm threshold of a port	1. Access the Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, or GRP routing interface configuration view. 2. Run the **port crc-error threshold** *threshold* command.
Configure the automatic recovery interval for ports going down when the number of CRC error packets exceeds the threshold	1. Access the global configuration view. 2. Run the **error-down auto-recovery cause crc-error interval** *interval* command.
Disable a port in error down state from going up automatically	1. Access the global configuration view. 2. Run the **no error-down auto-recovery cause crc-error** command.
Delete the CRC error packet alarm threshold of a port	1. Access the Ethernet bridge interface configuration view, Ethernet routing interface configuration view, GRP bridge interface configuration view, or GRP routing interface configuration view. 2. Run the **no port crc-error threshold** command.
Delete the alarm interval for CRC error packets	1. Access the global configuration view. 2. Run the **no crc-error protection interval** command.
View the check error configuration.	1. Access the common user view. 2. Run the **show crc-error config** command.

5.1.2.3 Displaying the Ethernet Interface Status

Background

Run the **show** command in the user view to display the operation condition of the configured Ethernet interface. You can verify the configuration by viewing the displayed information. In the Ethernet interface view, run the **reset count** command to clear the statistics of the Ethernet interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the Ethernet interface status and information	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show interface** ● **show interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **config** ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**
Display the basic information of all Ethernet interfaces and trunk interfaces (if configured) of the current device	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show interface eth-trunk** *trunk-number* **verbose** ● **show interface eth-trunk verbose** ● **show interface verbose**
Display the reference count of an Ethernet interface and its sub-interfaces	1. Access the common user view. 2. Run the following commands: ● **show l3int ethernet** *interface-number* ● **show l3int ethernet** *interface-number.subinterface-number*

5.1.2.4 Switching Between Different Ethernet Interface Configuration Views

Purpose

This section describes how to configure other interface attributes after you configure the current interface attribute.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Switch the current Ethernet interface configuration view to another Ethernet interface view	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the command **switch { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernetethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.

5.2 Configuring MAC Address Tables

To quickly forward packets, the switch needs to maintain a MAC address table. The MAC address entries include the MAC address of the device connected to the switch and the interface number of the switch connected to the device. The dynamic entries (not configured manually) of the MAC address table are learned by the switch. The method of how the switch learns MAC addresses is as follows: If one port (supposed to be Port A) receives a data frame, the switch analyzes the source MAC address (supposed to be MAC-SOURCE) of this data frame and determines that the message with the destination MAC address MAC-SOURCE can be forwarded by Port A. If MAC-SOURCE is included in the MAC address table, the switch updates the corresponding entry. If MAC-SOURCE is not included in the MAC address table, the switch adds this new MAC address (and the forwarding port corresponding to this MAC address) to the MAC address table.

For the message whose destination MAC address is found in the MAC address table, the system uses hardware to forward the message directly. For the message whose destination MAC address is not found in the MAC address table, the system forwards the message in broadcast mode. After broadcasting, if the message reaches the device corresponding to this destination MAC address, the destination device responds to this broadcast message and the response message includes the MAC address of this device. The switch adds the new MAC address to the MAC address forwarding table by address learning. The subsequent messages to the same destination MAC address are directly forwarded based on the new MAC address entry.

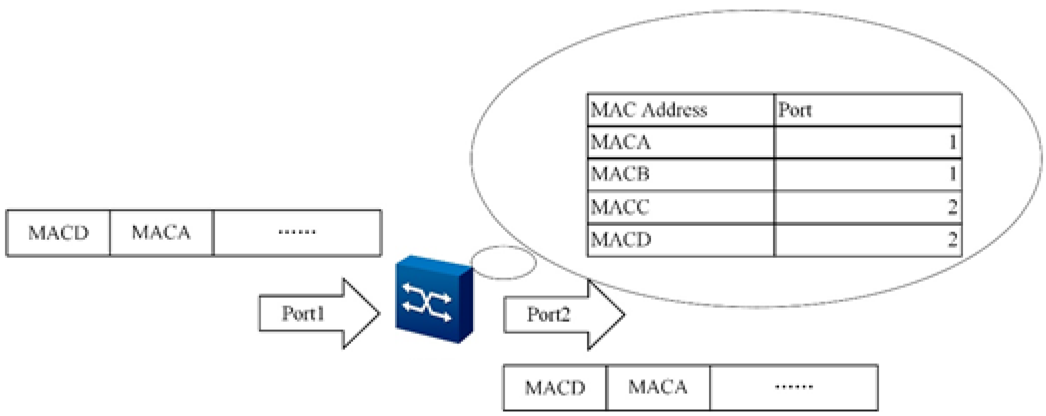


Figure 5-1 Message forwarded by the switch using forwarding table

5.2.1 Configuring a MAC Address Entry

Purpose

The administrator can manually add, modify, or delete entries of the MAC address table according to the actual condition.

Use static MAC addresses to bind user devices with interfaces. This can prevent unauthorized users with fake identity from obtaining data and improve device security.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Add a blackhole MAC address table entry	1. Access the global configuration view. 2. Run the **mac-address blackhole** *vlan-id mac-address* command.
Delete blackhole MAC entries	1. Access the global configuration view. 2. Run the following commands: ● **no mac-address blackhole** ● **no mac-address blackhole** *mac-address* ● **no mac-address blackhole** *vlan-id* ● **no mac-address blackhole** *vlan-id mac-address*
Display the MAC address learning limit configured on the switch	1. Access the interface configuration view (Ethernet), interface group configuration view or VLAN configuration view. 2. Run the following commands: ● **mac-limit {** *limit-value* | **default** } ● **mac-limit {** *limit-value* | **default } action { forward | drop }**
Add a static MAC address entry	1. Access the global configuration view. 2. Run the following commands: ● **mac-address static *vlan-id mac-address* { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **mac-address static** *vlan-id mac-address* **eth-trunk** *trunk-number*
Delete a MAC address entry	1. Access the global configuration view (the first command can be run in the slot node view). 2. Run the following commands: ● **no mac-address static** ● **no mac-address static** *vlan-id*

Purpose	Procedure
	● **no mac-address static** *mac-address* ● **no mac-address static** *vlan-id mac-address* ● **no mac-address static { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no mac-address static eth-trunk** *trunk-number*

5.2.2 Configuring Dynamic MAC Address Aging Time

Background

An appropriate aging time can help implement the MAC address aging function effectively. If the configured aging time is too long or too short, the switch broadcasts a large number of messages whose destination MAC address cannot be found, which affects the running performance of the switch. If the aging time is too long, the switch may store many outdated MAC address entries and this exhausts the MAC address table resources. As a result, the switch cannot update the MAC address table according to the change of the network. If the aging time is too short, the switch may delete effective MAC address entries.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Note:

Once the system is reset, dynamic entries are lost, but the stored static entries and blackhole entries are not aged or lost.

Purpose	Procedure
Configure the aging time of MAC address dynamic entries	1. Access the global configuration view. 2. Run the **mac aging-time** *aging-time* command.

5.2.3 Configuring MAC Address Flapping Detection

Purpose

This function detects whether MAC address flapping occurs on all devices.

Background

MAC address flapping means that two or three ports in one VLAN learn a MAC address and the learned MAC address entries overwrite the original ones. Generally, the interface by which the MAC address is learned first is the correct outbound interface and is called the original port, and all other ports learning the MAC address later are the move ports. Move ports are often ports in a loop or looped ports in a network. You must disable move ports or enable storm suppression for move ports.

By default, the system detects MAC address flapping for all VLANs of the switch. Virtualization of data centers (migration of virtual terminals) may also cause MAC address flapping, but this is normal and will not be detected as MAC address flapping. You can add the VLAN of a virtual terminal to the MAC address flapping detection whitelist to disable this function for this VLAN.

If the aging time for MAC address flapping entries is prolonged, flapping may occur again and the Error-Down time is prolonged. To detect MAC address flapping normally, modify the aging time for MAC address flapping entries.

If MAC address flapping occurs due to loopback in the network and the network does not support the loop breaking protocol, you can configure an action for an interface taken after MAC address flapping occurs, so as to break the loop.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure MAC address flapping detection. The function is enabled by default.	1. Access the global configuration view. 2. Run the **mac-address flapping detection** { **enable** | **disable** } command.
Configure the aging time for MAC address flapping entries	1. Access the global configuration view. 2. Run the **mac-address flapping aging-time {** ***aging-time*** **| default }** command.
Enable global MAC address flapping detection	1. Access the global configuration view. 2. Run the **mac-address flapping detection vlan** *vlan-id* **security-level { high | middle | low }** command.
Configure a VLAN whitelist for MAC address flapping detection, that is, specify VLANs for which	1. Access the global configuration view. 2. Run the **mac-address flapping detection exclude-vlan** *vlan-id* command.

Purpose	Procedure
MAC address flapping detection is disabled	
Enable the function of and set the time for reconnecting an interface to a VLAN after the interface is disconnected from the VLAN due to MAC address flapping	1. Access the global configuration view. 2. Run the **mac-address flapping quit-vlan recover-time {** *time* | **default }** command.
Enable automatically restoring the interface state from **down** to **up** when the interface state changes to **down** due to MAC address flapping and set the delay time for automatically restoring the interface state to **up**	1. Access the global configuration view. 2. Run the **error-down auto-recovery cause mac-address-flapping interval** *interval* command.
Disable automatically restoring the interface state from **down** to **up**	1. Access the global configuration view. 2. Run the **no error-down auto-recovery cause mac-address-flapping** command.
Configure the action for an interface after the interface MAC address flaps	1. Access the Ethernet bridge interface configuration view or interface configuration view (Trunk). 2. Run the **mac-address flapping action { quit-vlan | error-down }** command.
Configure the priority of the interface action when the MAC address flaps	1. Access the Ethernet bridge interface configuration view or interface configuration view (Trunk). 2. Run the **mac-address flapping action priority** { *priority* | **default** } command.
Disable the action for an interface after the interface MAC address flaps	1. Access the Ethernet bridge interface configuration view or interface configuration view (Trunk). 2. Run the **no mac-address flapping action** command.
View MAC address flapping activity records and aging records	1. Access the common user view. 2. Run the **show mac-address flapping record** command.
Delete MAC address flapping aging record	1. Access the common user view. 2. Run the **reset mac-address flapping record** command.

5.2.4 Configuring the MAC Address Learning or Aging Alarm Function

Purpose

This section describes how to configure the MAC address learning or aging alarm function.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable the MAC address learning or aging alarm function	1. Access the Ethernet bridge interface configuration view or interface configuration view (Trunk). 2. Run the **mac-address notification** { **add** | **remove** | **all** } command.
Disable the MAC address learning or aging alarm function	1. Access the Ethernet bridge interface configuration view or interface configuration view (Trunk). 2. Run the **no mac-address notification** command.
Configure the maximum number of MAC address learning or aging alarm entries	1. Access the global configuration view. 2. Run the **mac-address notification history-size** { *history-size* | **default** } command.
Configure the interval for MAC address learning or aging detection	1. Access the global configuration view. 2. Run the **mac-address notification interval** { *interval-value* | **default** } command.
Display MAC address learning or aging alarm entries	1. Access the common user view. 2. Run the **show mac-address notification history** command.
Delete all MAC address learning or aging alarm entries	1. Access the global configuration view. 2. Run the **reset mac-address notification history** command.

5.2.5 Displaying L2 MAC Address Entries

Purpose

This section describes how to quickly locate the specified MAC address entry for convenient query of specific information.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the L2 static forwarding table	1. Access the privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), common user view, or interface group configuration view. 2. Run the following commands: ● **show mac-address vlan** *vlan-id* ● **show mac-address vsi** *vsi-name* ● **show mac-address** *mac-address* ● **show mac-address** *mac-address* **vlan** ***vlan-id*** ● **show mac-address { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-address eth-trunk** *trunk-number*
Display the number of MAC addresses based on interface, VLAN, or slot	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show mac-address total-number** ● **show mac-address total-number { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-address total-number eth-trunk** *trunk-number* ● **show mac-address total-number vlan** *vlan-id*
Display dynamic MAC address table entry information based on interface or VLAN	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show mac-address dynamic { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-address dynamic eth-trunk** *trunk-number* ● **show mac-address dynamic vlan** *vlan-id*

Purpose	Procedure
Display configured MAC address learning limit rules	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), VLAN configuration view, or interface group configuration view. 2. Run the following commands: ● **show mac-limit** ● **show mac-limit interface** ● **show mac-limit interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-limit interface eth-trunk** *trunk-number*
Display static MAC address table entry information	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show mac-address static** ● **show mac-address static vlan** *vlan-id* ● **show mac-address static vlan** *vlan-id* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-address static vlan** ***vlan-id*** **eth-trunk** *trunk-number* ● **show mac-address static { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show mac-address static eth-trunk** *trunk-number*

5.3 ARP Configuration

The Address Resolution Protocol (ARP) mapping table can be maintained dynamically or manually. Static ARP is the mapping from manually configured IP address to MAC address. You can check, add, or delete entries of the ARP mapping table by using manual maintenance commands.

5.3.1 Adding or Deleting Static ARP Mapping Entries Manually

Purpose

This section describes how to add/delete static ARP mapping entries manually.
Static ARP entries can only be deleted manually, and will not be aged out or updated dynamically. These static ARP entries are always effective during normal operation of the switch.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Add a static ARP mapping entry	1. Access the global configuration view. 2. Run the following commands: ● **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id* ● **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* ● **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vpn-instance** *name* ● **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id* **vpn-instance** *name*

	- **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **vpn-instance** *name* - **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id* **inner-vlan** *inner-vid* - **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **inner-vlan** *inner-vid* - **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name* - **ip arp** *ip-address mac-address* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name* - **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number* - **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number* **vpn-instance** *name* - **ip arp** *ip-address mac-address* **vlan** *vlan-id* - **ip arp** *ip-address mac-address* **vlan** *vlan-id* **vpn-instance** *name* - **ip arp** *ip-address mac-address* **vlan** *vlan-id* **inner-vlan** *inner-vid* - **ip arp** *ip-address mac-address* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name* - **ip arp** *ip-address mac-address*
Delete a static ARP mapping table entry	1. Access the global view. 2. Run the following commands: - **no ip arp** *ip-address* - **no ip arp** *ip-address* **vpn-instance** *name*。

5.3.2 Clearing Dynamic ARP Mapping Entries

Purpose

This section describes how to clear dynamic ARP mapping entries.

You can manually delete all dynamic ARP mapping entries when necessary.

This command cancels mappings between IP and MAC addresses, which may lead to temporary access failures to some nodes. Therefore, exercise caution when using this command.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Clear dynamic ARP mapping entries	1. Access the global configuration view. 2. Run the **flush arp dynamic** command.

5.3.3 Viewing ARP Information

Purpose

This section describes how to view ARP information. You can view the ARP mapping table in LAN to detect faults. ARP establishes a relationship between network address and local network hardware address. Each record is kept in the cache for a period of time and then is discarded.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the current ARP learning mode of all VLANs	1. Access the common user view. 2. Run the show arp learning strict command.
Display ARP related information, including ARP dynamic address statistics and aging time of ARP mapping table entries.	1. Access the common user view. 2. Run the following commands: ● **show ip arp** ● **show ip arp** *ip-address* ● **show ip arp dynamic** ● **show ip arp static**

Configuration under multi-instance VPN is also supported.	● **show ip arp { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show ip arp eth-trunk** ***trunk-number*** ● **show ip arp vpn-instance** *name*。
Display the maximum number of dynamic ARP mapping entries that can be learned by an interface	1. Access the common user view. 2. Run the following commands: ● **show arp-limit maxnum vlan** *vlan-id* ● **show arp-limit maxnum { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show arp-limit maxnum eth-trunk** *turnk-number* ● **show arp-limit maxnum**

5.3.4 Configuring Dynamic ARP Mapping Entry Aging Time

Purpose

This section describes how to configure the aging time of dynamic ARP mapping entries.
Setting an appropriate aging time of dynamic ARP mapping entries can reduce the address resolution errors caused by slow updates of dynamic ARP entries.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure dynamic ARP mapping entry aging time	1. Access the global configuration view. 2. Run the **ip arp aging-time** { *aging-time* | **default** } command.

5.3.5 Enabling the ARP Module to Forward Host Routes

Purpose

This section describes how to enable the ARP module to forward host routes or disable such forwarding.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable the ARP module to forward host routes	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **arp direct-route enable** command.
Disable the ARP module to forward host routes	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **arp direct-route disable** command.

5.4 Link Aggregation Configuration

5.4.1 Overview of Port Aggregation

Port aggregation is to aggregate multiple ports into one single aggregation group to implement traffic sharing among member ports and improve connection reliability. Link aggregation is divided into manual aggregation, dynamic LACP aggregation, and static LACP aggregation. Ports in the same aggregation group must have the same port type. That is, if one of the ports is an electrical/optical port, all the others must be the same.

Currently, the Switch supports only manual and static LACP link aggregation modes.

5.4.2 Configuring the Aggregation Group Function

Caution

Make sure no member interface has been added to the Eth-Trunk interface before changing its working mode; otherwise, the Eth-Trunk working mode cannot be changed. To delete an existing member interface, run the **no join eth-trunk** command in the corresponding interface view.

Or run the **remove { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* command in the Trunk view.

Purpose

Run the following commands to configure an aggregation group along with basic functions and add multiple member interfaces to increase the bandwidth between devices and enhance reliability.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an Eth-Trunk interface and access its configuration view	1. Access the global configuration view. 2. Run the **interface eth-trunk** *trunk-number* command to create an aggregation group and access its configuration view. If the desired group already exists, access its configuration view directly.
Configure the working mode of Eth-Trunk	1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view.

Purpose	Procedure
	3. Run the **mode** { **manual** | **lacp-static** } command to configure a working mode for Eth-Trunk.
Add member interfaces to Eth-Trunk	Method 1: 1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the command **add { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* to add member interfaces. Method 2: 1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **join eth-trunk** *trunk-number* command to add the current interface to Eth-Trunk.
(Optional) Configure the load sharing mode	1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the following commands: ● **load-balance { src-mac | dst-mac | srcdst-mac | src-ip | dst-ip | srcdst-ip | default | schedule-profile }** ● **load-balance schedule-profile** *profile-name*。
(Optional) Set the active interface quantity threshold	Configure the maximum number of active interfaces 1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the **active-linknumber max** { *max-number* | **default** } command to configure the upper threshold of link aggregation active interface number. Configure the minimum number of active interfaces 1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the **active-linknumber min** { *min-number* | **default** } command to configure the lower threshold of link aggregation active interface number.
(Optional) Configure LACP priority of the system	1. Access the global configuration view. 2. Run the **lacp system-priority** { *priority* | **default** } command to configure the LACP priority for the current device's system.
Delete member interfaces from the interface configuration view (Trunk)	1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the following commands:

Purpose	Procedure
	● **remove { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **remove { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **to { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
Configure the timeout time for Eth-Trunk to receive LACP packets in LACP mode	1. Access the global configuration view. 2. Access the Eth-Trunk interface configuration view. 3. Run the **lacp timeout** *timeout-value* command to configure the timeout time for the Eth-Trunk interface to receive LACP packets in LACP mode.
Configure the load balancing mode for unknown unicast packets on a Trunk interface when the packets are forwarded by an aggregation port VLAN	1. Access the global configuration view. 2. Run the following commands: ● **unknown-unicast load-balance { dst-mac | src-mac | srcdst-mac | default }** ● **unknown-unicast load-balance schedule-profile** *name*。
Enable or disable the LACP port ID for a Trunk interface	1. Access the interface configuration view (Trunk) or Peerlink configuration view. 2. Run the **lacp port-id extension { enable | disable }** command.
Configure the LACP system ID for a Trunk interface.	1. Access the interface configuration view (Trunk) or Peerlink configuration view. 2. Run the **lacp system-id** *system-id-address* command.

5.4.3 Configuring Enhanced Load Balancing

Purpose

This section describes how to configure enhanced load balancing.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an enhanced load balancing template and enter the template view	1. Access the global configuration view. 2. Run the **schedule-profile** { *profile-name* | **default** } command to access the enhanced load balancing template view.
Configure the load balancing mode of IPv4 packets in the enhanced load balancing template	1. Access the global configuration view. 2. Access the enhanced load balancing template view. 3. Run the following commands: ● **ip field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | all | default }** ● **no ip field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port }**
Configure the load balancing mode of IPv6 packets in the enhanced load balancing template	1. Access the global configuration view. 2. Access the enhanced load balancing template view. 3. Run the following commands: ● **ipv6 field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | all | default }** ● **no ipv6 field { src-ip | dst-ip | vlan | l4-srcport | l4-dstport | protocol | src-port | dst-port | all | default }**
Configure the load balancing mode of L2 packets in the enhanced load balancing template	1. Access the global configuration view. 2. Access the enhanced load balancing template view. 3. Run the following commands: ● **l2 field { src-mac | dst-mac | l2-protocol | vlan | src-port | dst-port | all | default }** ● **no l2 field { src-mac | dst-mac | l2-protocol | vlan | src-port | dst-port }**
Configure the load balancing mode of MPLS packets in the enhanced load balancing template	1. Access the global configuration view. 2. Access the enhanced load balancing template view. 3. Run the following commands: ● **mpls field { top-label | 2nd-label | src-ip | dst-ip | vlan | src-port | dst-port | all | default }** ● **no mpls field { top-label | 2nd-label | src-ip | dst-ip | vlan | src-port | dst-port | all | default }**

5.4.4 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the LACP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the LACP configuration file	1. Access the common user view. 2. Run the **show lacp config** command to display the information of the LACP aggregation configuration file.
View the information of a specified or all LACP group(s)	1. Access the common user view. 2. Run the **show lacp eth-trunk** [*trunk-number*] command to display the status all or a specified LACP group(s).
View the LACP configuration	1. Access the common user view. 2. Run the **show lacp system** command to display LACP configurations.
View statistics on sent and received LACP packets in LACP mode	1. Access the common user view. 2. Run the **show lacp statistic interface eth-trunk** *trunk-number* command to view statistics on sent and received LACP packets in LACP mode.
View attributes of an interface and related information	1. Access the common user view. 2. Run the following commands: ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**
View the configuration of a Trunk interface	1. Access the common user view. 2. Run the following commands: ● **show interface eth-trunk** *trunk-number* **verbose** ● **show interface eth-trunk verbose** ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**
View the statistics on an interface	1. Access the common user view. 2. Run the following commands: ● **show interface statistic brief eth-trunk** *trunk-number* ● **show interface statistic eth-trunk** *trunk-number*
View the reference count of a Trunk interface	1. Access the common user view. 2. Run the **show l3int eth-trunk** *trunk-number* command.

Purpose	Procedure
Enable or disable debugging of a load balancing template	1. Access the privileged user view. 2. Run the following commands: ● **debug schedule-profile { config | event | all }** ● **no debug schedule-profile { config | event | all }**
View details about an enhanced load balancing template	1. Access the common user view. 2. Run the following commands: ● **show schedule-profile** ● **show schedule-profile** *profile-name*
View the configuration of unknown unicast load balancing	1. Access the common user view. 2. Run the **show unknown-unicast load-balance** command to view the configuration of unknown unicast load balancing.
Enable or disable debugging of an LACP module	1. Access the privileged user view. 2. Run the following commands: ● **debug lacp { timer | event | churn | mux | rx | tx | config | logic | sync | all }** ● **no debug lacp { timer | event | churn | mux | rx | tx | config | logic | sync | all }**
Clear the LACP statistic of all interfaces	1. Access the global configuration view. 2. Run the **reset lacp statistic** command to clear the LACP statistic of all interfaces.
Clear the LACP statistic of all interfaces	1. Access the global configuration view. 2. Run the command **reset lacp statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* to clear the LACP statistic of all interfaces.
Clear the LACP statistic of a Trunk interface	1. Access the global configuration view. 2. Run the **reset lacp statistic interface eth-trunk** *trunk-number* command to clear the LACP statistic of a Trunk interface.

5.4.5 Typical Link Aggregation Example

Network Requirements

Configure a link aggregation group on two directly connected switches to improve the bandwidth and reliability between them.

The requirements are as follows.

- The link between the two devices provides the redundancy backup function. If part of the links is faulty, the standby link takes over to guarantee normal data transmission.
- The active link provides the load sharing function.

Network Diagram

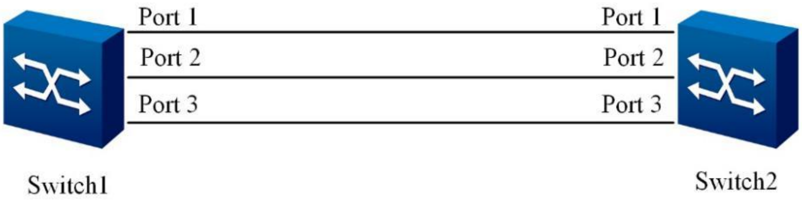


Figure 5-2 Link aggregation configuration topology

Configuration

Note: The configuration of both ends is the same and here we only list configuration of one end.

```
1. Create a link aggregation group
Switch(config)#interface eth-trunk 1
Switch(config-eth-trunk-1)#no shutdown
Switch(config-eth-trunk-1)#mode lacp-static
2. Add interfaces 1 to 3 to the aggregation group
Switch(config)#interface 10gigaethernet 1/0/1 to 10gigaethernet 1/0/3
Switch(config-10ge1/0/1->xge1/0/3)#no shutdown
Switch(config-10ge1/0/1->xge1/0/3)#join eth-trunk 1
3. After configuration is complete, view the aggregation group information.
Switch#show lacp eth-trunk 1
eth-trunk 1:
        LACP Status: master       Port number: 3

gigaethernet-1/0/1
  Port Status: Up and bind
  Flag: S – Device is sending Slow LACPDUs
        F – Device is sending fast LACPDUs
  Local information:
        Mode        Flags    Priority   AdminKey   OperKey    PortId   State
```

```
            active      F          32768       0x19        0x19        0x1        0xa9d7f8
    Partner's information:
            Port                   Flags    SysPri     PortPri    AdminKey   OperKey
OperPort OperState DevID
            1                      F         32768       32768       0x0         0x19        0x1
0x9dfb6c   0x00046798185d

  gigaethernet-1/0/2
    Port Status: Up and bind
    Flag: S – Device is sending Slow LACPDUs
           F – Device is sending fast LACPDUs
    Local information:
            Mode        Flags     Priority   AdminKey   OperKey    PortId   State
            active      F          32768       0x19        0x19        0x2        0xa9d7f8
    Partner's information:
            Port                   Flags    SysPri     PortPri    AdminKey   OperKey
OperPort OperState DevID
            2                      F         32768       32768       0x0         0x19        0x2
0x9dfb6c   0x00046798185d

  gigaethernet-1/0/3
    Port Status: Up and bind
    Flag: S – Device is sending Slow LACPDUs
           F – Device is sending fast LACPDUs
    Local information:
            Mode        Flags     Priority   AdminKey   OperKey    PortId   State
            active      F          32768       0x19        0x19        0x3        0xa9d7f8
    Partner's information:
            Port                   Flags    SysPri     PortPri    AdminKey   OperKey
OperPort OperState DevID
            3                      F         32768       32768       0x0         0x19        0x3
0x9dfb6c   0x00046798185d
```

5.5 VLAN Configuration

5.5.1 Overview of VLAN

Meaning of VLAN

A local area network (LAN) is logically divided into multiple subsets and each subset has its own broadcast domain called a virtual local area network (VLAN).

Briefly, VLAN sets the devices in a LAN into different network segments logically but not physically to implement broadcast domain isolation in the LAN.

VLAN Function

- VLAN isolates the broadcast domain, reduces broadcast storms, and enhances security.
- In a large network, VLAN can restrict network faults within itself and enhance network robustness.

5.5.2 Creating a VLAN

Purpose

This section describes how to create a VLAN and then configure other VLAN functions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a VLAN and access the VLAN view	1. Access the global configuration view. 2. Run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view.
Create and access the VLANIF interface configuration view	1. Access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to create and access the VLANIF interface configuration view.
Delete an existing VLANIF	1. Access the global configuration view. 2. Run the **no vlan** *vlan-id* command to delete the specified VLANIF interface configuration view.

Purpose	Procedure
Create a VLAN and access the VLAN view	1. Access the global configuration view. 2. Run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view.
Delete one VLAN or multiple VLANs in batches	1. Access the global configuration view. 2. Run the **no vlan** *vlan-id1* [*vlan-id2*] command to delete one VLAN or multiple VLANs in batches.
Switch the VLAN configuration view	1. Access the global configuration view. 2. Run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view. 3. Run the **switch vlan** *vlan-id* command in the VLAN configuration view to create other VLANs and access the corresponding VLAN configuration view.

5.5.3 Configuring an Interface-based VLAN

Purpose

This section describes how to configure an interface-based VLAN.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the default VLAN of an interface and add the interface to this VLAN	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port link-type** *type* command to set link-type to **access** or **dot1q-tunnnel**. 4. Run the **port default vlan** *vlan-id* command to configure the default VLAN of an interface and add the interface to this VLAN.
Configure the VLAN that a hybrid interface belongs to	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } command to configure the type of VLANs for the Hybrid port.
Configure the default VLAN of a hybrid interface	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port hybrid pvid** { *vlan-id* | **default** } command to configure the default VLAN of a hybrid interface.

Purpose	Procedure
Set the link type (also called interface type) for an interface	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port link-type** { **access** | **trunk** | **hybrid** | **default** } command to set the link type for an interface.
Configure the default VLAN of a Trunk interface	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port trunk pvid** { *vlan-id* | **default** } command to configure the default VLAN of a Trunk interface.
Add a Trunk interface to a VLAN	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port trunk allow-pass vlan all** command to add a Trunk interface to a VLAN.

5.5.4 Configuring Other Parameters of VLAN

Purpose

This section describes how to configure other parameters of VLAN. You can configure the parameters according to the actual condition.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the descriptive information of the VLANIF interface	1. Access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to create and access the VLANIF interface configuration view. 3. Run the **alias** *description* command to configure the descriptive information of the VLANIF interface.
Configure the descriptive information of a VLAN	1. Access the global configuration view. 2. Run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view. 3. Run the **alias** *description* command to configure the descriptive information of a VLAN.
Configure how a VLAN processes an unknown unicast packet before forwarding the packet	1. Access the global configuration view. 2. Run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view.

Purpose	Procedure
	3. Run the **unknown-unicast** { **forward** | **drop** } command to configure how a VLAN processes an unknown unicast packet before forwarding the packet.
Configure how a VLAN processes an unknown unicast packet before forwarding the packet	1. Access the global configuration view. 2. Run the following commands to configure how a VLAN processes an unknown unicast packet before forwarding the packet: ● **unknown-unicast vlan** *vlan-list* **{ forward | drop }** ● **vlan** *vlan-id* **unknown-unicast { forward | drop }**
Configure the load balancing mode for unknown unicast packets on a Trunk interface when the packets are forwarded by an aggregation port VLAN	1. Access the global configuration view. 2. Run the **unknown-unicast load-balance { dst-mac|src-mac|srcdst-mac|schedule-profile name |default }** command.
Set the VLAN type to common VLAN	1. Access the global configuration view. 2. Access the VLANIF interface configuration view or run the **vlan** *vlan-id1* [*vlan-id2*] command to create one or more VLANs and access the VLAN view. 3. Run the **vlan normal** command to set the VLAN type to common VLAN.
Configure the delay UP time for L3 interfaces	1. Access the Ethernet routing interface configuration view, VLAN interface configuration view, or BD interface configuration view. 2. Run the **protocol up-delay-time** { *time* | **default** } } command.

5.5.5 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the VLAN function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the configuration of the VLAN interface	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view.

Purpose	Procedure
	2. Run the **show interface vlan config** command to view the VLAN interface configuration.
View VLAN information	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, VLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the following commands to view VLAN information: ● **show vlan** ● **show vlan all** ● **show vlan all** *vlan-list* ● **show vlan property** ● **show vlan property** *vlan-list* ● **show vlan verbose** ● **show vlan** *vlan-id* **verbose**
View the reference count of a VLAN interface	1. Access the common user view. 2. Run the **show l3int vlan** *vlan-id* command.

5.5.6 Configuration Example

Network Requirements

In a company, the PCs of the R&D department and marketing department interconnect with the department servers using Switch Switch-1 and Switch Switch-2 respectively. It is required that the PCs of the R&D department access department server 1 and those of the marketing department access department server 2, but the communication between two departments be forbidden.

- Set two VLANs (VLAN 100 and VLAN 200) according to requirements, and set their descriptors to "Development100" and "Market200" respectively.
- Set the PCs of the R&D department and Server 1 to VLAN 100.
- Set the PCs of the marketing department and Server 2 to VLAN 200.

Network Diagram

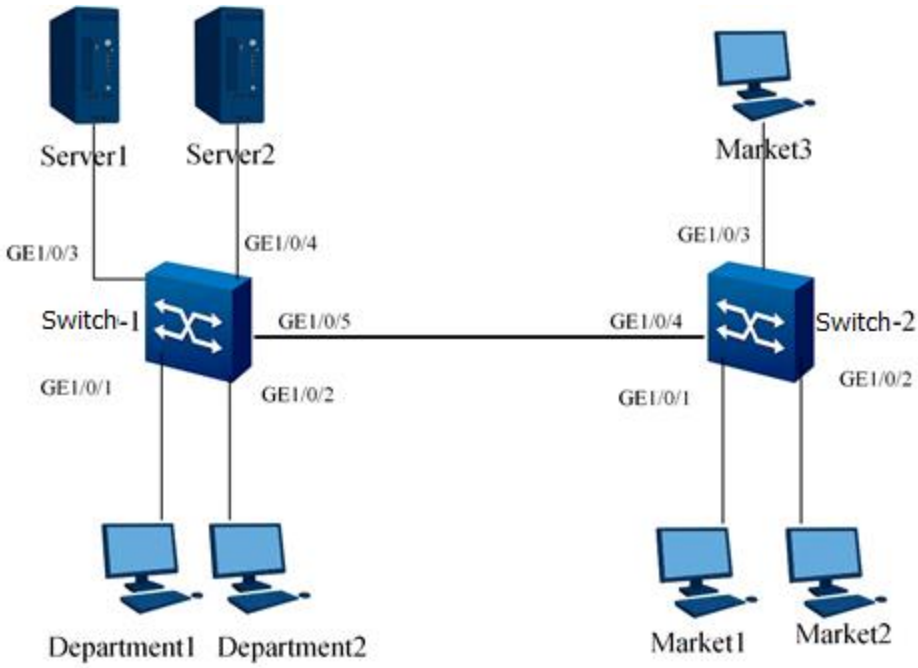


Figure 5-3 VLAN configuration topology

Configuration

1. Configure Switch-1.
Switch-1#configure
%Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Create VLAN 100 and access its configuration view.
Switch-1(config)#interface vlan 100
Switch-1(config-vlan-100)#
Describe VLAN 100 as Development100.
Switch-1(config-vlan-100)#description Development100
Add interfaces xgigaethernet1/0/1, xgigaethernet1/0/2, and xgigaethernet1/0/3 to VLAN 100, and configure VLAN 100 as the PVID of these interfaces.
Switch-1(config-vlan-100)#quit
Switch-1(config)#
Switch-1(config)#interface xgigaethernet 1/0/1
Switch-1(config-10ge1/0/1)#port hybrid vlan 100 untagged
Switch-1(config-10ge1/0/1)#port hybrid pvid 100
Switch-1(config-10ge1/0/1)#quit
Switch-1(config)#interface xgigaethernet 1/0/2
Switch-1(config-10ge1/0/2)#port hybrid vlan 100 untagged
Switch-1(config-10ge1/0/2)#port hybrid pvid 100
Switch-1(config-10ge1/0/2)#quit
Switch-1(config)#interface 10gigaethernet 1/0/3
Switch-1(config-ge1/0/3)#port hybrid vlan 100 untagged
Switch-1(config-ge1/0/3)#port hybrid pvid 100
Switch-1(config-ge1/0/3)#quit
Switch-1(config)#
Create VLAN 200 and access its configuration view.
Switch-1(config)#interface vlan 200
Switch-1(config-vlan-200)#

Describe VLAN 200 as Market200.
Switch-1(config-vlan-200)#description Market200
Add interfaces gigaethernet1/0/4 and gigaethernet1/0/5 to VLAN 100, and configure VLAN 200 as the PVID of these interfaces.
Switch-1(config-vlan-100)#quit
Switch-1(config)#
Switch-1(config)#interface 10gigaethernet 1/0/4
Switch-1(config-10ge1/0/4)#port hybrid vlan 200 untagged
Switch-1(config-10ge1/0/4#port hybrid pvid 200
Switch-1(config-10ge1/0/4)#quit
Switch-1(config)#interface 10gigaethernet 1/0/5
Switch-1(config-10ge1/0/5)#port hybrid vlan 200 tagged
Switch-1(config-10ge1/0/5)#port hybrid pvid 200
Switch-1(config-10ge1/0/5)#quit

2. Configure Switch-2.
Create VLAN 200 and access its configuration view.
Switch-2#configure
%Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Switch-2(config)#interface vlan 200
Describe VLAN 200 as Market200.
Switch-2(config-vlan-200)#description Market200
Add interfaces 10gigaethernet1/0/1, 10gigaethernet1/0/2, 10gigaethernet1/0/3, and 10gigaethernet1/0/4 to VLAN 100, and set the PVIDs of 10gigaethernet1/0/1, 10gigaethernet1/0/2, and 10gigaethernet1/0/3 to VLAN 100.
Switch-2(config-vlan-100)#quit
Switch-2(config)#
Switch-2(config)#interface 10gigaethernet 1/0/1
Switch-2(config-10ge1/0/1)#port hybrid vlan 200 untagged
Switch-2(config-10ge1/0/1)#port hybrid pvid 200
Switch-2(config-10ge1/0/1)#quit
Switch-2(config)#interface 10gigaethernet 1/0/2
Switch-2(config-10ge1/0/2)#port hybrid vlan 200 untagged
Switch-2(config-10ge1/0/2)#port hybrid pvid 200
Switch-2(config-10ge1/0/2)#quit
Switch-2(config)#interface 10gigaethernet 1/0/3
Switch-2(config-10ge1/0/3)#port hybrid vlan 200 untagged
Switch-2(config-10ge1/0/3)#port hybrid pvid 200
Switch-2(config-10ge1/0/3)#quit
Switch-2(config)#interface 10gigaethernet 1/0/4
Switch-2(config-10ge1/0/4)#port hybrid vlan 200 tagged
Switch-2(config-10ge1/0/4)#quit
Switch-2(config)#

5.6 VLAN Mapping Configuration

5.6.1 Overview of VLAN Mapping

VLAN mapping replaces the inner and outer VLAN tags in data frames to implement mapping between user VLAN and carrier VLAN. Based on VLAN tag replacement, the VLAN aggregation function enables transmission of user services according to the carrier's network planning.

VLAN mapping is directly configured on ports, which is different from the configuration of the old VLAN translation module, whereby a VLAN translation entry is created and then bound to a port. VLAN mapping only allows modifying VLAN tags, but not adding or deleting VLAN tags.

VLAN mapping supports the following basic functions:

- Matching outer VIDs and modifying outer tags
- Matching outer VID ranges and modifying outer tags
- Matching outer and inner VIDs and modifying inner and outer tags
- Matching outer and inner VIDs and modifying outer tags
- Matching outer priorities and modifying outer tags
- Matching outer VIDs and priorities and modifying outer tags
- Matching outer VID ranges and priorities and modifying outer tags
- Matching inner VIDs and modifying inner tags

5.6.2 Configuring VLAN Mapping

Purpose

This section describes how to configure VLAN mapping.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the 1:1 VLAN forwarding entry and match the outer VLAN ID in the packet to modify the outer VLAN ID and priority of the forwarded packet	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view.

Purpose	Procedure
	3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-mapping vlan** *outside-vlan-id* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** outside-vlan-id **map-vlan** *outside-mapping-vlan-id* **remark-8021p** priority
Configure the N:1 VLAN conversion entry (In N:1 mode, multiple user-side VLAN IDs within the specified range are mapped to a network-side VLAN ID; the VLAN ID in the packet is matched to modify the outer VLAN ID and priority of the forwarded packet.)	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-mapping vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*
Configure the single VLAN data frame transmitted via the port with the port's L2 VLAN tag to form a double-layer tag, and match the outer VLAN ID of the packet to add the outer VLAN ID and priority to the forwarded packet	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-stacking vlan** *stacking-vlan-id* **stack-vlan** *stacking-mapping-vlan-id* ● **vlan-stacking vlan** *stacking-vlan-id* **stack-vlan** *stacking-mapping-vlan-id* **remark-8021p** *priority*
Configure the N:1 VLAN data frame transmitted via the port with the port's	1. Run the **configure** command to access the global configuration view.

Purpose	Procedure
L2 VLAN tag (In N:1 mode, multiple VLAN tags are mapped to the port's outer VLAN tag to form a double-layer tag, and the outer VLAN ID of the packet is matched to add the outer VLAN ID and priority to the forwarded packet.)	2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-stacking vlan** *stacking-vlan-id1* **to** *stacking-vlan-id2* **stack-vlan** *stacking-mapping-vlan-id* ● **vlan-stacking vlan** *stacking-vlan-id1* **to** *stacking-vlan-id2* **stack-vlan** *stacking-mapping-vlan-id* **remark-8021p** *priority*
Match the outer and inner VLAN IDs in the packet to modify the outer VLAN ID and priority of the forwarded packet, and match the outer VLAN ID in the packet to modify the outer VLAN ID and priority of the forwarded packet	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*
Match the outer VLAN ID and N:1 inner VLAN ID in the packet to modify the outer VLAN ID and priority of the forwarded packet (In N:1 mode, multiple inner VLAN IDs are mapped to the port's outer VLAN tag; the inner and outer VLAN IDs in the packet are matched to modify the outer VLAN ID and priority of the forwarded packet.)	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands:

Purpose	Procedure
	● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id1* **to** *inner-vlan-id 2* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id1* **to** *inner-vlan-id 2* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*
Map inner and outer VLAN IDs to the specified VLAN ID of the new single-layer tag	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the command **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-single-vlan** *map-single-vlan*.
Delete all the configured VLAN conversion entries	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **no vlan-mapping all** command.
Delete the designated VLAN conversion entry	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the following commands: ● **no vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id* ● **no vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner--mapping-vlan-id1* **to** *inner--mapping-vlan-id2*

Purpose	Procedure
	● **no vlan-mapping vlan** *outside-vlan-id* **to** *outside-mapping-vlan-id*
Configure the action of replacing the packet VLAN ID in the flow action	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the **vlan-mapping enable** command to enable VLAN mapping. 4. Run the following commands: ● **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* ● **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority* ● **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-inner-vlan** *inner-mapping-vlan-id* ● **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-inner-vlan** *inner-mapping-vlan-id* **remark-8021p** *priority*
Match the outer and inner VIDs to modify the outer and inner tags and priorities of the forwarded packet	1. Run the **configure** command to access the global configuration view. 2. Run the **interface { gigaethernet | xgigaethernet }** *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view or interface group configuration view. 3. Run the following commands: ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *inner-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *inner-mapping-vlan-id* **remark-8021p** *priority*

5.6.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the VLAN mapping function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable VLAN mapping debugging	1. Remain in the current privileged user view. 2. Run the **debug vlan-mapping** command.
Disable VLAN mapping debugging	1. Remain in the current privileged user view. 2. Run the **no debug vlan-mapping** command.
Display VLAN mapping information, including configuration and interface information	1. Run the corresponding command to access the common user view, privileged user view, global configuration view, or interface configuration view (Ethernet). 2. Run the following commands: ● **show vlan-mapping** ● **show vlan-mapping config** ● **show vlan-mapping interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*

5.6.4 Configuration Example

Network Diagram

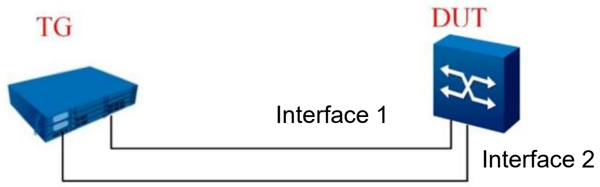


Figure 5-4 VLAN mapping configuration topology

Configuration

Example of configuration:

1. Add Interface 1 and Interface 2 to VLAN 100 and VLAN 200 in tag mode.

2. Configure a QinQ entry on Interface 1.

3. Capture packets on the interfaces to view the VLAN translation results and determine whether the QinQ entry is effective.

5.7 QinQ Configuration

802.1Q-in-802.1Q (QinQ) indicates encapsulating the VLAN tag of a user private network into the public network VLAN tag so that the packets contain two layers of VLAN tags to be transmitted in the backbone network (public network) of the carrier. The packet in the public network is transmitted only according to the outer VLAN tag (public VLAN Tag), and the private VLAN tag of users is filtered.
QinQ addresses the following problems:

- Solves the VLAN ID resource shortage of public network.
- Allows users to set their own private VLAN IDs to prevent conflict with the public network VLAN ID.
- Provides a simple L2 VPN solution for small-scale metropolitan area networks (MANs) or enterprise networks.

5.7.1 Overview of QinQ

QinQ is an L2 tunnel protocol based on the IEEE 802.1Q technology. The name QinQ is derived from the fact that a frame transmitted in the public network contains two 802.1Q tags: a public tag and a private tag.
The core concept of QinQ is to encapsulate the private VLAN tag in the public VLAN tag so that the packet with two tags can be transmitted in the network carrier's backbone network, thus providing a simple L2 VPN tunnel.
QinQ is directly configured on ports, which is different from the configuration of the old VLAN translation module, whereby a VLAN translation entry is created and then bound to a port. QinQ only allows adding VLAN tags, but not modifying or deleting VLAN tags.

5.7.2 Configuring Flexible QinQ for a Single VLAN or a Batch of VLANs

Purpose

This section describes how to configure flexible QinQ for a single VLAN or a batch of VLANs.

When a packet in this VLAN needs to traverse the carrier's network, you can use this command to add a VLAN tag to the packet to form a dual-layer VLAN.

When enabling flexible QinQ, pay attention to the following points:

- The interface must be a hybrid interface and is valid only in the inbound direction.

The stacked outer VLAN must exist, and the current interface must be added to the stack VLAN in untagged mode.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure flexible QinQ for a single VLAN or a batch of VLANs	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the interface configuration view (Ethernet or Trunk). 3. Run the following commands: ● **vlan-stacking vlan** *vlan-id1* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id1* **8021p** *priority* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority* **stack-vlan** *vlan-id2*
Configure flexible QinQ based on 802.1p priority and a single VLAN ID or a batch of VLAN IDs	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the interface configuration view (Ethernet or Trunk). 3. Run the following commands: ● **vlan-stacking vlan** *vlan-id1* **stack-vlan** *vlan-id2* **remark-8021p** *priority* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **stack-vlan** ***vlan-id2*** **remark-8021p** *priority* ● **vlan-stacking vlan** *vlan-id1* **8021p** *priority* **stack-vlan** *vlan-id2* **remark-8021p** *priority* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority* **stack-vlan** *vlan-id2* **remark-8021p** *priority*

Delete the configured flexible QinQ	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the interface configuration view (Ethernet or Trunk). 3. Run the following commands: ● **no vlan-stacking all** ● **no vlan-stacking vlan** *vlan-id1* ● **no vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* ● **no vlan-stacking vlan** *vlan-id1* **8021p** *priority* ● **no vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority*

5.7.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the QinQ function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable debugging of the flexible QinQ module	1. Remain in the current privileged user view. 2. Run the **debug vlan-stacking** command.
Disable debugging of the flexible QinQ module	1. Remain in the current privileged user view. 2. Run the **no debug vlan-stacking** command.
Display information about flexible QinQ	1. Run the corresponding command to access the common user view, privileged user view, global configuration view, or interface configuration view (Ethernet or Trunk). 2. Run the following commands: ● **show vlan-stacking** ● **show vlan-stacking config interface** ● **show vlan-stacking config interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show vlan-stacking interface** ● **show vlan-stacking interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*

5.7.4 Configuration Example

Network Diagram

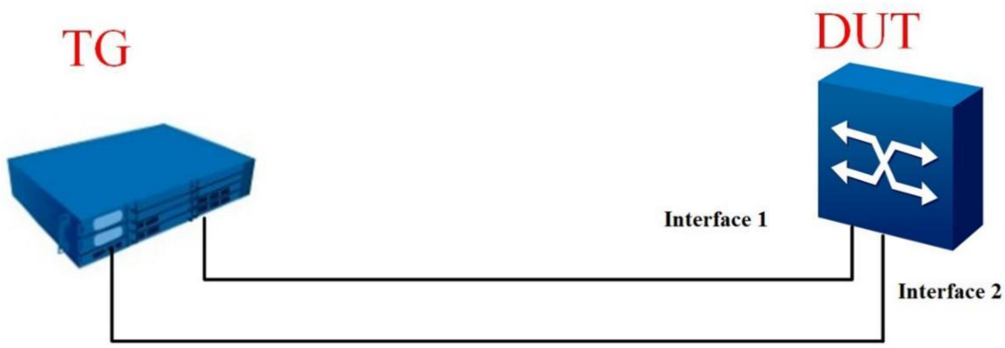


Figure 5-5 QinQ configuration topology

Configuration

Example of configuration:

1. Add Interface 1 and Interface 2 to VLAN 100 and VLAN 200 in tag mode.
2. Configure a QinQ entry on Interface 1.
3. Capture packets on the interfaces to view the VLAN translation results and determine whether the QinQ entry is effective.

5.8 Configuring an ARP Proxy

5.8.1 Introduction to ARP Proxy

ARP proxy includes routed ARP proxy, intra-VLAN ARP proxy, inter-VLAN ARP proxy, and protocol-based ARP proxy.

Routed ARP Proxy

Routed ARP proxy enables communication among PCs or switches in the same network segment but on different physical networks. If the default gateway address (the route from the intermediate system to the current system) is not configured for the current host of a switch, data cannot be forwarded. Routed ARP proxy can solve this problem as follows: the host sends an ARP request (to get the MAC address of the destination); after receiving the request, the switch for which ARP proxy is enabled returns its MAC address as a response to the ARP request and cheat the host to forward data. The switch for which ARP proxy is enabled can hide details of physical networks so that inner hosts of Ethernet A and Ethernet B on different physical networks but in the same network segment can communicate with each other.

Intra-VLAN ARP Proxy

If two users in the same VLAN configured with user isolation want to communicate with each other, intra-VLAN ARP proxy must be enabled for interfaces associated with this VLAN. If intra-VLAN ARP proxy is enabled for a switch interface, after the interface receives an ARP request packet in which the destination address is not the interface address, the switch searches for the ARP entry of this interface instead of discarding the packet immediately. If the proxy conditions are met, the switch sends its MAC address to the ARP request sender. Intra-VLAN ARP proxy is used for communication between users in a VLAN configured with user isolation.

Inter-VLAN ARP Proxy

If two users in the same Super VLAN but different Sub VLANs want to communicate with each other, inter-VLAN ARP proxy must be enabled for interfaces associated with these VLANs. If inter-VLAN ARP proxy is enabled for a switch interface, after the interface receives an ARP request packet in which the destination address is not the interface address, the switch searches for the ARP entry of this interface instead of discarding the packet immediately. If the proxy conditions are met, the switch sends its MAC address to the ARP request sender.

Inter-VLAN ARP proxy is used to enable inter-VLAN ARP proxy for VLANIF interface of a Super VLAN and then allow communication between users of different Sub VLANs.

Protocol-based ARP Proxy

The ARP proxy module provides an array of protocol binding structures. The protocol needing proxy adds the IP and MAC addresses of the proxy to the array. When the ARP module receives an ARP request from the local machine, it calls the callback function registered by the ARP proxy to find the protocol binding array. If there is a corresponding entry, the corresponding MAC address in the entry is used as the source MAC address of the ARP response.

5.8.2 Configuring an ARP Proxy

Purpose

This section describes how to configure an ARP proxy.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Disable the routed ARP proxy function on a VLAN interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **arp-proxy** { **enable** | **disable** } command.

5.8.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the ARP proxy function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display the ARP proxy configuration	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface

Purpose	Procedure
	configuration view, or remain in the current privileged user view, or access the VLANIF configuration view or sub-interface configuration view. 2. Run the show arp-proxy config command.
Display the interface information of the ARP proxy	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view, or remain in the current privileged user view, or access the VLANIF configuration view or sub-interface configuration view. 2. Run the **show arp-proxy interface** command.
the ARP proxy configuration in VLANs	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view, or remain in the current privileged user view, or access the VLANIF configuration view or sub-interface configuration view. 2. Run the **show arp-proxy vlan** command.
Enable or disable synchronous debugging of ARP proxy	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command or **interface eth-trunk** *trunk-number* command to access the interface configuration view, or remain in the current privileged user view, or access the VLANIF configuration view or sub-interface configuration view. 2. Run the **debug arp-proxy** command or the **no debug arp-proxy** command.

5.8.4 Configuration Example

Network Requirements

Configure a routed ARP proxy as shown in Figure 5-6. Connect 10GE 1/1 and 10GE 1/2 of Switch A to two hosts in the same network segment 172.16.0.0/16, respectively. No default gateway is configured for Host A and Host B. Enable routed ARP proxy for the switch so that hosts on different physical networks can communicate with each other.

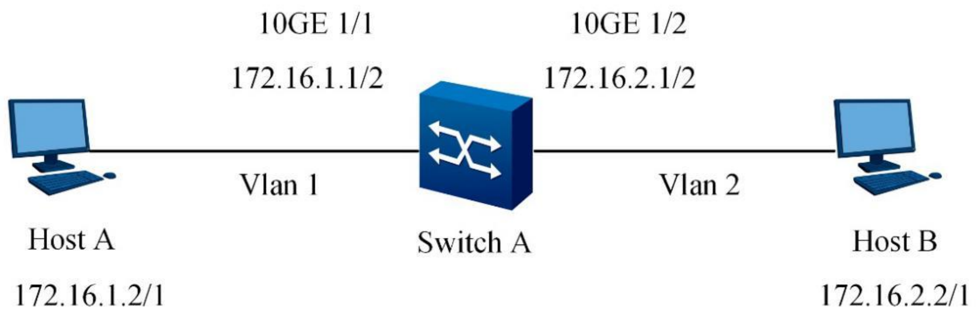


Figure 5-6 Network diagram of configuring routed ARP proxy

Configuration Suggestion

Configure a routed ARP proxy as follows:

(1) Configure the IP address of an interface

(2) Enable routed ARP proxy for the interface

Data Preparation

To perform the configuration, prepare the following data:

- IP address of the VLAN interface
- IP addresses of the hosts

Configuration

(1) Create VLAN 1, configure its IP address, and add GE 1/0/1 to VLAN 1

Switch(config)#interface vlan 1

Switch(config-vlan-1)#ip address 172.16.1.1/24

Switch(config-vlan-1)#no shutdown

Switch(config)#interface xgigaethernet 1/0/1

Switch(config-10ge1/0/1)#join vlan 1 untagged

Switch(config-10ge1/0/1)#pvid 1

Switch(config-10ge1/0/1)#no shutdown

Switch(config-10ge1/0/1)#quit
(2) Enable routed ARP proxy for VLAN 1
Switch(config)#interface vlan 1
Switch(config-vlan-1)#arp-proxy enable
Switch(config-vlan-1)# quit
(3) Create VLAN 2, configure its IP address, and add GE 1/0/2 to VLAN 2
Switch(config)#interface vlan 2
Switch(config-vlan-2)#ip address 172.16.2.1/24
Switch(config-vlan-2)#no shutdown
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#join vlan 2 untagged
Switch(config-10ge1/0/2)#pvid 2
Switch(config-10ge1/0/2)#no shutdown
Switch(config- ge1/0/2)#quit
(4) Enable routed ARP proxy for VLAN 2
Switch(config)#interface vlan 2
Switch(config-vlan-2)#arp-proxy enable
Switch(config-vlan-2)# quit
(5) Configure hosts
Set the IP address of Host A to 172.16.1.2/16.
Set the IP address of Host B to 172.16.2.2/16.
(6) Verify the configuration results
Check whether Host A can ping Host B.
Check whether the MAC address of Host B in the ARP entry of Host A is the MAC address of GE 1/0/1 of the switch.

5.9 Configuring Port Security

5.9.1.1 Enabling or Disabling Port Security

Purpose

This section describes how to enable or disable port security. After the port security function is enabled on an interface, MAC addresses learned on this interface are saved as secure dynamic MAC addresses, which will not be aged out. These secure dynamic MAC addresses will be lost after a reboot of the switch and need to be learned again.

Other configurations related to port security, such as the protection action, secure MAC address learning limit, and sticky MAC addresses, can be performed only after port security is enabled.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable port security	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the **port-security** { **enable** | **disable** } command.

5.9.1.2 Enabling or Disabling Sticky-mac for an Interface

Purpose

This section describes how to enable or disable sticky-mac for an interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable sticky-mac for an interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the **port-security enable** command. 4. Run the **port-security mac-address sticky { enable | disable }** command.

5.9.1.3 Manually Adding a Secure MAC Address

Purpose

This section describes how to add or delete a secure MAC address manually.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Manually add a secure MAC address	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the **port-security mac-address sticky enable** command. 4. Run the **port-security mac-address sticky** *vlan-id mac-address* command.
Manually delete a secure MAC address	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the following commands: ● **no port-security mac-address sticky** ● **no port-security mac-address sticky vlan** *vlan-id* ● **no port-security mac-address sticky vlan** *vlan-id mac-address*

5.9.1.4 Configuring the Maximum Number of Secure MAC Addresses Learned by an Interface

Purpose

This section describes how to set the maximum number of secure MAC addresses learned by an interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the maximum number of secure MAC addresses learned by an interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the **port-security enable** command. 4. Run the **port-security maximum** { *max-value* | **default** } command.

5.9.1.5 Configuring Protection Action for the Port Security Function

Purpose

This section describes how to configure a protection action for the port security function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure Protection Action for the Port Security Function	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** *interface-type interface-number* command to access the configuration view of an interface or interface group configuration view. 3. Run the **port-security enable** command. 4. Run the **port-security protect-action { protect | restrict | shutdown }** command.

5.10 Configuring Port Isolation

5.10.1 Port Isolation Overview

To enable L2 isolation among packets, users can add different ports to different VLANs but this may waste the limited VLAN resources. The port isolation function can isolate ports in the same VLAN. Users only need to add ports to an isolation group to isolate L2 data among ports in the isolation group. The port isolation function provides safer and more flexible networking solutions for users.

5.10.2 Configuring Port Isolation

Purpose

The port isolation function can isolate ports in the same VLAN and thus provide safer and more flexible networking solutions for users.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure unidirectional port isolation	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk). 3. Run the following commands: ● **port-uniisolate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **port-uniisolate interface eth-trunk** *trunk-number* ● **no port-uniisolate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no port-uniisolate interface eth-trunk** *trunk-number*
Configure L2 or L3 port isolation	1. Access the global configuration view. 2. Run the **port-isolate mode** { **l2** | **all** } command.
Create a port isolation group	1. Access the global configuration view. 2. Run the **port-isolate group** *group-number* command.
Add an interface to an isolation group	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the following commands:

Purpose	Procedure
	● **join port-isolate group** *group-id* ● **join port-isolate group** *group-list*
Delete an interface from an isolation group	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the following commands: ● **no join port-isolate group** *group-id* ● **no join port-isolate group** *group-list* ● **no join port-isolate group all**
Add a port to an isolation group	1. Access the global configuration view. 2. Run the **port-isolate group** *group-number* command. 3. Run the following commands: ● **add interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **add interface eth-trunk** *trunk-number*
Delete a port from an isolation group	1. Access the global configuration view. 2. Run the **port-isolate group** *group-number* command. 3. Run the following commands: ● **no interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no interface eth-trunk** *trunk-number*

5.10.3 Maintaining Port Isolation

Purpose

This section describes how to check or locate the fault when the port isolation function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View information about all or specified port isolation groups	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show port-isolate group** ● **show port-isolate group** *group-number*
View the configuration of unidirectional port isolation	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the following commands: ● **show port-uniisolate interface** ● **show port-uniisolate interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show port-uniisolate interface eth-trunk** *trunk-number*
View information about all port isolation groups	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show port-isolate information** command.
View the isolation group configuration as a configuration file	1. Access the privileged user view, global configuration view, common user view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show port-isolate config** command.

5.11 Configuring MLAG

5.11.1 Introduction to MLAG

In a data center scenario, to provide redundancy, each set-top switch is connected to two aggregated switches. To avoid looping, half of the uplinks are blocked by spanning tree, thus reducing the available bandwidth between the aggregation layer and the rack by 50%.

There is bandwidth waste in data center networks. Enterprise networks tolerate this waste of bandwidth because the applications are not bandwidth-sensitive. However, with the development of technology, such as rich media applications, inexpensive computer servers, and increasing bandwidth requirements, the problem of insufficient network bandwidth in data centers is obvious. MLAG can solve this bandwidth bottleneck and make full use of bandwidth in a network.

Data centers and high-performance cloud computing networks have higher requirements for network reliability. MLAG logically aggregates ports of two switches together, providing system-level redundancy and network-level elasticity compared to extending link aggregation to a pair of data center switches.

Main advantages of MLAG:

- Allows users to design a network without blocking links
- Improves bandwidth usage efficiency
- Provides network-level elasticity design and system-level redundancy
- Connects to MLAG switches without requiring additional proprietary protocol. Required only IEEE 802.3ad LACP support

5.11.2 Configuring an MLAG Group and System Parameters

Purpose

This section describes how to enable an MLAG group and configure MLAG system parameters.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create or delete an MLAG group	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to create an MLAG group or run the **no mlag-group** *mlag-group* command to delete an MLAG group.

Purpose	Procedure
Configure an LACP MLAG system ID	1. Access the global configuration view. 2. Run the **lacp mlag system-id** *mac-address* command.
Configure LACP MLAG system priority	1. Access the global configuration view. 2. Run the **lacp mlag priority** { *priority-value* | **default** } command.
Configure a reserved MLAG interface when an active-active detection conflict occurs	1. Access the global configuration view. 2. Run the following commands: ● **mlag exclude interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **mlag exclude interface eth-trunk** *trunk-number*。
Delete the configured reserved MLAG interface	1. Access the global configuration view. 2. Run the following commands: ● **no mlag exclude interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no mlag exclude interface eth-trunk** *trunk-number*

5.11.3 Configuring MLAG View Parameters

Purpose

Configure MLAG view parameters

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an Eth-Trunk interface for an MLAG member aggregation group	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **mlag** *mlag-member* **interface eth-trunk** *trunk-number* command.
Delete the configured MLAG member aggregation group	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **no mlag** *mlag-member* command.

Purpose	Procedure
Configure an Eth-Trunk interface as a peer-link interface	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **peerlink interface eth-trunk** *trunk-number* command.
Cancel the configuration of configuring an Eth-Trunk interface as a peer-link interface	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **no peerlink interface** command.
Set a list of VLANs through which MLAG links cannot pass	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **peerlink exclude vlan** *vlan-list* command.
Delete the configured list of VLANs through which MLAG links cannot pass	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **no peerlink exclude vlan** *vlan-list* command.
Configure the MLAG priority	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **priority** { *priority-value* | **default** } command.
Configure or delete a security password	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **security-key** { **simple** | **md5** } { **plain** | **cipher** } *key* command to configure a security password or run the **no security-key** command to delete the security password.
Configure detecting the local IPv4 or IPv6 address and VPN instance in active-active mode	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the following commands: ● **source-address** *ipv4-address* ● **source-address** *ipv4-address* **peer-address** *peer-ipv4-address* ● **source-address** *ipv4-address* **vpn-instance** *name* ● **source-address** *ipv4-address* **vpn-instance** *name* **peer-address** *peer-ipv4-address* ● **source-address** *ipv6-address* ● **source-address** *ipv6-address* **peer-address** *peer-ipv6-address*

Purpose	Procedure
	● **source-address** *ipv6-address* **vpn-instance** *name* ● **source-address** *ipv6-address* **vpn-instance** *name* **peer-address** *peer-ipv6-address* ● **no source-address**
Configure a sending interval timer of Hello packets	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **timer hello** { *hello-interval* | **default** } command.
Configure a multiplier timer for Hello packet sending interval	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **timer hold-on-failure multiplier {** *value* | **default }** command.
Configure a delay time for an MLAG member interface to report the UP state	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **up-delay** { *delay-value* | **default** } [**auto-recovery interval** { *interval-value* | **default** }] command.
Enable or disable the DAD enhancing function in MLAG mode	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **dad enhance { enable | disable }** command.

5.11.4 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the MLAG function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable MLAG debugging	1. Remain in the current privileged user view. 2. Run the **debug mlag { in | out | timer | notify | global | if | packet | error | all }** command.
Disable MLAG debugging	1. Remain in the current privileged user view. 2. Run the **no debug mlag { in | out | timer | notify | global | if | packet | error | all }** command.
Clear the MLAG counter	1. Access the global configuration view. 2. Run the **mlag-group** *mlag-group* command to access the MLAG configuration view. 3. Run the **reset counter** command.
View MLAG system information	1. Run the **disable** command to return to the common user view. 2. Run the **show mlag** command.
View the MLAG configuration file information	1. Run the **disable** command to return to the common user view. 2. Run the **show mlag config** command.
View MLAG configuration consistency.	1. Run the **disable** command to return to the common user view. 2. Run the s**how mlag consistency** command.
View the MLAG reserved interface information	1. Run the **disable** command to return to the common user view. 2. Run the **show mlag exclude interface** command.
View MLAG information	1. Run the **disable** command to return to the common user view. 2. Run the **show mlag-group** *mlag-group* command.

5.11.5 Configuration Example

5.11.5.1 Typical L2 MLAG Case

Network Requirements

SW1 and SW2 are downlink switches, and the master and slave switches are members of the MLAG domain and run MLAG. The numbers at both ends of the link represent port numbers. The peer addresses of the master and slave switches are **192.168.1.1** and **192.168.1.2,** respectively. The administrator ensures that these addresses are reachable.

Network Diagram

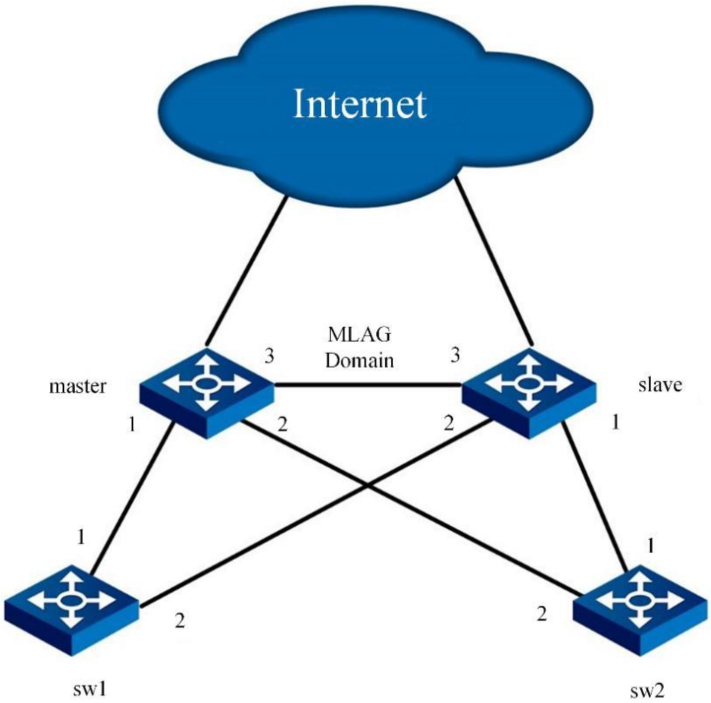


Figure 5-7 Network diagram of a typical L2 MLAG

Configuration

1. Configure SW1 and SW2

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2

2. Configure the switch Master

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 100

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.1 peer-address 192.168.1.2

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

3. Configure the switch Slave

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 200

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.2 peer-address 192.168.1.1

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

Switch(config)#lacp mlag system-id 00:00:00:01:02:03 (configure the MAC address of the master switch on the slave switch)

5.11.5.2 Typical L3 MLAG Case

Network Requirements

SW1 and SW2 are downlink switches, and the master and slave switches are members of the MLAG domain and run MLAG. The numbers at both ends of the link represent port numbers. The peer addresses of the master and slave switches are **192.168.1.1** and **192.168.1.2,** respectively. The administrator ensures that these addresses are reachable.

The MLAG switches are the gateways of the downlink switches **10.0.0.100** and **10.0.1.100**. The gateway addresses are **100.0.0.1** and **100.0.1.1**, respectively.

Network Diagram

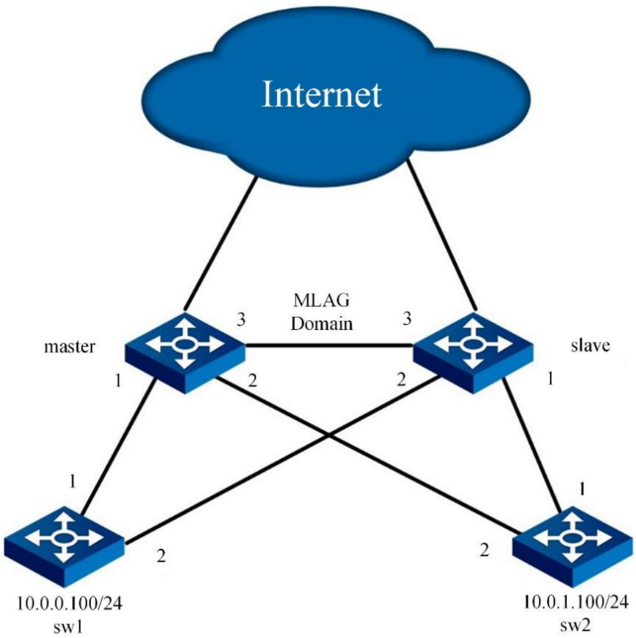


Figure 5-8 Network diagram of a typical L3 MLAG

Configuration

1. Configure SW1 and SW2

```
Switch(config)#interface eth-trunk 1
Switch(config-eth-trunk1)#mode lacp-static
Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1
Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2
```

2. Configure the switch Master

```
Switch(config)#vlan 10,20
Switch(config)#interface vlan 10
Switch(config-vlanif-10)#ip address 100.0.0.1
Switch(config-vlanif-10)#exit
Switch(config)#interface vlan 20
Switch(config-vlanif-10)#ip address 100.0.1.1
Switch(config-vlanif-10)#exit
Switch(config)#interface eth-trunk 1
Switch(config-eth-trunk1)#mode lacp-static
Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1
Switch(config-eth-trunk1)#port link-type access
Switch(config-eth-trunk1)#port default vlan 10
Switch(config-eth-trunk1)#exit
Switch(config)#interface eth-trunk 2
Switch(config-eth-trunk2)#mode lacp-static
Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2
Switch(config-eth-trunk2)#port link-type access
Switch(config-eth-trunk2)#port default vlan 20
Switch(config-eth-trunk2)#exit
Switch(config)#interface eth-trunk 3
Switch(config-eth-trunk3)#mode lacp-static
Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3
Switch(config-eth-trunk3)#exit
Switch(config)#mlag-group 1
Switch(config-mlag-1)#priority 100
Switch(config-mlag-1)#peerlink interface eth-trunk 3
Switch(config-mlag-1)#mlag 1 interface eth-trunk 1
Switch(config-mlag-1)#mlag 2 interface eth-trunk 2
Switch(config-mlag-1)#source-address 192.168.1.1 peer-address 192.168.1.2
Switch(config-mlag-1)#dad enhance enable
```

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

3. Configure the switch Slave

Switch(config)#vlan 10,20

Switch(config)#interface vlan 10

Switch(config-vlanif-10)#ip address 100.0.0.1

Switch(config-vlanif-10)#exit

Switch(config)#interface vlan 20

Switch(config-vlanif-10)#ip address 100.0.1.1

Switch(config-vlanif-10)#exit

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#port link-type access

Switch(config-eth-trunk1)#port default vlan 10

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk2)#port link-type access

Switch(config-eth-trunk2)#port default vlan 20

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 200

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.2 peer-address 192.168.1.1

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

Switch(config)#lacp mlag system-id 00:00:00:01:02:03 (configure the MAC address of the master switch on the slave switch)

Chapter 6 IP Service Configuration

This chapter describes IP services of the Switch.

6.1 Configuring IPv4

6.1.1 Configuring In-band, Out-of-band, and Loopback IP Addresses

Purpose

This section describes how to configure in-band, out-of-band, and loopback IP addresses.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure in-band, out-of-band, and loopback IP addresses	Configure an in-band IP address: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands to configure an in-band IP address: ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address* Configure an out-of-band IP address: 1. Access the global configuration view. 2. Access the out-of-band interface configuration view. 3. Run the following commands to configure an out-of-band IP address: ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address* Configure a loopback IP addresses: 1. Access the global configuration view. 2. Access the loopback interface configuration view. 3. Run the following commands: ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*
Delete in-band, out-of-band, and loopback IP addresses of a device	1. Access the global configuration view. 2. Access the VLANIF configuration view, out-of-bind interface configuration view, Tunnel interface configuration view, or loopback interface configuration view 3. Run the **no ip address** *ip-address* command.

6.1.2 Configuration Commands of Interface IP Address

Purpose

This section describes configuration commands of interface IP address.

The operation sets the IP address and the mask address of the interface on the device to implement interconnection in the network. To enable an interface to connect to multiple subnets, you can configure multiple IP addresses for the interface, where one IP address functions as a primary IP address and other IP addresses function as secondary IP addresses. If the interface already has a primary IP address, when you configure a primary IP address for the interface, its original primary IP address is deleted, and the new one takes effect. Before deleting the primary IP address, you must delete all secondary IP addresses.

All IP addresses configured for each interface cannot be in the same subnet.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an IP address for a VLANIF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 3. Run the following commands: ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*
Delete all the IP addresses or the designated IP address of a VLANIF interface	1. Access the global configuration view. 2. Run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 3. Run the following commands: ● **no ip address** *ip-address* ● **no ip address**
Configure the MTU value for an IPv4 interface	1. Access the global configuration view. 2. Access the Tunnel interface configuration view. 3. Run the **mtu** *mtu-value* command.
Configure strict L3 IP forwarding	1. Access the global configuration view. 2. Run the **ip forward-strict { enable | disable }** command.
Configure an IPv4 prefix list	1. Access the global configuration view. 2. Run the following commands: ● **ip prefix-list** *listname* { **deny | permit** } *ipv4-address/mask-length* ● **ip prefix-list** *listname* { **deny | permit }** *ipv4-address/mask-length* { **greater-equal | less-equal** } *prefix-length*

Purpose	Procedure
	● **ip prefix-list** *listname* { **deny | permit** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix length* ● **ip prefix-list** *listname* **index** *index-numbe*r { **deny | permit** } *ipv4-address/mask-length* ● **ip prefix-list** *listname* **index** *index-number* { **deny | permit** } *ipv4-address/mask-length* { **greater-equal | less-equal** } *prefix-length* ● **ip prefix-list** *listname* **index** *index-number* { **deny | permit** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*
Cancel the configured IPv4 prefix list	1. Access the global configuration view. 2. Run the following commands: ● **no ip prefix-list** *listname* ● **no ip prefix-list** *listname* **index** *index-number*
Configure the maximum number of TCP connections	1. Access the global configuration view. 2. Run the **ip tcp max-conncect** *maxnum* command.
Enable or disable sending IP packets with an incorrect TTL to the CPU	1. Access the global configuration view. 2. Run the **ip ttl-err to-cpu { enable | disable }** command.
Enable or disable sending ICMP redirect packets	1. Access the global configuration view. 2. Run the corresponding command to access the VLANIF configuration view. 3. Run the **icmp redirect send { enable | disable }** command.
Enable ICMP packets to carry a timestamp when sent to the CPU or disable the function	1. Access the global configuration view. 2. Run the **icmp timestamp to-cpu { enable | disable }**command.
Configure an IPv4 slave address specific for OSPF/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the following commands: ● **mlag ip address** *ipv4-address mask-address* ● **mlag ip address** *ipv4-address/M*
Delete the IPv4 slave address specific for OSPF/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **no mlag ip address** command.

6.1.3 Configuring the TCP Connection Count

Purpose

This section describes how to configure an IP address for a VLANIF interface.
The operation limits the maximum number of TCP connections. For example, when a Telnet service is enabled on the switch, you can set the maximum number of connections.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the TCP connection count	1. Access the global configuration view. 2. Run the **ip tcp max-conncect** *maxnum* command.

6.1.4 Viewing Configuration of an VLAN Interface

Purpose

This section describes how to view the configuration of a designated VLAN interface or all the VLAN interfaces.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the configuration of a designated VLAN interface or all the VLAN interfaces	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the **show interface vlan config** command.

6.1.5 Viewing the TCP/UDP Connection Status

Purpose

This section describes how to view the current TCP/UDP connection status entry.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View the current TCP/UDP connection status entry	1. Access the common user view, global configuration view, or privileged user view. 2. Run the **show ip connect-table** command.

6.1.6 Viewing IP Statistics

Purpose

This section introduces how to view IP related statistics, including the live IP statistics, TCP statistics, UDP statistics, ICMP statistics, IGMP statistics, and TCP/UDP connection table information.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View IP statistics	1. Access the privileged user view, global configuration view, or common user view. 2. Run the following commands: ● **show ip statistic** ● **show ip tcp statistic** ● **show ip udp statistic** ● **show ip icmp statistic**

6.1.7 Viewing System IP Interface Information

Purpose

This section describes how to view the system IP interface information.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the IPv4 interface information	1. Access the privileged user view, global configuration view, common user view, or VLANIF configuration view. 2. Run the **show ip interface** command.
View IP statistics	1. Access the privileged user view, global configuration view, or common user view. 2. Run the following commands: ● **show ip statistic** ● **show ip tcp statistic** ● **show ip udp statistic** ● **show ip icmp statistic** ● **show ip connect-table**

6.1.8 Configuration Example

Network Requirements

The switch Switch connects to the LAN via the Ethernet interface 10 **gigaethernet1/0/1**. The PCs in this LAN belong to two different network segments **0.18.11.0/24** and **10.18.12.0/24**. The configuration requirements are as follows: Users can access these two networks via the switch Switch, but the PCs in these two network segments cannot communicate with each other.

Network Diagram

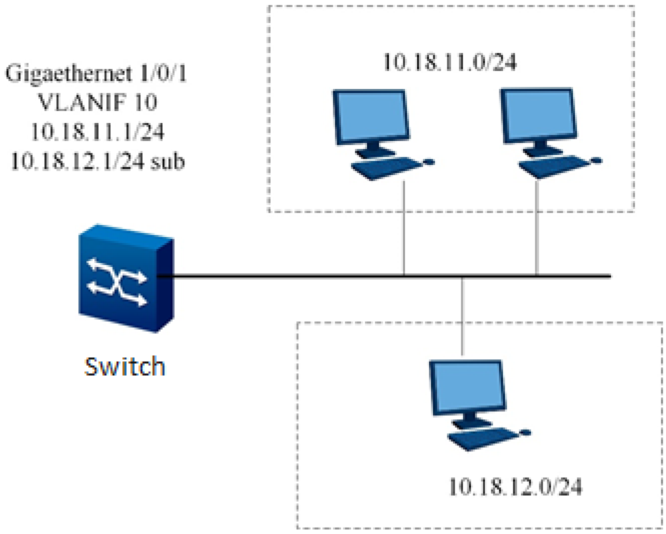


Figure 6-1 IPv4 address configuration topology

Configuration

Configure an IP address for VLAN10 of Switch

```
Switch#configure
Switch(config)#interface vlan 10
Switch(config-vlan-10)#ip address 10.18.11.1/24
Switch(config-vlan-10)#ip address 10.18.12.1/24 sub
Switch(config-vlan-10)#quit
Switch(config)#
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port hybrid vlan 10 untagged
Switch(config-10ge1/0/1)#port hybrid pvid 10
Switch(config-10ge1/0/1)#quit
```

6.2 Configuring IPv6

6.2.1 Configuring Basic IPv6 Functions

6.2.1.1 Configuring IPv6 Addresses

Purpose

This section describes how to configure the IPv6 unicast address, anycast address, multicast address, and link local address on an interface manually.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Set the IPv6 address and the prefix length for an interface manually	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. In the global configuration view, run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 3. Run the following commands: ● **ipv6 address** *ipv6-address/prefix-length* **eui-6** ● **ipv6 address** *ipv6-address/mask-length* **sub**
Delete the configured IPv6 address and its prefix	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. In the global configuration view, run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 3. Run the following commands to delete all the addresses or a designated address of an interface: ● **no ipv6 address** ● **no ipv6 address** *ipv6-address*
Delete the configured IPv6 multicast address of an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command in the global configuration view to access the VLANIF configuration view. 3. Run the **no ipv6 address** *ipv6-address* **eui-64** command.
Enable or disable the IPv6 function for an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. In the global configuration view, run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 3. Run the **ipv6** { **enable** | **disable** } command.

Purpose	Procedure
Enable IPv6 neighbors to forward host routes or disable such forwarding	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **ipv6 nd direct-route { enable | disable }** command.
Configure an IPv6 slave address specific for OSPFv3/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **mlag ipv6 address** *ipv6-address/M* command.
Configure an IPv6 link-local address specific for OSPFv3/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **mlag ipv6 address** *ipv6-address* **link-local** command.
Delete the IPv6 slave address specific for OSPFv3/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **no mlag ipv6 address** command.
Delete the IPv6 link-local address specific for OSPFv3/BGP over MLAG	1. Access the VLANIF configuration view or BD interface configuration view. 2. Run the **no mlag ipv6 address link-local** command.

6.2.1.2 Configuring a Static IPv6 Routing Entry

Purpose

This section describes how to add or delete a static IPv6 routing entry.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Add a static IPv6 routing entry	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the command **ipv6 route-static** *ipv6-address Prefix-len* { *ipv6-nexthop-address* | **interface tunnel | interface vlan** }.
Delete a static IPv6 routing entry	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **no ipv6 route-static** { *ipv6-address prefix-len* | **all** } command.

6.2.1.3 Configuring the IPv6 Unicast Routing Forwarding Function

Purpose

This section describes how to enable or disable the IPv6 unicast routing forwarding function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the IPv6 unicast routing forwarding function	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **ipv6 unicast-forwarding enable** command.
Disable the IPv6 unicast routing forwarding function	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **ipv6 unicast-forwarding disable** command.

6.2.1.4 Configuring an MTU Value of an IPv6 Packet Sent by an Interface

Purpose

This section describes how to configure an MTU value for an interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Set an MTU value for an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command in the global configuration view to access the VLANIF configuration view. 3. Run the **ipv6 mtu** *mtu-value* command.
Restore the MTU value of an interface to the default value	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command in the global configuration view to access the VLANIF configuration view. 3. Run the **ipv6 mtu default** command.

6.2.2 Configuring Other Functions of IPv6

6.2.2.1 Checking IPv6 Network Connectivity and Host Reachability

Purpose

This section describes how to check whether the IPv6 network connection is faulty or how to monitor the network line quality.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Check IPv6 network connectivity and host reachability After an ICMPv6 response packet is sent, the switch waits for the response from the destination host. Configuration under multi-instance VPN is also supported.	1. Access the privileged user view. 2. Run the following commands: ● **ping6** *ipv6-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } value { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-t** ● **ping6** ipv6-address { **-n** | **-l** | **-w** } value **-s** ipv6-source-address

Purpose	Procedure
	● **ping6** ipv6-address { **-n** | **-l** | **-w** } value **-s** ipv6-source-address **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **vpn-instance** *name* **-t**
Test the length of a sent ICMP packet	1. Access the privileged user view. 2. Run the following commands: ● **ping6** *ipv6-address* **-i vlan** *vlan-id* ● **ping6** *ipv6-address* **-i vlan** *vlan-id* **vpn-instance** *name*
Check IPv6 network connectivity and ping the designated host until the operation is manually stopped. Configuration under multi-instance VPN is also supported.	1. Access the privileged user view. 2. Run the following commands: ● **ping6** *ipv6-address* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* **-t** ● **ping6** *ipv6-address* **vpn-instance** *name* ● **ping6** *ipv6-address* **vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* **vpn-instance** *name* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* **vpn-instance** *name* **-t**
Configure an EUI-64 global unicast address	1. Access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 2. Run the following commands: ● **ipv6 address** *ipv6-address/mask-length* **eui-64** ● **ipv6 address** *ipv6-address/mask-length* **eui-64 sub**
Delete the designated EUI-64 global unicast address	1. Access the VLANIF configuration view, Tunnel interface configuration view, or loopback interface configuration view. 2. Run the **no ipv6 address** *ipv6-address* **eui-64** command.
Configure a local IPv6 address for a link	1. Access the VLANIF configuration view. 2. Run the **ipv6 address** *ipv6-address* **link-local** command.
Delete the local IPv6 address of a link	1. Access the VLANIF configuration view. 2. Run the **no ipv6 address link-local** command.

Purpose	Procedure
Configure a local address of an automatically generated link	1. Access the VLANIF configuration view. 2. Run the **ipv6 address auto link-local** command.
Delete the local address of the automatically generated link	1. Access the VLANIF configuration view. 2. Run the **no ipv6 address auto link-local** command.
Configure an EUI-64 global unicast address	1. Access the VLANIF configuration view, tunnel interface configuration view, loopback interface configuration view, or out-of-band interface configuration view. 2. Run the following commands: ● **ipv6 address** *ipv6-address/mask-length* **eui-64** ● **ipv6 address** *ipv6-address/mask-length* **eui-64 sub**
Delete the designated EUI-64 global unicast address	1. Access the VLANIF configuration view, tunnel interface configuration view, loopback interface configuration view, or out-of-band interface configuration view. 2. Run the **no ipv6 address** *ipv6-address* **eui-64** command.

6.2.3 Configuring the IPv6 Neighbor Discovery Function

6.2.3.1 Configuring the Maximum Interval of IPv6 Neighbor Request Message Transmission

Purpose

This section describes how to configure the maximum interval of IPv6 neighbor request message transmission.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Flush all entries in the IPv6 neighbor table	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **flush ipv6 neighbor all** command in the global configuration view.
Flush all dynamic entries in	1. Run the **configure** command in the privileged user view to access the global configuration view.

Purpose	Procedure
the IPv6 neighbor table	2. Run the **flush ipv6 neighbor dynamic** command in the global configuration view.
Flush all static entries in the IPv6 neighbor table	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **flush ipv6 neighbor static** command in the global configuration view.
Configure an IPv6 neighbor discovery life cycle	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **ipv6 nd lifetime** { *life-time* | **default** } command in the global configuration view.

6.2.3.2 Configuring an IPv6 Static Neighbor Entry

Purpose

This section describes how to configure an IPv6 static neighbor entry.

Background

Currently, the device supports up to 128 static neighbor entries.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Add an entry of IPv6 static neighbor	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view or sub-interface configuration view. 3. Run the following commands: ● **ipv6 neighbor** *ipv6-address mac-address* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **ipv6 neighbor** ipv6-address mac-address **eth-trunk** trunk-number
Delete an entry of IPv6 static neighbor	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view or sub-interface configuration view. 3. Run the **no ipv6 neighbor** *ipv6-address* command.

6.2.4 Configuring the IPv6 Debugging Function

Purpose

This section describes debugging for received and sent IPv6 packets, neighbor discovery, and routing. This operation is used for maintaining and debugging the device IPv6 protocol stack.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable debugging for received and sent IPv6 packets	1. Access the privileged user view. 2. Run the **debug ipv6 { in | out | error | all }** command.
Disable debugging for received and sent IPv6 packets	1. Access the privileged user view. 2. Run the **no debug ipv6 { in | out | error | all }** command.
Enable debugging for received and sent RAW IPv6 packets	1. Access the privileged user view. 2. Run the **debug rawip6 { in | out | error | all }** command.
Disable debugging for received and sent RAW IPv6 packets	1. Access the privileged user view. 2. Run the **no debug rawip6 { in | out | error | all }** command.
Enable the IPv6 ICMP debugging function	1. Access the privileged user view. 2. Run the **debug icmp6 all** command.
Disable the IPv6 ICMP debugging function	1. Access the privileged user view. 2. Run the **no debug icmp6 all** command.
Enable debugging for received and sent IPv6 TCP packets	1. Access the privileged user view. 2. Run the **debug tcp6 { in | out | error | event | all }** command.
Disable debugging for received and sent IPv6 TCP packets	1. Access the privileged user view. 2. Run the **no debug tcp6 { in | out | error | event | all }** command.
Enable debugging for received and sent IPv6 UDP packets	1. Access the privileged user view. 2. Run the **debug udp6** { **in** | **out** | **error** | **all** } command.
Disable debugging for received and sent IPv6 UDP packets	1. Access the privileged user view. 2. Run the **no debug udp6** { **in** | **out** | **error** | **all** } command.

6.2.5 Viewing the IPv6 Configuration

Purpose

This section describes how to view the IPv6 configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View the interface IPv6 basic information	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the following commands: ● **show ipv6 interface** ● **show ipv6 interface vpn-instance** *name*
View the information of all IPv6 neighboring nodes on the device (information under multi-instance VPN can also be displayed)	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ipv6 neighbor** ● **show ipv6 neighbor vpn-instance** *name*
View the IPv6 routing entry information of the device	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the **show ipv6 route** command.
Display IPv6 summary route information	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the following commands: ● **show ipv6 route** ● **show ipv6 route summary**
Display IPv6 statistics	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the following commands: ● **show ipv6 route** ● **show ipv6 route summary** ● **show ipv6 statistic**
Display the IPv6 loopback interface information	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the **show ipv6 interface loopback** *loopback-number* command.

Purpose	Procedure
Display the IPv6 VLAN interface information	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the **show ipv6 interface vlan** *vlan-id* command.
Display the entry information of an IPv6 address prefix list	1. Access the common user view, privileged user view, or global configuration view. 2. Run the following commands: ● **show ipv6 prefix-list** ● **show ipv6 prefix-list** *list-name*
Display VLAN-specific IPv6 statistics	1. Access the common user view, privileged user view, global configuration view, or VLANIF configuration view. 2. Run the following commands: ● **show ipv6 statistic interface vlan** *vlan-id* ● **show ipv6 statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● show ipv6 statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number.subinterface*

6.2.6 Configuration Example

Network Requirements

Two switches connect to each other via their interfaces **gigaethenet1/0/1**, which are added to VLANIF10. Configure an IPv6 global unicast address for VLANIF10 to make VLANIF10 communicate with each other.

Network Diagram

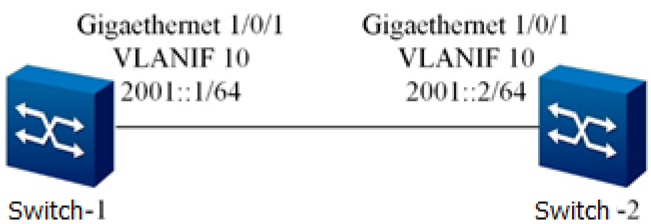


Figure 6-2 IPv6 address configuration topology

Configuration

1. Configure an IP address for VLAN10 of Switch-1.

```
Switch-1#configure
Switch-1(config)#interface vlan 10
# Enable the IPv6 function for the interface.
Switch-1(config-vlan-10)#ipv6 enable
Switch-1(config-vlan-10)#ipv6 address 2001::1/64
Switch-1(config-vlan-10)#quit
Switch-1(config)#
Switch-1(config)#interface 10gigaethernet 1/0/1
Switch-1(config-10ge1/0/1)#port hybrid vlan 10 untagged
Switch-1(config-10ge1/0/1)#port hybrid pvid 10
Switch-1(config-10ge1/0/1)#quit
```

2. Configure an IP address for VLAN10 of Switch-2.

```
Switch-2#configure
Switch-2(config)#interface vlan 10
# Enable the IPv6 function for the interface.
Switch-2(config-vlan-10)#ipv6 enable
Switch-2(config-vlan-10)#ipv6 address 2001::2/64
Switch-2(config-vlan-10)#quit
Switch-2(config)#
Switch-2(config)#interface 10gigaethernet 1/0/1
Switch-2(config-10ge1/0/1)#port hybrid vlan 10 untagged
Switch-2(config-10ge1/0/1)#port hybrid pvid 10
Switch-2(config-10ge1/0/1)#quit
```

6.3 Configuring DHCP

6.3.1 Introduction to DHCP

Background

A PC connected to the Internet needs to know its IP address and other information before sending or receiving data, such as gateway address, subnet mask, and DNS server IP address. The PC can obtain the information via the Bootstrap Protocol (BOOTP), which is a remote boot protocol appearing earlier. BOOTP communicates with the remote server to obtain the information required for communication. It is mainly used for the client without disks to obtain its IP address, server IP address, boot mapping file name, and gateway IP address from the server.

BOOTP is designed to be used in a relatively static environment. Each host has a permanent network connection. The administrator creates a BOOTP configuration file that defines a group of BOOTP parameters for each host. Since the configuration usually remains unchanged, this file is not changed frequently. The configuration usually remains unchanged for weeks.

With unceasing scale expansion and the increasing complexity of the network, it often occurs that the number of PCs exceeds the number of available IP addresses. With the widespread use of portable PCs and wireless networks, PCs are usually carried to different locations and therefore the corresponding IP addresses must be updated accordingly. This makes network configuration more complex. The Dynamic Host Configuration Protocol (DHCP) is developed to meet these requirements.

DHCP adopts the client/server communication mode. The client submits a configuration application to the server and the server returns the configuration information to implement dynamic configuration, such as the IP address.

Terms

- DHCP server

  The DHCP service provider, by interacting with the DHCP client via DHCP packets, assigns appropriate IP addresses to clients of various types and also assigns other network parameters to the clients as needed.

- DHCP client

  It is the trigger and driver of the entire DHCP process, and interacts with the DHCP server through the DHCP packet to obtain the IP address and other network parameters.

- DHCP relay

  The DHCP relay is the relay transponder of DHCP packets. It is located between the DHCP client and the DHCP server that are in different network segments to provide the relay service. It removes the constraint that the DHCP client and DHCP server must be located in the same network segment.

- DHCP snooping

  It provides the DHCP server's L2 monitoring function. This function helps record user IP addresses and MAC addresses.

General DHCP Options

To be compatible with BOOTP, DHCP reserves the message format of BOOTP. The difference between DHCP messages and BOOTP messages lies mainly in the **Option** field. The added function of DHCP based on BOOTP is achieved by the **Option** field.

DHCP uses the **Option** field to transmit control information and network configuration parameters to implement dynamic address allocation and provide more abundant network configuration for the client.

The following are the common DHCP options:

- Option 3: The router option, specifying the gateway address assigned to the client.
- Option 6: The DNS server option, specifying the DNS server address assigned to the client.
- Option 51: The IP address lease option.
- Option 53: The DHCP message type option, identifying the type of the DHCP message.
- Option 55: The request list option, which is used by the client to specify the network configuration parameters to be obtained from the server. The value of this option must be the value of the parameter requested by the client.
- Option 66: The TFTP server option, specifying the domain name of the TFTP server assigned to the client.
- Option 67: The startup file name option, specifying the name of the startup file assigned to the client.
- Option 150: The TFTP server address option, specifying the IP address of the TFTP server assigned to the client.

- Option 121: The classless routing option, which includes a group of classless static routes (that is, the mask of the destination address can be any value and can be used to divide the subnet). When the client receives this option, it adds these static routes to the routing table.
- Option 33: The static route option, which includes a group of classified static routes (that is, the mask of the destination address is a natural mask and cannot be used to divide the subnet). When the client receives this option, it adds these static routes to the routing table. If Option 121 already exists, this option is ignored.

For introduction to more DHCP options, see RFC 2132.

Advantages and Disadvantages of DHCP

DHCP uses the client/server communication mode. All IP network configuration parameters are managed by the DHCP server centrally, which is also responsible for processing the DHCP requests sent from the client. The client uses the IP network parameters assigned by the server for communication.

According to different requirements of the client, DHCP provides the following three types of IP address allocation policies. The administrator can specify the corresponding policy of DHCP to respond to each network or host.

- Allocate addresses manually: The administrator binds static IP addresses with a few specific clients (such as WWW server) and sends the preconfigured IP addresses to these clients via DHCP.
- Allocate addresses automatically: DHCP allocates the IP address with unlimited lease to the client.
- Allocate addresses dynamically: DHCP allocates the IP address with a specified validity period to the client. When the validity period is due, the client needs to apply for the address again.

DHCP expands BOOTP in the following two aspects:

- DHCP allows the PC to obtain an IP address quickly and dynamically. To use the DHCP dynamic address allocation mechanism, the administrator must configure the DHCP server to provide a group of IP addresses, which are collectively called the address pool. Once a new PC connects to the network, it communicates with the server and applies for an IP address. The server selects an address from the configured address pool and allocates it to this PC.

- Compared with BOOTP, DHCP provides more abundant network configuration for the client.

DHCP has the following disadvantages:

- When there are multiple DHCP servers in the network, one DHCP server cannot identify the IP addresses that have been leased by other servers.
- The DHCP server cannot communicate with the client located in a different network segment unless the packets are forwarded by the DHCP relay.

Caution

- The DHCP Option 82 function takes effect only after the DHCP relay is enabled.
- You are advised to use the DHCP Option 82 function on the device closest to the DHCP client to precisely locate the user.

6.3.2 Introduction to DHCP Server

Application Environment

The DHCP server is commonly used to allocate IP addresses in the following situations:

- The network scale is large, which requires a great amount of manual configuration workload, and it is difficult to manage the entire network centrally.
- The number of hosts in the network is greater than the number of IP addresses supported by the network, which makes it unable to allocate a static IP address to each host and limits the number of users accessing the network (this situation occurs on Internet access service providers). Most users must obtain IP addresses dynamically by DHCP.
- Only a few hosts in the network require static IP addresses. That is, most hosts have no need for static IP addresses.

DHCP Server Address Management

The DHCP server selects the IP address and other related parameters from the address pool and allocates them to the client. After the device serving as the DHCP server receives the DHCP request from the client, it selects an idle IP address from an appropriate address pool according to the configuration and sends the address together with other related parameters (such as the DNS server address and address lease period) to the client.

DHCP Server Security Function

- Pseudo-server detection

  In case a DHCP server is secretly set up in the network, when other users apply for IP addresses, this DHCP server interacts with the DHCP client, which causes the users to obtain incorrect IP addresses and makes them unable to access the network normally. This kind of DHCP server is called the DHCP pseudo-server.

  Once the DHCP pseudo-server detection function is enabled on the DHCP server, when the DHCP client sends the DHCP-Request packet, the DHCP server obtains the IP address of the server that allocates the IP address to the client and records this IP address and the interface receiving the packet. This provides convenience for the administrator to detect and handle the DHCP pseudo-server in time.

- Detection of duplicate IP addresses

  To avoid IP address conflicts caused by repeated allocation of the same IP address, the DHCP server needs to detect the IP address before allocating it to the client.

  The DHCP server implements address detection by Ping. It determines whether an address conflict exists by detecting whether it can receive the Ping response from the IP address in the specified time period. The server sends an ICMP packet destined for the IP address that is to be allocated. If the DHCP server does not receive the response within the specified time period, it continues to send the ICMP packet until the number of Ping operations reaches the maximum. If it still does not receive any response, it allocates the address to the client, ensuring that the IP address allocated to the client is unique.

- Address matching detection (anti-static IP user)

  When the DHCP server allocates the IP address to a user, it records the binding relationship between the IP address and MAC address. You can also configure the user address entry manually (that is, the static binding between the IP address and MAC address). To prevent unauthorized users from configuring an IP address statically and accessing other networks, you can enable address matching detection on the device. If the corresponding relationship between IP address and MAC address configured by the user does not exist in the user address table of the DHCP server (including the DHCP entries dynamically recorded and the user address entries manually configured), the DHCP server does not allow the user to access the external network. This function is only applicable in the situation where the DHCP client and server are in the same network segment.

6.3.3 Introduction to DHCP Relay

Application Environment

The original DHCP protocol requires that the client and the server be in the same network segment. A DHCP server must be configured in each network segment to configure the hosts dynamically. This is not cost-effective. The DHCP relay solves this problem. It provides a relay service between the DHCP client and the DHCP server that are in different network segments and sends the DHCP packet to the destination DHCP server across the network segment. The DHCP relay allows the DHCP clients located in different network segments to use the same DHCP server, which saves the cost and also facilitates centralized management.

The DHCP relay is between the DHCP client and the DHCP server that are located in different network segments and provides a relay service for the DHCP client and the DHCP server.

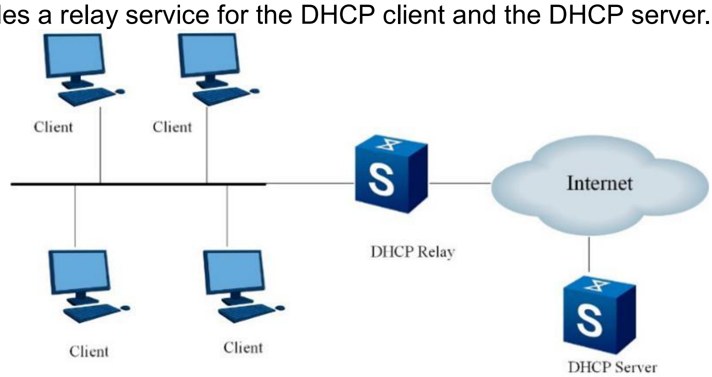


Figure 6-3 DHCP application environment

Option 82 Supported by DHCP Relay

In case the DHCP server and the DHCP client are not in the same subnet, the DHCP relay agent is required to forward DHCP request packets if the client wants to be allocated with the IP address from the DHCP server. Before the DHCP relay agent sends the DHCP packet from the client to the DHCP server, you can insert an option so that the DHCP server can get the client information precisely and allocate an IP address and other parameters flexibly according to the corresponding policy. This option is called **DHCP relay agent information** option and its option number is 82; therefore, it is also called Option 82 and the related standard document is RFC3046.

Option 82 is the extended application of DHCP option and therefore it does not affect the DHCP original application whether the DHCP server carries Option 82 or not. Besides, it depends on whether the DHCP server supports Option 82. The following two situations do not affect the original basic DHCP service: The DHCP server not supporting Option 82 receives the packet inserted with Option 82, or the DHCP server supporting Option 82 receives the packet without Option 82 inserted. To support the extended application of Option 82, the DHCP server must support Option 82 and the packet received must be inserted with the Option 82 information.

Option 82 can identify different users and the server can allocate different IP addresses to different users according to Option 82 to achieve QoS, security, and charging management.

DHCP Relay Security Function

- Address matching detection

  When the DHCP client obtains the IP address from the DHCP server via the DHCP relay, the DHCP relay records the binding relationship between the IP address and MAC address. You can also configure the user address entry manually (that is, the static binding between the IP address and MAC address). To prevent unauthorized users from configuring an IP address statically and accessing other networks, the device supports the address matching detection function of the DHCP relay and you can enable this function on the device. If the corresponding relationship between the IP address and MAC address configured by the user is not in the user address table of the DHCP relay (including the entries dynamically recorded by the DHCP relay and the user address entries manually configured), the DHCP relay does not allow this user to access the external network.

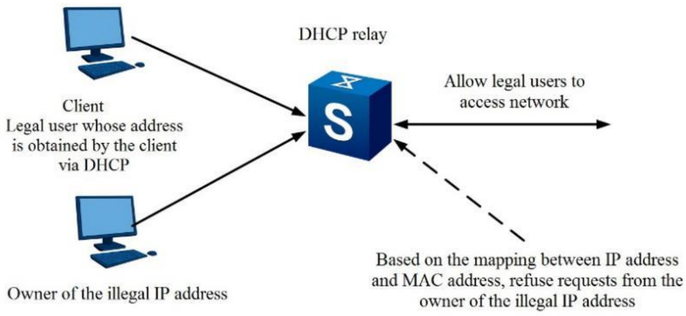


Figure 6-4 DHCP security network diagram

- Scheduled update of user table entries

When the DHCP client obtains the IP address from the DHCP server via the DHCP relay, the DHCP relay records the binding relationship between the IP address and MAC address. When the DHCP client releases this IP address, it sends the unicast DHCP-Release packet to the DHCP server. Because the DHCP relay does not process this packet, the user address entry on the DHCP relay is not updated in real time. You can configure the scheduled update function for the dynamic user table entry on the DHCP relay to solve the above problem.

The DHCP relay sends the DHCP-Request packet to the DHCP server with an IP address allocated to the DHCP client and its own MAC address at set intervals.

If the DHCP server responds with the DHCP-ACK packet, this IP address can be allocated and the DHCP relay ages the corresponding entry in the dynamic user address table.

If the DHCP server responds with the DHCP-NAK packet, this IP address is still on the lease term and the DHCP relay does not age the table entry corresponding to this IP address.

- Pseudo-server detection

In case there is a DHCP server secretly set up in the network, when a client applies for the IP address, this DHCP server interacts with the DHCP client, which causes the client to obtain the incorrect IP address. This kind of DHCP server is called the DHCP pseudo-server.

Once the DHCP pseudo-server detection function is enabled on the DHCP relay, when the DHCP client sends the DHCP-Request packet, the DHCP relay obtains the IP address of the server that allocates the IP address to the client and records this IP address and the interface receiving the packet. This provides convenience for the administrator to detect and handle the DHCP pseudo-server in time.

6.3.4 Configuring the DHCP Server

Prerequisite

Make sure the DHCP client and Switch can communicate with each other properly.

Purpose

This section describes how to configure the DHCP server to allocate IP addresses.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable DHCP globally on the device	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp start** command.

6.3.5 Configuring the Security Function of the DHCP Server

Prerequisite

The DHCP server has been configured.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the DHCP pseudo-server detection function	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp server detect { enable | disable }** command.

6.3.6 Configuring a DHCP Relay

Purpose

This section describes how to configure a DHCP relay so that the DHCP server can allocate IP addresses to users across network segments.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable DHCP globally on the device	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp start** command.
Set the working mode of DHCP interface to Relay	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **ip dhcp relay** command.
Configure an IP address for a DHCP server proxied by the DHCP relay	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **dhcp relay server-ip** *ip-address* command.
Enable or disable DHCP relay support for Option 82	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **dhcp option82** { **enable** | **disable** } command.
Configure a strategy for processing Option 82 request contained in packets sent by a DHCP client for the DHCP relay	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **dhcp option82** { **drop** | **keep** | **replace** } command.
Configure a sub-option Circuit ID of the DHCP Option 82 option, that is, the circuit ID content	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **dhcp option82 circuit-id** *circuitid* command.
Configure a sub-option Remote ID of the DHCP Option 82 option, that is, the remote ID content	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **dhcp option82 remote-id** *remoteid* command.
Configure the DHCP pseudo-server detection function	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp server detect { enable | disable }** command.
Configure a scheduled update period for a DHCP relay user table entry	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp relay user refresh-interval {** *interval* | **default }** command.

6.3.7 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the DHCP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable DHCP relay debugging	1. Remain in the current privileged user view. 2. Run the **debug dhcp relay** command.
Enable DHCP server debugging	1. Remain in the current privileged user view. 2. Run the **debug dhcp server** command.
Clear statistics of the DHCP relay	1. Remain in the current privileged user view. 2. Run the **reset dhcp relay statistic** command.
View the status of the DHCP function parameter configuration of the device	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show dhcp** command.
View the DHCP configuration of the device	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show dhcp config** command.
View the configuration of a DHCP relay server	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show dhcp relay** command.
View the statistics of a DHCP relay	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show dhcp relay statistic** command.
View the DHCP configuration of a specific VLAN interface	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show dhcp vlan** *vlan-id* **config** command.
Enable administrators to view	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view,

Purpose	Procedure
server information in the network	run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the show dhcp fake-server command.

6.3.8 Configuration Example

Network Requirements

The DHCP server assigns IP addresses dynamically to clients located in different network segments **10.1.1.0/24** and **10.1.2.1/24**.

The requirements are as follows:

- The lease term of IP addresses in the **10.1.1.0/24** network segment is 12 hours. The DNS server IP address is **10.1.1.200** and the egress gateway address is **10.1.1.1**.
- The lease term of IP addresses in the **10.1.2.0/24** network segment is 24 hours. The DNS server IP address is **10.1.2.200** and the egress gateway address is **10.1.2.1**.

Network Diagram

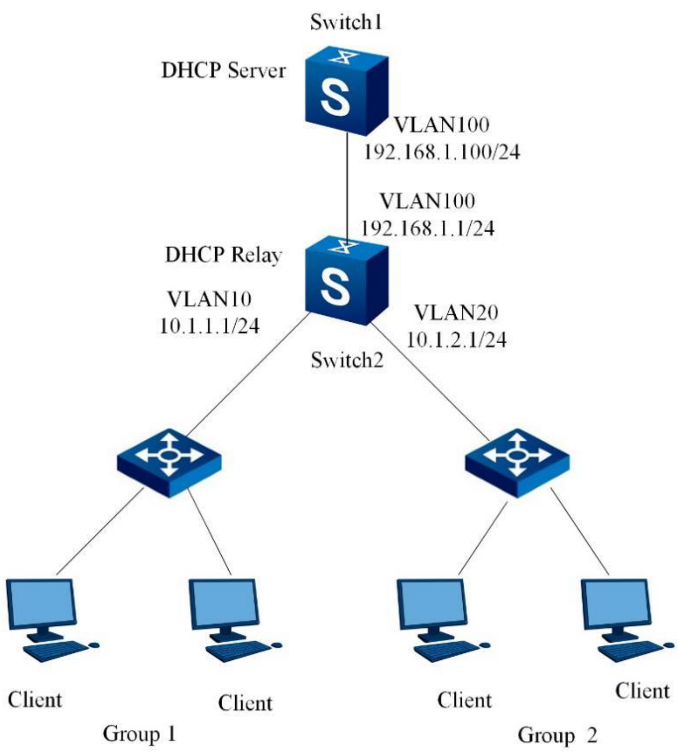


Figure 6-5 DHCP configuration topology

Configuration

1. Configure the DHCP server.

// Configure the IP address of Vlan-interface100 of the DHCP server.

Switch#configure
Switch(config)#dhcp start
Switch(config)#interface vlan 100
Switch(config-vlan-100)#ip address 192.168.1.100/24

2. Configure the DHCP relay.

// Configure the IP address of Vlan-interface10 of the DHCP relay and set its working mode to Relay.

Switch#configure
Switch(config)#dhcp start
Switch(config)#interface vlan 10
Switch(config-vlan-10)#ip address10.1.1.1/24
Switch(config-vlan-10)#ip dhcp relay
Switch(config-vlan-10)#dhcp relay server-ip 192.168.1.100

// Configure the IP address of Vlan-interface20 of the DHCP relay and set its working mode to Relay.

Switch#configure
Switch(config)#interface vlan 20
Switch(config-vlan-20)#ip address 10.1.2.1/24
Switch(config-vlan-20)#ip dhcp relay
Switch(config-vlan-20)#dhcp relay server-ip 192.168.1.100

// Configure the IP address of Vlan-interface100 of the DHCP relay and set its working mode to Relay.

Switch#configure
Switch(config)#interface vlan 100
Switch(config-vlan-100)#ip address 192.168.1.1/24
Switch(config-vlan-100)#ip dhcp relay

6.4 Configuring DHCP Client

6.4.1 DHCP Client Overview

Working Principle of DHCP Client

DHCP adopts the client/server communication mode. The client submits a configuration application to the server and the server returns the configuration information to implement dynamic configuration, such as the IP address.

To obtain a legal dynamic IP address, the DHCP client needs to exchange different types of information with the DHCP server in different periods.

Working process of the DHCP client:

- Discover period: The DHCP client sends DISCOVER packets to locate the DHCP server. As the DHCP server is unknown to the DHCP client, the packets are sent in broadcast mode.
- Selection period: If there are multiple DHCP servers replying offer packets to the DHCP client, the DHCP client receives only the first arrived offer packet and then sends a REQUEST packet in broadcast mode. In this way, the DHCP client informs other unselected DHCP servers to reclaim the IP addresses they provide.
- Validity verification on the address assigned by the DHCP server: After receiving the ACK packet returned by a DHCP server, the DHCP client sends an ARP inspection for free to check whether the IP address is available. If the IP address is not available, a DECLINE packet is sent in broadcast mode and IP address application is re-initiated.
- Tenancy update: Generally, the IP address assigned by the DHCP server to the DHCP client has a tenancy period. After the period expires, the DHCP client needs to update the tenancy period if it still wants to use it.

1. When the IP address tenancy reaches half of its period (T1), the DHCP client automatically sends a REQUEST packet to the DHCP server in unicast mode for IP tenancy update. If the DHCP client receives the ACK packet, the tenancy is updated successfully. If the DHCP client receives the NAK packet, it re-initiates the application process.

2. If no response is received from the DHCP server when the tenancy period reaches 87.5% (T2) of its validity period, the DHCP client broadcasts a packet to the DHCP Server to request a lease renewal. If the DHCP Client receives an ACK packet, the lease renewal is successful. If the DHCP Client receives a NAK packet, the DHCP Client must send a packet to apply for a new IP address.

- IP address released by DHCP client: When the DHCP client no longer needs the assigned IP address, it sends a RELEASE packet to the DHCP server to inform the latter to release the IP address tenancy.

6.4.2 Configuring Basic Functions of DHCP Client

Prerequisite

The DHCP server has been configured in the network.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the DHCP client to automatically obtain an IP address or disable this function	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **ip address dhcp { enable | disable }** command.
Renew the IP address obtained by the DHCP client	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **ip address dhcp renew** command.
Release the IP address obtained by the DHCP client	1. Run the **configure** command to access the global configuration view. 2. Run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 3. Run the **ip address dhcp release** command.

6.4.3 Configuring Option Information in Auto-config Mode and Customization Mode

Prerequisite

The DHCP server has been configured in the network.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the auto-config mode	1. Run the **configure** command to access the global configuration view. 2. Run the **dhcp client auto-config mode** { **compatible** | **user-define** | **default** } command to set the Auto-config mode to Huawei compatible mode, customization mode, or default Switch mode.
Configure the ftp-name option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client ftp-name option** *name-value* ● **dhcp client ftp-name option** *name-value* **sub-option** *sub-name-value*
Configure the ftp-password option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client ftp-password option** *password-value* ● **dhcp client ftp-password option** *password-value* **sub-option** *sub-password-value*
Configure the ftp-server-ip option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client ftp-server-ip option** *serverip-value* ● **dhcp client ftp-server-ip option** *serverip-value* **sub-option** *sub-serverip-value*
Configure the image-file option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client image-file option** *imagefile-value* ● **dhcp client image-file option** *imagefile-value* **sub-option** *sub-imagefile-value*
Configure the reboot-time option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client reboot-time option** *reboottime-value* ● **dhcp client reboot-time option** *reboottime-value* **sub-option** *sub-reboottime-value*
Configure the auth-message	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client auth-message option** *authmessage-value*

Purpose	Procedure
option and the sub-options	● **dhcp client auth-message option** *authmessage-value* **sub-option** *sub-authmessage-value*
Configure the image-file option and the sub-options	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **dhcp client image-file option** *imagefile-value* ● **dhcp client image-file option** *imagefile-value* **sub-option** *sub-imagelistfile-value*

6.4.4 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the DHCP client fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable DHCP client debugging	1. Run the **configure** command to access the global configuration view or remain in the current privileged user view without executing any commands. 2. Run the **debug dhcp client { state | in | out | packet | all }** command.
View the DHCP client status of all VLAN interfaces or a specified VLAN interface	1. Run the **configure** command to access the global configuration view or remain in the current privileged user view, or run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 2. Run the following commands: ● **show dhcp client** ● **show dhcp client VLAN** *vlan-id*
View all the configuration information of auto-config on a VLAN interface	1. Run the **configure** command to access the global configuration view or remain in the current privileged user view or access the common user view, or run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 2. Run the **show dhcp client auto-config vlan** *vlan-id* command.
View the DHCP client Tx/Rx packet information of all VLAN interfaces or a specified VLAN interface	1. Run the **configure** command to access the global configuration view or remain in the current privileged user view, or run the **interface vlan** *vlan-id* command to access the VLANIF configuration view. 2. Run the following commands: ● **show dhcp client statistic** ● **show dhcp client statistic VLAN** *vlan-id*

Purpose	Procedure
View information about a DHCPv6 interface	1. Access the common user view. 2. Run the following commands: ● **show dhcpv6 interface** ● **show dhcpv6 interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*
View information about a DHCPv6 relay interface	1. Access the common user view. 2. Run the following commands: ● **show dhcpv6 relay** ● **show dhcpv6 relay interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*
View statistics of a DHCPv6 interface	1. Access the common user view. 2. Run the following commands: ● **show dhcpv6 statistic** ● **show dhcpv6 statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*

6.4.5 Configuration Example

Network Requirements

DHCP is a protocol typically working in server/client mode. The DHCP client and DHCP server in the following figure are in the same subnet for direct DHCP interaction.

Network Diagram

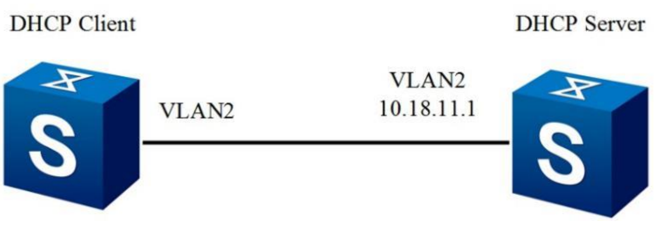


Figure 6-6 DHCP client configuration topology

Configuration

1. Configure a VLAN for an interface on the DHCP client switch.
Switch#configure
Switch(config)#vlan 2
Switch(vlan-2)#quit
Switch(config)#interface xge1/0/2
Switch(config-10ge1/0/2)#no shutdown
Switch(config-10ge1/0/2)#port hybrid vlan 2 untagged
Switch(config-10ge1/0/2)#port hybrid pvid 2
Switch(config-10ge1/0/2)#quit

2. Enable automatic dynamic IP address obtaining for the DHCP client.
Switch(config)#interface vlan 2
Switch(config-vlan-2)#ip address dhcp enable

3. Verify the obtained configuration result.
Switch#show dhcp client
DHCP client information:
Interface:vlan-2
    Current state…..: Bound
  Allocated IP……: 10.18.11.2
  Subnet Mask…..:255.255.255.0
  Server IP……….:10.18.11.1
  Allocated lease..:86400 seconds
  Lease T1 time…:43200 seconds
  Lease T2 time…:75600 seconds
  Lease Obtained.:2100/06/28 Mon 5:23:36 AM
  Lease timeout…:2100/06/29 Tue 5:23:36 AM
Transaction ID….:0x7f43
Client ID…………:01 00 04 67 99 9e 6c
DHS……………...:
Gateway…………:10.18.11.1
Domain…………..:
Lease time will time out in 0 days 23 hours 59 minutes 50 seconds.

4. Update the tenancy on the DHCP client interface.
Switch(config)#int vlan 2
Switch(config-vlan-2)#ip address dhcp renew

5. Verify the configuration result of tenancy update, updated from 23:59:50 to 23:59:56.

Switch(config)#show dhcp client
DHCP client information:
Interface:vlan-2
    Current state…..: Bound
  Allocated IP……: 10.18.11.2
  Subnet Mask…...:255.255.255.0
  Server IP……….:10.18.11.1
  Allocated lease..:86400 seconds
  Lease T1 time…:43200 seconds
  Lease T2 time…:75600 seconds
  Lease Obtained.:2100/06/28 Mon 5:24:55 AM
  Lease timeout…:2100/06/29 Tue 5:24:55 AM
Transaction ID….:0x7f43
Client ID…………:01 00 04 67 99 9e 6c
DHS……………...:
Gateway…………:10.18.11.1
Domain…………..:
Lease time will time out in 0 days 23 hours 59 minutes 56 seconds.

6. Release the IP address of the DHCP client interface.

Switch(config)#int vlan 2
Switch(config-vlan-2)#ip address dhcp release

7. Verify the configuration result of tenancy update.

Switch(config-vlan-2)#ip address dhcp release
Switch(config-vlan-2)#show dhcp client vlan 2
        Current state…..: Release
        Allocated IP……: 0.0.0.0
        Subnet Mask…...:0.0.0.0
        Server IP………..:0.0.0.0

Chapter 7 Configuring L3 IP

This chapter describes the basic content, configuration procedure, and configuration examples of the routing function of the Switch.

7.1 Configuring Basic IP Routing Functions

7.1.1 Configuring ECMP

Purpose

This section describes how to configure ECMP.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create an Equal Cost Multi-path (ECMP) enhanced template and access the ECMP template view	1. Run the **configure** command to access the global configuration view. 2. Run the **ecmp-profile** *profile-name* command.
Configure an ECMP load balancing mode	1. Run the **configure** command to access the global configuration view. 2. Run the **ecmp load-balance { src-ip | default }** command.
Bind or unbind an ECMP load balancing mode to or from a profile	1. Run the **configure** command to access the global configuration view. 2. Run the **ecmp load-balance profile** *profile-name* command.
View the configuration of an ECMP template	1. Access the common user view. 2. Run the following commands: ● **show ecmp-profile** *profile-name* ● **show ecmp-profile**
Display the ECMP load balancing information	1. Access the common user view. 2. Run the **show ecmp load-balance** command.

7.2 Configuring Static Routes

7.2.1 Configuring Static IPv4 Routes

Purpose

This section describes how to add or delete a static IPv4 route.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Add a static IPv4 route	1. Access the global configuration view. 2. Run the following commands: ● **ip route-static** *ip-address mask-address nexthop-address* ● **ip route-static** *ip-address mask-address nexthop-address* **preference {** *preference-value* | **default** } ● **ip route-static** *ip-address mask-address nexthop-address* **track bfd** *track-number* ● **ip route-static** *ip-address mask-address* **interface null** *null-number* ● **ip route-static** *ip-address mask-address* **interface tunnel** *tunnel-number*
Delete one or all static IPv4 routes	1. Access the global configuration view. 2. Run the following commands: ● **no ip route-static** *ip-address mask-address nexthop-address* **track bfd** ● **no ip route-static** *ip-address mask-address* ● **no ip route-static** *ip-address mask-address nexthop-address*
Delete a designated VPN instance corresponding to a static IPv4 route	1. Access the global configuration view. 2. Run **the no ip route-static all** command.
Configure the IP route that passes the null interface	1. Access the global configuration view. 2. Run the **ip route-static** *ip-address mask-address* **interface null** *null-number* command.

7.2.2 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the static route configuration function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View one or more routing records	1. Access the privileged user view, global configuration view, or common user view. 2. Run the following commands: ● **show ip route** ● **show ip route** *ip-address*
View route statistics in the IPv4 routing table	1. Access the privileged user view, global configuration view, or common user view. 2. Run the **show ip route statistic** command.
Display summary route information	1. Access the privileged user view, global configuration view, or common user view. 2. Run the **show ip route summary** command.

7.3 Configuring OSPF

7.3.1 OSPF Overview

7.3.1.1 Background Information

Open Shortest Path First (OSPF) is developed by the OSPF working group of Internet Engineering Task Force. It is designed for TCP/IP networks and supports CIDR and the function of marking external routing information. OSPF verifies route update and uses IP multicast when transmitting/receiving updates. OSPF can respond to topology change quickly using a small amount of routing traffic.

OSPF forwards IP packets only using the destination address in the IP packet header. IP packets are forwarded within an autonomous system (AS), and are not re-encapsulated by other protocols. OSPF is a dynamic routing protocol, which can detect topology change in an AS quickly (such as router interface failure) and can calculate a new loop-free route after a period of convergence. Convergence takes a short time and uses a small amount of routing traffic.

In the connection status routing protocol, each router maintains a database to describe the AS topology structure. This database is called connection status database. All the participating routers share the same database. Each item in the database describes the status of the designated router (such as the available interface of the router and the reachable neighbor). The router sends its status to the entire AS via flooding.

All routers run the same algorithm simultaneously. According to the connection status database, each router constructs a tree of the shortest path, taking itself as the root. The tree gives the path to each destination in the AS. The source of the routing information is the leaf on the tree. If multiple paths of the same value reach the same destination, the data traffic is evenly distributed among the paths. The path distance is a non-dimensional number.

OSPF allows aggregation of a group of networks, which is called area. The area hides its inner topology from the other parts in the AS. The hidden information effectively reduces the routing traffic. Meanwhile, routing in the area depends only on the topology of the area, which prevents incorrect routing information.

The area is generally a subnet-based IP network. OSPF supports flexible IP subnet configuration. Each path distributed by OSPF contains the destination IP address and mask. Two subnets in one IP network can be of different sizes (that is, with different masks), which are called variable length subnetting. Packets are forwarded according to optimal matching (longest matching). The host path is processed as the subnet with a mask only containing 1s (0xffffffff).

All information exchanged via OSPF is verified, which means only the trusted routers in the AS can participate in routing. Multiple verification methods are available for different IP subnets. External routing information (such as the route obtained by a router via an external gateway protocol such as BGP [reference23]) is advertised over the entire AS. The external data is independent from the OSPF protocol connection status data. Each external path can be marked by the advertising router, and sends extra information between autonomous system boundary routers (ASBRs).

7.3.1.2 Protocol Features

- Wide application range: OSPF supports networks of various scales with up to hundreds of routers.
- Fast convergence: OSPF sends an update packet once the network topology changes so that other nodes in the AS can synchronize the change quickly.
- No loop: OSPF calculates routing using the shortest-path tree algorithm according to the collected link statuses. This algorithm guarantees that there is no loop routing in OSPF.
- Area setting: The network of an AS can be set to areas for management. The routing information transmitted between areas is further abstracted, which reduces the network bandwidth occupation.
- Equal-cost multi-path routing: OSPF supports multiple equal-cost multi-path routes to the same destination.
- Route classification: OSPF uses four types of routes: intra-area route, inter-area route, class 1 external route, and class 2 external route, in order of priority.
- Verification: OSPF supports interface-based packet verification, which guarantees the security of packet exchange.
- Multicast transmission: On the links that support multicast, OSPF sends protocol packets using a multicast address, which reduces the impact on other devices.

7.3.1.3 Basic Concepts

Calculation Process of OSPF Routing

The calculation process of OSPF routing is described as follows:

1. Each OSPF router generates a link state advertisement (LSA) according to the surrounding network topology, and sends the LSA to other OSPF routers using the update packet.
2. Each OSPF router collects the LSAs sent from other routers. All the LSAs form a link state database (LSDB), which describes the network topology of the entire AS.
3. The OSPF router converts the LSDB into a weighted directed graph, which reflects the topology of the entire network. Each OSPF router obtains the same weighted directed graph.

4. Based on the directed graph, each OSPF router uses the SPF algorithm to calculate a tree of the shortest path taking itself as the root. The tree shows the routing of each node in the AS.

Router ID

To run the OSPF protocol, a router must have a router ID. Router ID is an integer of 32 bits without symbols, which is the unique identifier of the router in the AS.

The router ID can be either configured manually or be generated by the system automatically. If the protocol fails to obtain the router ID by automatic generation, the following rules take effect:

1. Maximum static loopback address
2. Maximum static primary address
3. Maximum static secondary address
4. Maximum static link local address
5. Maximum address distributed by DHCP

If the protocol fails to obtain the router ID, the router ID is 0. In this case, network configuration cannot be performed for multi-instance.

You can also run the command to configure an ID manually. The input ID must be the local IP address; otherwise, the command is invalid. To improve network stability, the OSPF ID does not change with the IP address. Even if the corresponding IP address is deleted, the OSPF ID remains unchanged. In this case, the OSPF ID must be modified manually. After the modification, information such as OSPF neighbor and database is updated. A large amount of protocol traffic occurs within a period resulting in network impact. Therefore, do not use this command frequently whenever possible.

OSPF Protocol Packet

OSPF has five types of protocol packets:

1. Hello packet: Sent periodically to discover and maintain the OSPF neighbor relationship.
2. Database description (DD) packet: Describes the abstraction of the local LSDB and is used to synchronize the database when two routers start to establish adjacency.
3. Link state request (LSR) packet: Requests the required LSA from the peer end.
4. Link state update (LSU) packet: Sends the required LSA to the peer end.
5. Link state acknowledgment (LSAck) packet: Verifies the received LSA.

LSA Types

The description of routing information in OSPF is encapsulated in LSA and then transmitted. Common LSA types are as follows.

1. Router LSA (type 1): Generated by each router. It describes the router link status and overhead, and is transmitted within the attributed area.
2. Network LSA (type 2): Generated by the designated router (DR). It describes the link status of the local network segment, and is transmitted within the attributed area.
3. Network summary LSA (type 3): Generated by an area border router (ABR). It describes the routing of a certain network segment within the area and advertises it to other areas.
4. ASBR summary LSA (type 4): Generated by an ABR. It describes the route destined for an ASBR and advertises it to the corresponding area.
5. AS external LSA (type 5): Generated by an ASBR. It describes the route destined for the network outside the AS and advertises it to all areas except the stub area and not-so-stubby area (NSSA).
6. NSSA LSA (type 7): Generated by an ASBR. It describes the route destined for the network outside the AS, and is transmitted only within the NSSA.

Neighbor and Adjacency

In OSPF, neighbor and adjacency are two different concepts.

1. Neighbor relationship: After enabled, the SPF router sends a Hello packet externally via the OSPF interface. The OSPF router that receives the Hello packet checks parameters in the packet. If the parameters of the two routers are consistent, a neighbor relationship is established.
2. Adjacency relationship: Two routers that form a neighbor relationship do not necessarily form an adjacency relationship, which depends on the network type. They form an adjacency relationship only if they exchange the DD packets and LSAs successfully.

7.3.1.4 OSPF Area and Route Aggregation

Area Setting

As the network scale is expanding, the quantity of routers that run OSPF is increasing. The network and routers change as follows:

1. Network change

The probability of topology change increases and the network becomes unstable, leading to the transmission of a large number of OSPF protocol packets in the network and reduction of network bandwidth utilization. At each topology change, all routers in the network re-calculate routing.

2. Router change

(1) LSDB increase

(2) Storage occupation increase

(3) More complex SPF algorithm

(4) CPU load increase

3. Area Setting

To solve the above problems, OSPF sets an AS into different areas. Areas are different logical groups of routers. Each group is identified by an area ID. The edge of an area is a router instead of a link. One network segment (link) only belongs to one area. That is, each interface that runs OSPF must indicate to which area it belongs, as shown in Figure 7-1.

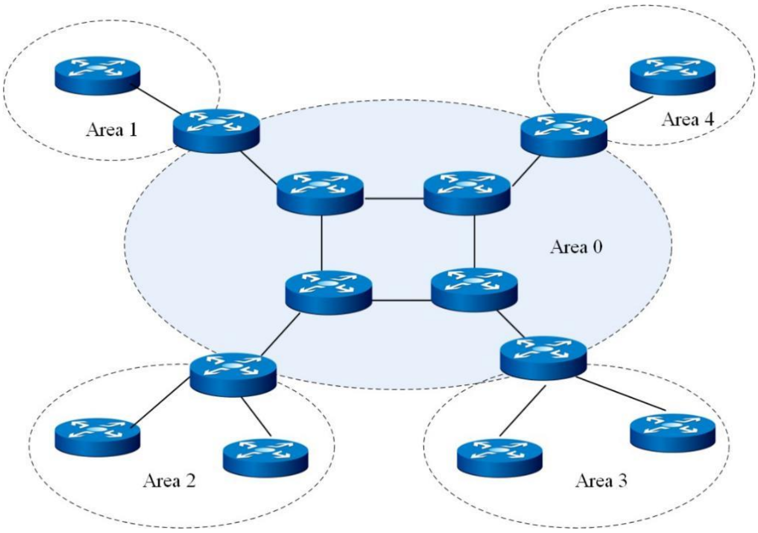


Figure 7-1 Area setting

After an area is set, route aggregation can be performed on the edge router of the area to reduce the quantity of LSAs that are advertised to other areas. Setting areas can also minimize the impact caused by network topology change.

Router Types

As shown in Figure 7-2, OSPF routers can be classified into the following four types according to their locations in the AS:

1. Internal router

All interfaces of an internal router belong to one OSPF area.

2. ABR

An ABR can belong to more than two areas, one of which must be the backbone area. An ABR connects the backbone area and non-backbone area. It can be connected to the backbone area either physically or logically.

3. Backbone router

At least one interface of a backbone router belongs to the backbone area. Therefore, all the ABRs and the internal routers in Area 0 are backbone routers.

4. ASBR

An ASBR exchanges routing information with other ASs. An ASBR is not necessarily located at the edge of the AS but may be located inside the area, or it may be an ABR. As long as an OSPF-enabled router imports external routing information, it is an ASBR.

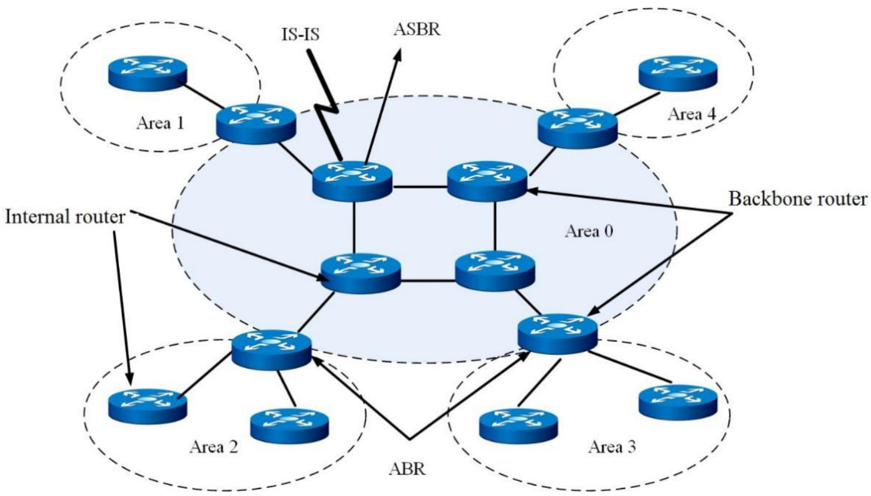


Figure 7-2 Types of OSPF-enabled routers

Backbone Area

After areas are set for OSPF, not all areas are equal. One area is different, which is called the backbone area. Its area ID is 0.

The backbone area is responsible for routing between areas. The routing information between non-backbone areas must be transmitted via the backbone area. OSPF has the following rules:

All non-backbone areas must be properly connected to the backbone area, and the backbone area must be reachable. In practical application, the requirement may not be met because of network topology limitations. In this case, you can configure OSPF virtual connection to meet the requirement.

Virtual Connection

Virtual connection is a logical connection path created between two ABRs via a non-backbone area. A virtual connection forms a point-to-point connection between two ABRs. The area that provides a route inside a non-backbone area for both ends of the virtual connection is called a transit area.

Virtual connection has the following features:

1. Both ends of the virtual connection must be ABRs.
2. Virtual connection takes effect only if it is configured at both ends.
3. Like a physical interface, the virtual connection can be configured with interface parameters, such as the Hello packet sending interval.
4. When two ABRs transmit OSPF packets to each other, the OSPF-enabled routers between them only forward the packets. Because the destination addresses of the protocol packets are not these routers, the packets are transparent to these routers and are forwarded as common IP packets.

Stub Area

1. Features of a stub area:

The ABR in a stub area does not transmit the received route outside of the AS, which greatly reduces the size of the routing table on routers and the amount of transmitted routing information in the area.

Stub area is an optional configuration. Not all areas meet the configuration requirement. Generally, a stub area is the non-backbone area that has only one ABR and is located at the edge of the AS.

To make sure the route outside the AS is still reachable, the ABR in the stub area generates a default route and distributes it to non-ABR routers in the stub area.

2. Precautions about stub area configuration:

The backbone area cannot be configured as a stub area.
To configure an area as a stub area, all routers in the area must be configured to belong to the stub area.
No ASBR can exist in the stub area. That is, routes outside the AS cannot be transmitted within the local area. Virtual connection cannot pass through the stub area.

NSSA

NSSA is a new type of areas added to RFC1587 NSSA Option, together with a new type of LSA: NSSA LSA (also called type 7 LSA).
NSSA is a transformation of the stub area. NSSA shares a lot of similarities with the stub area.

1. Features of NSSA:

Similar to the stub area, the NSSA cannot be configured with virtual connection.
NSSA does not permit the import of AS-External-LSA (that is, type 5 LSA), but permits the import of type 7 LSA.
Type 7 LSA is generated by the ASBR in NSSA and transmitted within the NSSA.
When type 7 LSA reaches the ABR of NSSA, the ABR converts type 7 LSA into AS-External LSA before transmitting it to other areas.

2. Example of NSSA:

As shown in Figure 7-3, the AS that runs OSPF contains three areas: Area 1, Area 2, and Area 0.
Area 1 is defined as an NSSA. The non-OSPF network that is connected to Area 1 and Area 2 runs RIP. After the RIP route that Area 1 receives from the RIP network is transmitted to the ASBR in NSSA, the NSSA ASBR generates type 7 LSA to be transmitted in Area 1. After type 7 LSA reaches the NSSA ABR, it is converted into type 5 LSA to be transmitted to Area 0 and Area 2.
The RIP route that Area 2 receives from the RIP network generates type 5 LSA via the ASBR in Area 2 to be transmitted in OSPF AS. Because Area 1 serves as NSSA, the type 5 LSA does not reach Area 1.

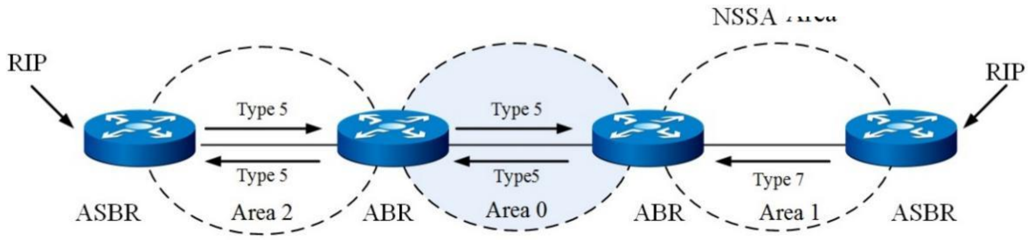


Figure 7-3 NSSA

Route Aggregation

Route aggregation is a process where ABR aggregates routes with the same prefix into one route to be distributed to other areas.

After an AS is divided into different areas, route aggregation can be performed between areas to reduce routing information and the routing table size and thereby speed up router calculation.

For example, three routes, 19.1.1.0/24, 19.1.2.0/24 and 19.1.3.0/24, exist in Area 1. If route aggregation is configured on ABR to aggregate the three routes into one route 19.1.0.0/16, the ABR generates one aggregated LSA and distributes it to routers in other areas.

Route Types

OSPF classifies routes into four levels in order of priority:

Intra-area route

Inter-area route

Type 1 external route

Type 2 external route

1. AS internal route

Intra-area routes and inter-area routes of an AS describe the internal network structure of the AS. By default, the protocol priority of intra-area routes and inter-area routes is 10.

2. AS external route

An external route is a route to the destination address outside of an AS. OSPF classifies the imported external routes of an AS into two types: type 1 and type 2. By default, the protocol priority of intra-area routes and inter-area routes is 150.

Type 1 external route is the received IGP route (for example, a static route or RIP route). Because this type of route is highly trusted, the calculated external route overhead is consistent with the route overhead inside the AS, and is comparable to the OSPF route overhead. That is, the overhead of type 1 external route equals the overhead from the local router to corresponding ASBR plus the overhead from ASBR to the destination address of the route.

Type 2 external route is the received EGP route. Because this type of route is not highly trusted, OSPF considers that the overhead from ASBR to the outside of the AS is far greater than that from the inside of the AS to ASBR; therefore, the former is considered first during route overhead calculation. That is, the overhead of type 2 external route equals the overhead from ASBR to the destination address of the route. If the overhead values calculated for two routes are equal, the overhead from the local router to the corresponding ASBR is considered.

7.3.1.5 OSPF Network

OSPF Network Types

The network is classified into the following four types according to the link layer protocol type:

1. Broadcast type

If the link layer protocol is Ethernet and Fiber Distributed Digital Interface (FDDI), OSPF considers the network type as broadcast by default. In a broadcast network, protocol packets are generally transmitted in multicast mode (224.0.0.5 and 224.0.0.6).

2. Non-broadcast multi-access (NBMA) type

If the link layer protocol is frame relay, ATM or X.25, OSPF considers the network type as NBMA by default. In an NBMA network, protocol packets are generally transmitted in unicast mode.

3. Point-to-multipoint (P2MP) type

No link layer protocol is considered as the P2MP type by default. The P2MP type is forcibly converted from other network types. Generally, the non-fully-meshed NBMA is changed to the P2MP type. In a P2MP network, protocol packets are generally transmitted in multicast mode (224.0.0.5).

4. Point-to-point (P2P) type

If the link layer protocol is PPP, HDLC or LAPB, OSPF considers the network type as P2P by default. In a P2MP network, protocol packets are generally transmitted in multicast mode (224.0.0.5).

DR and BDR

In a broadcast network and NBMA network, any two routers transmit information to each other. If *n* routers exist in the network, nx(n–1)/2 adjacency relationships must be established. Therefore, the routing change of any router leads to several times of transmission, which wastes bandwidth resources. To solve this problem, OSPF defines designated router (DR), backup designated router (BDR), and the router other than DR and BDR (called DR Other).

1. DR

All routers only send information to DR, and DR broadcasts the network link status.

2. BDR

If DR fails, routers in the network must re-elect a new DR and synchronize with the new DR. This takes a long time and route calculation is incorrect during this period. To shorten the process, OSPF proposes the concept of BDR. BDR is actually a backup for DR. The BDR is elected when DR is elected. BDR establishes an adjacency relationship with all routers in the local network segment and exchanges routing information. After DR fails, BDR becomes the new DR. The process takes a short time because no re-election is required and the adjacency relationship has been established in advance. In this case, a new BDR must be elected, which takes a long time but does not affect route calculation.

3. DR Other

The routers other than DR and BDR (called DR Other) neither establish adjacency relationships with each other nor exchange routing information, which reduces the quantity of adjacency relationships between routers in the broadcast network and NBMA network.

DR/BDR Election

1. DR/BDR election process

DR and BDR are not manually designated but are elected by all routers in the local network segment. The DR priority of the router interface determines the qualification of the interface for DR and BDR election. In the local network segment, the routers with DR priority greater than 0 can be candidates. The vote in election is the Hello packet. The election process is as follows:

Each router writes the elected DR to the Hello packet and sends it to other routers in the network segment.

If two routers in the same network segment announce simultaneously that they are DRs, the router with the higher DR priority is elected. If they have the same priority, the one with the greater router ID is elected. If the priority of a router is 0, the router is not elected to be DR or BDR.

2. Features of DR/BDR election

DR can be elected only if the interface type is broadcast or NBMA. Interfaces of P2P or P2MP type need no DR election.

DR is a concept in a network segment for the router interface. A router may be DR on one interface and may be BDR or DR Other on other interfaces.

If DR and BDR are elected, after a new router joins, it does not become the DR in the network segment even if its DR priority is the greatest.

DR may not be necessarily the router with the greatest DR priority; in the same way, BDR may not be necessarily the router with the second greatest DR priority.

7.3.1.6 OSPF Packet Format

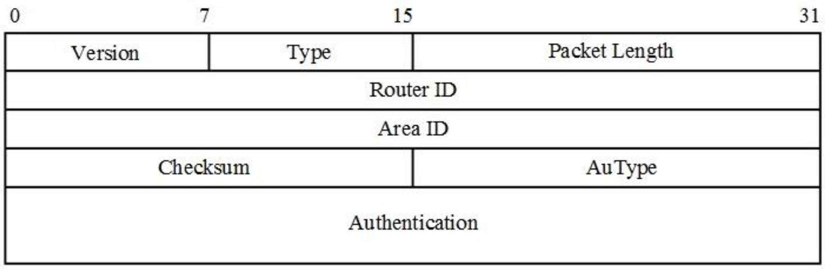
OSPF Packet Structure

OSPF uses IP packets to encapsulate protocol packets directly (the protocol number is 89). The structure of a complete OSPF packet (taking the LSU packet as an example) is as follows.

IP Header	OSPF Packet Header	Number of LSAs	LSA Header	LSA Data

OSPF Packet Header

There are five OSPF packet types, which share the same packet header, as shown in the following figure.



The meanings of the main fields are as follows.

Version: OSPF version. For OSPFv2, the version is 2.

Type: OSPF packet type. The values are 1 to 5, corresponding to the Hello packet, DD packet, LSR packet, LSU packet, and LSAck packet, respectively.

Packet length: Total length (in bytes) of the OSPF packet, including the packet header.

AuType: Authentication type, including non-authentication (0), simple authentication (1), and MD5 authentication (2).

Authentication: The value depends on the authentication type. If the authentication type is 0, this field is not defined; if the authentication type is 1, this field indicates the password; if the authentication type is 2, this field contains the information of the key ID, MD5 authentication data length, and SN.

The MD5 authentication data is appended to the OSPF packet but not included in the **Authentication** field.

Hello Packet

Hello packet is the most common packet and sent to the neighbor of the local router periodically. It includes the value of timers, DR, BDR and the known neighbors. The format of the Hello packet is as follows.

<table>
<tr><td>0</td><td>7</td><td>15</td><td>31</td></tr>
<tr><td>Version</td><td>Type=1</td><td colspan="2">Packet Length</td></tr>
<tr><td colspan="4">Router ID</td></tr>
<tr><td colspan="4">Area ID</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">AuType</td></tr>
<tr><td colspan="4">Authentication</td></tr>
<tr><td colspan="4">Network Mask</td></tr>
<tr><td colspan="2">HelloInterval</td><td>Options</td><td>Rtr Pri</td></tr>
<tr><td colspan="4">RouterDeadinterval</td></tr>
<tr><td colspan="4">Designated Router</td></tr>
<tr><td colspan="4">Backup Designated Router</td></tr>
<tr><td colspan="4">Neighbor</td></tr>
<tr><td colspan="4">...</td></tr>
</table>

The meanings of the main fields are as follows.

Network Mask: Mask of the network where the interface that sends the Hello packet is located.

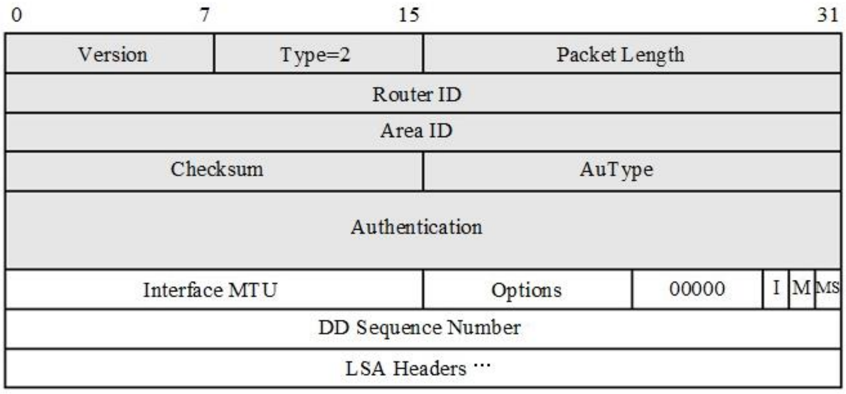
HelloInterval: Interval of Hello packet transmission. Two adjacent routers that have different Hello intervals cannot be neighbors.

Rtr Pri: The DR priority. If this field is 0, the router cannot be DR/BDR.

RouterDeadInterval: The failure time. If no Hello packet is received from the neighbor during this time, the neighbor fails. Two adjacent routers that have different failure times cannot be neighbors.

DD Packet

When two routers synchronize the database, the DD packet is used to describe their own LSDBs, including the header of each LSA in the LSDB (the header of LSA can identify an LSA uniquely). The LSA header occupies only a small data volume in the entire LSA, which reduces the protocol packet traffic between routers. The peer router determines whether it has this LSA according to the LSA header. The format of DD packet is shown in the figure below.



The meanings of the main fields are as follows.

Interface MTU: Without fragmentation, the longest IP packet length that can be sent by the interface.

I (Initial): When multiple DD packets are sent successively, the value of the first DD packet is 1; otherwise, the value is 0.

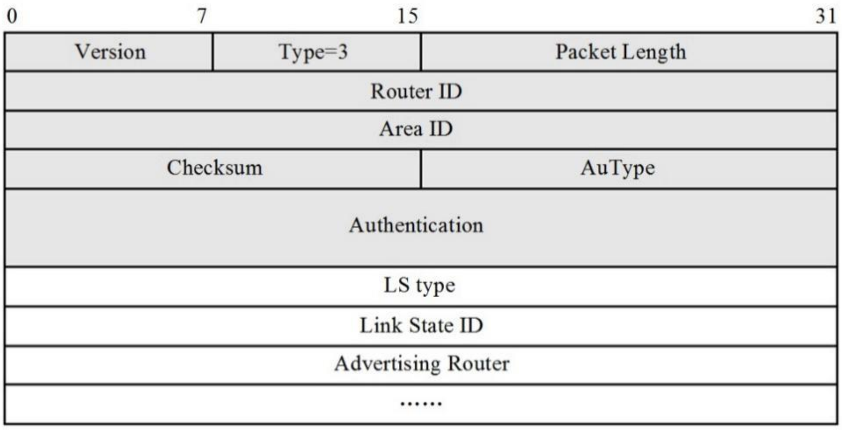
M (More): When multiple DD packets are sent successively, the value of the last DD packet is 0; otherwise, the value is 1, indicating there are other DD packets followed.

MS (Master/Slave): When two OSPF routers exchange DD packets, they determine the master-slave relationship first. The router with the greater router ID is the master. The value 1 indicates the sender is the master.

DD Sequence Number: DD packet SN. The starting SN is defined by the master. The SN increments by 1 each time a DD packet is transmitted. The slave confirms the transmission according to the SN of the master. The master and slave use the SN to guarantee the reliability and completeness of DD packet transmission.

LSR Packet

After two routers exchange the DD packet, they know which LSAs of the peer router do not exist in the local LSDB. In this case, the LSR packet is sent to request the required LSA from the peer. The request includes the abstract of the required LSA. The format of the LSR packet is as follows.



The meanings of the main fields are as follows.

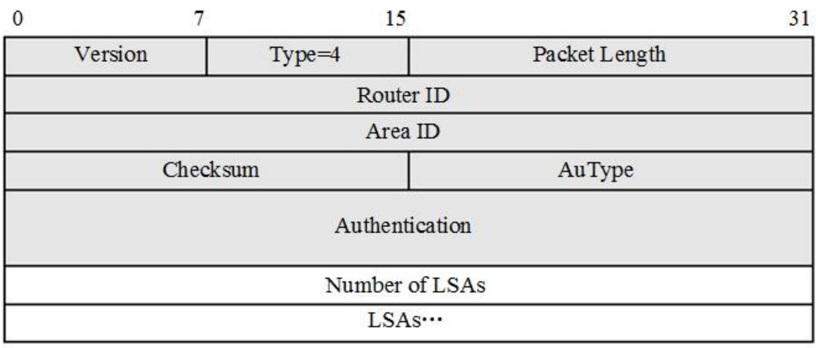
LS type: The LSA type. For example, type 1 indicates router LSA.

Link State ID: A field in the LSA header, depending on the LSA type.

Advertising Router: ID of the router that generates the LSA.

LSU Packet

The LSU packet is used to send a complete set of required LSAs to the peer router. The LSU packet format is shown in the figure below.



LSAck Packet

The LSAck packet is used to confirm the received LSU packet, including the header of LSA (one LSAck packet can confirm multiple LSAs). The LSU packet format is shown in the figure below.

0	7	15	31
Version	Type=5	Packet Length	
Router ID			
Area ID			
Checksum		AuType	
Authentication			
LSA Headers···			

LSA Header Format

All LSAs share the same header. The format is shown in the figure below.

0	7	15	31
LS Age		Options	LS Type
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	

The meanings of the main fields are as follows.

LS age: The duration of LSA generation (unit: seconds). The value of this field is constantly increasing no matter whether the LSA is transmitted on link or saved in LSDB.

LS type: The LSA type.

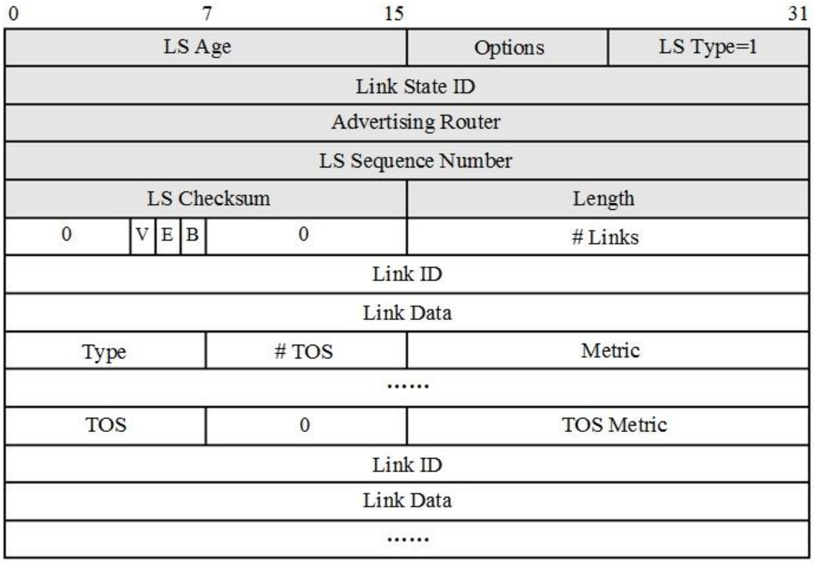
Link State ID: Its value depends on the LSA type.

LS sequence number: LSA sequence number, according to which other routers can determine which LSA is the latest one.

length: Total length of LSA, including the LSA header (unit: bytes).

Router LSA

The format of router LSA is shown in the figure below.



The meanings of the main fields are as follows.

Link State ID: ID of the router that generates the LSA first.

V (Virtual Link): If the router that generates the LSA is the end of the virtual connection, set this field to 1.

E (External): If the router that generates the LSA is an ASBR, set this field to 1.

B (Border): If the router that generates the LSA is an ABR, set this field to 1.

 # links: The amount of link information described in LSA, including all links and interfaces in a certain area on the router.

Network LSA

Network LSA is sent by the DR in the broadcast network or NBMA network. LSA records the IDs of all routers in the network, as shown in the following figure.

0 7	15	31
LS Age	Options	LS Type=2
Link State ID		
Advertising Router		
LS Sequence Number		
LS Checksum	Length	
Network Mask		
Attached Router		
......		

The meanings of the main fields are as follows.

Link State ID: Interface address of the DR router.

Network Mask: The mask of a broadcast network or NBMA network address.

Attached Router: IDs of all routers connected to the same network, including the router ID of DR.

Summary LSA

Type 3 LSA and type 4 LSA share the same format, and both are generated by ABR, as shown in the figure below.

0 7	15		31
LS Age		Options	LS Type=3 or 4
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	
Network Mask			
0	Metric		
TOS	TOS Metric		
......			

The meanings of the main fields are as follows.

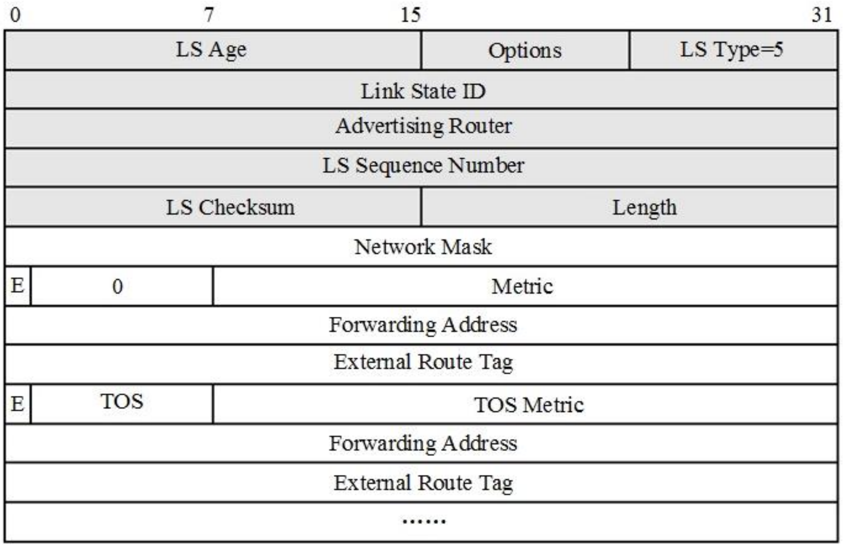
Link State ID: For type 3 LSA, this field is the advertised network address; for type 4 LSA, this field is the router ID of ASBR.

Network Mask: The network address mask of type 3 LSA. This field has no meaning for type 4 LSA, so set it to 0.0.0.0.

metric: Overhead of the route directed to the destination address.

AS-External LSA

Generated by ASBR, AS-External LSA describes the information of the route destined outside the AS, as shown in the figure below.



The meanings of the main fields are as follows.

Link State ID: Destination address outside of the AS to be advertised.

Network Mask: Mask of the destination address to be advertised.

E (External Metric): Type of the external metric value. Set this field to 1 for type 2 external route, and set this field to 0 for type 1 external route.

metric: Routing overhead.

Forwarding Address: The packets sent to the advertised destination address are forwarded to this address. The field is typically set to 0, indicating the advertising router is the next hop.

External Route Tag: Tag added to the external route. This field can be used for managing external routes. It is not used by OSPF.

NSSA external LSA

Generated by ASBR, NSSA external LSA can only be transmitted within the NSSA. Its format is same as that of AS-External LSA.

7.3.2 Configuring OSPF

7.3.2.1 Configuring Global OSPF

7.3.2.1.1 Enabling an OSPF Process

Purpose

This section describes how to enable and disable an OSPF process.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable the default OSPF process	1. Access the global configuration view. 2. Run the **router ospf** command.
Enable the designated OSPF process	1. Access the global configuration view. 2. Run the **router ospf** *process-id* command.
Disable the default OSPF process	1. Access the global configuration view. 2. Run the **no router ospf** command.
Disable the designated OSPF process	1. Access the global configuration view. 2. Run the **no router ospf** [*process-id*] command.
Disable all OSPF processes	1. Access the global configuration view. 2. Run the **no router ospf all** command.

7.3.2.1.2 Enabling the VPN Instance Designated by an OSPF Process

Purpose

This section describes how to enable the VPN instance designated by an OSPF process.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable the VPN instance designated by an OSPF process	1. Access the global configuration view. 2. Run the **router ospf** *process-id* **vpn-instance** *name* command.
Enable the VPN instance designated by the default OSPF process	1. Access the global configuration view. 2. Run the **router ospf vpn-instance** *name* command.

7.3.2.1.3 Resetting an OSPF Process

Purpose

This section describes how to reset an OSPF process.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Reset an OSPF process	1. Access the privileged user view. 2. Run the **reset ospf** command.
Reset the designated OSPF process	1. Access the privileged user view. 2. Run the **reset ospf** *process-id* command.

7.3.2.1.4 Clearing OSPF Statistics

Purpose

This section describes how to clear OSPF statistics.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Clear OSPF statistics	1. Access the privileged user view or OSPFv2 configuration view. 2. Run the **reset ospf counters** command.

7.3.2.2 Configuring an OSPF Node

7.3.2.2.1 Configuring a Router-id or Router ID

Purpose

This section describes how to configure a Router-id or router ID.

Background

By default, no Router-id or router ID is configured for the system, and the switch selects an interface IP address as its router ID.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the switch ID	1. Access the global configuration view. 2. Access the OSPFv2 configuration view, BGP-VPN IPv4 address family configuration view, or BGP-VPN IPv6 address family configuration view. 3. Run the **router-id** *ip-address* command.

7.3.2.2.2 Configuring an OSPF Interface

Purpose

This section describes how to configure an OSPF interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an OSPF interface and area	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **network** *network-address network-mask* **area** *area-id* command.
Delete an OSPF interface	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no network** *network-address network-mask* **area** *area-id* command.

7.3.2.2.3 Configuring a Stub Area

Purpose

This section describes how to configure a stub area.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a common stub area	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **stub** command.
Configure a total stub area	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **stub no-summary** command.
Configure the overhead of the default summary LSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **default-cost** { *cost* | **default** } command.
Delete a stub area	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no area** *area-id* **stub** command.
Configure a stub router	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **stub router** command.
Configure a stub router and set the interval during which a device acts as a stub router when it is restarted or faulty	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **stub router on-startup** [*on-startup-time* | **default**] command.
Delete a stub router	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no stub router** command.

7.3.2.2.4 Configuring an NSSA

Purpose

This section describes how to configure an NSSA.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **nssa** command.
Configure the default LSA overhead of an NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **nssa default-cost** { *cost-value* | **default** } command.
Configure the no summary NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **nssa no-summary** command.
Configure aggregation advertising/no advertising for an NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **nssa range** *dst-network dst-mask* { **advertise** | **no-advertise** } command.
Configure the designated conversion router or candidate conversion router for an NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **nssa translator { always | candidate }** command.
Delete an NSSA	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no area** *area-id* **nssa** command.
Delete NSSA aggregation	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no area** *area-id* **nssa range** *dst-address/dst-mask* command.

7.3.2.2.5 Configuring Area Aggregation

Purpose

This section describes how to configure area aggregation.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure area aggregation	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **no-advertise** } command.
Delete area aggregation	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no area** *area-id* **range** *dst-address dst-mask* command.

7.3.2.2.6 Configuring a Routing Protocol Filter Policy

Purpose

This section describes how to configure a routing protocol filter policy.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a routing protocol filter policy	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **filter route-policy** *route-policy-name* command.
Cancel a routing protocol filter policy	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no filter route-policy** *route-policy-name* command.

7.3.2.2.7 Enabling the FRR Function

Purpose

This section describes how to enable fast route redistribution (FRR).

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable FRR	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **frr** { **enable | disable**} command.

7.3.2.2.8 Configuring GR

Purpose

This section describes how to configure graceful restart (GR).

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable GR	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **graceful-restart** command.
Configure a GR period	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **graceful-restart period** *restart-time* command.
Enable the GR helper	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run **the graceful-restart helper** command.
Disable GR	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no graceful-restart** command.
Disable the GR helper	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no graceful-restart helper** command.

Purpose	Procedure
Implement GR	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **graceful-restart begin** command.

7.3.2.2.9 Enabling the Opaque Function

Purpose

This section describes how to enable the opaque function.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the opaque function	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run **the opaque** { **enable | disable**} command.

7.3.2.2.10 Configuring an Interval for Route Calculation

Purpose

This section describes how to configure an interval of route calculation.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an interval for route calculation	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **spf-running-interval** { *interval* | **default** } command.

7.3.2.2.11 Configuring OSPF TTL

Purpose

This section describes how to configure OSPF TTL.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set a valid TTL value of OSPF	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **valid-ttl-hops** { *hops-number* | **default** } command.

7.3.2.2.12 Configuring OSPF Redistribution

Purpose

This section describes how to configure OSPF redistribution.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure OSPF redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run **the redistribute { static | connect | rip | bgp | isis | ospf }** command.
Disable OSPF redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no redistribute { static | connect | rip | bgp | isis | ospf }** command.
Delete redistribution of the designated network	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the following commands: ● **no redistribute { static | connect | bgp }** *dst-address dst-mask*

Purpose	Procedure
	● **no redistribute { rip | ospf | isis }** *process-id dst-address dst-mask*
Configure a routing policy of redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **redistribute { static | connect | rip | bgp | isis | ospf } route-policy** *policy-name* command.
Delete a routing policy of redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no redistribute { static |connect | rip | bgp | isis | ospf } route-policy** *policy-name* command.
Configure the redistribution overhead	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the following commands: ● **redistribute { connect | static | bgp } metric** *router-cost* type *cost-type* ● **redistribute { rip | ospf | isis }** *process-id* **metric** *router-cost* type *cost-type*
Configure the overhead of the network to be redistributed	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the following commands: ● **redistribute** { **connect** | **static** | **bgp** } *dst-network network-mask* **metric** *router-cost* **type** *cost-type* ● **redistribute** { **rip** | **ospf** | **isis** } *process-id dst-network network-mask* **metric** *router-cost* **type** *cost-type*
Configure the translate bit of redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the following commands: ● **redistribute { connect | static | bgp }** *dst-network network-mask* **{ translate | no-translate }** ● **redistribute { rip | ospf | isis }** *process-id dst-network network-mask* **{ translate | no-translate }**
Configure rejection of the specific external route	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the following commands: ● **redistribute { connect | static | bgp }** *dst-network network-mask* **{ not-advertise | advertise }** ● **redistribute { rip | ospf | isis }** *process-id dst-network network-mask* **{ not-advertise | advertise }**

Purpose	Procedure
Set to redistribute routes	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **redistribute { rip | isis | ospf }** *process-id* command.
Cancel route redistribution	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no redistribute { rip | isis | ospf }** *process-id* command.

7.3.2.2.13 Enabling the Trap Report Function of OSPF

Purpose

This section describes how to enable the trap report function of OSPF.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable the trap report function of OSPF	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **snmp-trap { enable | disable }** command.
Enable or disable the detailed trap report function of OSPF	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the command **snmp-trap { enable | disable } trap-name { ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange | ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa | ospfnbrrestarthelperstatuschange | ospfnbrstatechange | ospfnssatranslatorstatuschange | ospforiginatelsa | ospfrestartstatuschange | ospftxretransmit | ospfvirtifauthfailure | ospfvirtifconfigerror | ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit | ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange }.**

7.3.2.2.14 Configuring a Reference Bandwidth of OSPF Overhead

Purpose

This section describes how to configure a reference bandwidth of OSPF overhead.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a reference bandwidth of OSPF overhead	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **bandwidth-reference** { *bandwidth* | **default** } command.

7.3.2.2.15 Configuring Compatibility with RFC1583

Purpose

This section describes how to configure compatibility with RFC1583.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure compatibility with RFC1583	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **rfc1583 compatible { enable | disable }** command.

7.3.2.2.16 Configuring Default Route Advertisement

Purpose

This section describes how to configure default route advertisement.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure default route advertisement	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **default-route-advertise always** command.
Cancel default route advertisement	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **no default-route-advertise** command.

7.3.2.3 Configuring an OSPF Interface

7.3.2.3.1 Configuring OSPF Interface Parameters

Purpose

This section describes how to configure the parameters of an OSPF interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the type of an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf if-type { broadcast | p2p | nbma | p2multip }** command.
Configure the priority of an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **ip ospf priority** { *priority* | **default** } command.
Configure the overhead of an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf cost** { *cost* | **default** } command.
Configure an interval for sending Hello packets by an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **ip ospf hello-interval** *hello-interval* ● **ip ospf hello-interval default**
Configure the neighbor timeout	1. Access the global configuration view.

Purpose	Procedure
time of an OSPF interface	2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **ip ospf dead-interval** *interval* ● **ip ospf dead-interval default**
Configure the retransmission interval of an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf retransmit-interval** { *retransmit-interval-time* | **default** } command.
Configure the transmission delay of an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf transmit-delay** { *transmit-delay-time* | **default** } command.
Configure the interval of polling packet transmission	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf poll-interval** { *poll-interval-time* | **default** } command.
Configure simple password authentication for an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf authentication simple-password** *key-value* command.
Configure MD5 authentication for an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf authentication md5** *key-id md5-key* command.
Clear the authentication configuration of an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **no ip ospf authentication** command.
Specify a slave IPv4 address as the source IPv4 address	1. Access the VLANIF configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, loopback interface configuration view, BD interface configuration view, Ethernet routing interface configuration view, or GRP routing interface configuration view. 2. Run the **ip ospf source sub-address** *ipv4-address command.*
Cancel using a slave IPv4	1. Access the VLANIF configuration view, Ethernet sub-interface configuration view, Trunk sub-interface configuration view, loopback interface

Purpose	Procedure
address as the source IPv4 address	configuration view, BD interface configuration view, Ethernet routing interface configuration view, or GRP routing interface configuration view. 2. Run the **no ip ospf source sub-address** command.

7.3.2.3.2 Configuring BFD

Purpose

This section describes how to configure BFD.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure BFD	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run **ip ospf bfd { enable | disable }** command.

7.3.2.3.3 Configuring an MTU Value for an OSPF Interface

Purpose

This section describes how to configure an MTU value for an OSPF interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an MTU value for an OSPF interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **ip ospf mtu** { *mtu* | **default** } command.
Configure MTU detection	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view.

Purpose	Procedure
	3. Run the **ip ospf mtu-ignore { enable | disable }** command.

7.3.2.3.4 Configuring a Passive Interface

Purpose

This section describes how to configure a passive interface.

Background

A passive interface refers to an OSPF interface that does not send or receive protocol messages and does not establish any neighbor relation. However, the interface route is included in the Router LSA for internal route propagation. It can be used for the stub route.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a passive interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip ospf passive-interface** command.

7.3.2.4 Viewing OSPF Configuration

Purpose

This section describes how to view the OSPF configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the brief OSPF information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf brief** ● **show ip ospf brief process** *process*
Display the OSPF configuration	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the **show ip ospf config** command.
Display the OSPF interface information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf interface** ● **show ip ospf interface** *ip-address* ● **show ip ospf interface count** ● **show ip ospf interface process** *process*
Display the OSPF neighbor information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf neighbor** ● **show ip ospf neighbor** *ip-address* ● **show ip ospf neighbor process** *process* ● **show ip ospf neighbor state statistic** ● **show ip ospf neighbor state count**

Purpose	Procedure
Display the OSPF area information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf area** ● **show ip ospf area (A.B.C.D)** ● **show ip ospf area** *area-id* ● **show ip ospf area process** *process*
Display the OSPF database information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf database** ● **show ip ospf database area** *area-id* ● **show ip ospf database area** *area-id* **process** ***process*** ● **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id adverrouter-id* ● **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id adverrouter-id process* ● **show ip ospf database { include | exclude | begin } substring** *string* ● **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 }** ● **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 } process** *process* ● **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id adverrouter-id area-id* ● **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id adverrouter-id area-id process* ● **show ip ospf database age** *min-age max-age* ● **show ip ospf database age** *min-age max-age* **count** ● **show ip ospf database count** ● **show ip ospf database count process** *process* ● **show ip ospf database expire**

Purpose	Procedure
	● **show ip ospf database expire { include | exclude | begin } substring** *string* ● **show ip ospf database expire count** ● **show ip ospf database expire process** *process* ● **show ip ospf database expire process** *process* **{ include | exclude | begin } substring** *string* ● **show ip ospf database process** *process* ● **show ip ospf database process** *process* **{ include | exclude | begin } substring** *string* ● **show ip ospf database total count**
Display the OSPF routing information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the following commands: ● **show ip ospf route** ● **show ip ospf route count** ● **show ip ospf route count process** *process* ● **show ip ospf route process** *process* ● **show ip ospf route total count**
Display the OSPF BFD information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the s**how ip ospf bfd session** command.
Display the OSPF trap information	1. Access the privileged user view, global configuration view, common user view, OSPFv2 routing configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the **show ip ospf trap** command.
Display the OSPF BFD session information	1. Access the common user view, privileged user view, global configuration view, OSPFv2 route configuration view, VLANIF configuration view, or loopback interface configuration view. 2. Run the **show ip ospf bfd session** command.

7.3.3 OSPF Configuration Example

7.3.3.1 Example of Configuring Basic OSPF Functions

Network Requirements

As shown in Figure 7-4, all devices run OSPF and the AS is divided into 3 areas.

Switch_1 and Switch_2 are ABRs for transmitting routes among areas.

After configuration, each router can learn the routes destined for all network segments in the AS.

Network Diagram

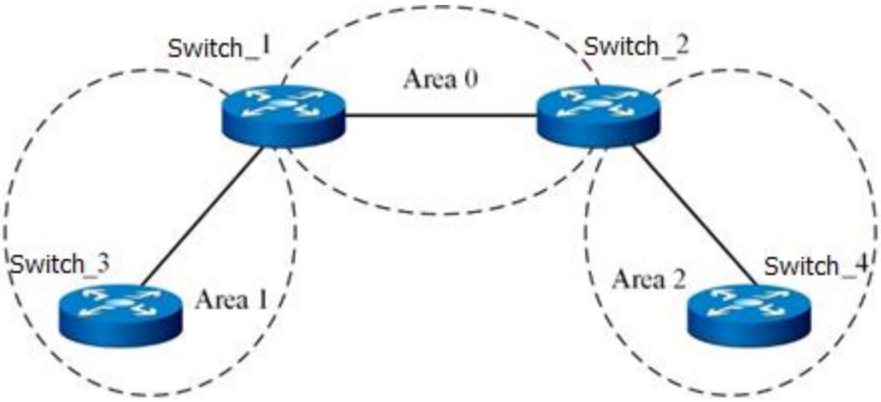


Figure 7-4 Network diagram of basic OSPF configuration

Configuration Data

Interface addresses of Switch_1: 1.1.1.1/24 and 3.1.1.1/24

Interface addresses of Switch_2: 1.1.1.2/24 and 4.1.1.2/24

Interface address of Switch_3: 3.1.1.3/24

Interface address of Switch_4: 4.1.1.4/24

Configuration

Switch_1:

```
Switch_1(config)#router ospf
Switch_1(config-ospf-1)#router-id 1.1.1.1
Switch_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Switch_1(config)#
```

Switch_2:

```
Switch_2(config)#router ospf
Switch_2(config-ospf-1)#router-id 1.1.1.2
```

Switch_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Switch_2(config)#
Switch_3:
Switch_3(config)#router ospf
Switch_3(config-ospf-1)#router-id 3.1.1.3
Switch_3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Switch_3(config)#
Switch_4:
Switch_4(config)#router ospf
Switch_4(config-ospf-1)#router-id 4.1.1.4
Switch_4(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Switch_4(config)#

Configuration Verification

Run the **show ip ospf neighbor** command to view the following OSPF information:

OSPF Process 1

IpAddress	NeighborID	Option	Priority	State	Event	Aging
1.1.1.2	1.1.1.2	2	1	full	6	39
3.1.1.3	3.1.1.3	2	1	full	6	30

Run the **show ip ospf database** command to view the following OSPF information:

Database of OSPF Process 1

Router LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	146	0x80000003	0xdbff	36
1.1.1.2	1.1.1.2	147	0x80000003	0xd9fe	36

Network LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.2	1.1.1.2	147	0x80000001	0x83c3	32

SummaryNetwork LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.0	1.1.1.1	146	0x80000002	0xf8f5	28
4.1.1.0	1.1.1.2	138	0x80000001	0xe706	28

Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	147	0x80000002	0xccb	36
3.1.1.3	3.1.1.3	139	0x80000004	0xd66c	48

Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	147	0x80000001	0x5fde	32

SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	187	0x80000001	0x15dc	28
4.1.1.0	1.1.1.1	136	0x80000002	0xd7b1	28

Run the **show ip ospf route** command to check the following OSPF information:

OSPF Instance 1

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	1.1.1.2	ABR	INTRA	0
1.1.1.0	255.255.255.0	1.1.1.1	Network	INTRA	
3.1.1.0	255.255.255.0	3.1.1.1	Network	INTRA	
4.1.1.0	255.255.255.0	1.1.1.2	Network	INTER	

7.3.3.2 Configuring an OSPF Stub Area

Network Requirements

As shown in Figure 7-5, all devices run OSPF. The AS is divided into 3 areas. Switch_1 and Switch_2 are ABRs that transmit the routes between areas.

After configuration, each device can learn the routes destined for all network segments in the AS.

Network Diagram

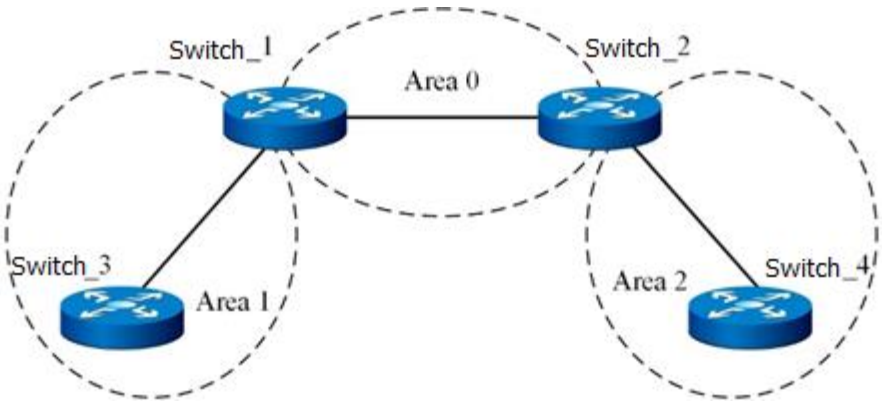


Figure 7-5 OSPF stub area network diagram

Configuration

The basic configuration and topology are the same as those described in 7.3.3.1 Example of Configuring Basic OSPF Functions.

Configure Area 1 as a stub area.

Switch_1:

Switch_1(config)#router ospf

Switch_1(config-ospf-1)#area 1 stub

Switch_1(config)#

Switch_3:

Switch_3(config)#router ospf

Switch_3(config-ospf-1)# area 1 stub

Switch_3(config)#

Introduce a type 5 LSA with the address 100.1.1.1 to Switch_4

Configuration Verification

1. When the area of Switch_3 is a normal area, the routing table contains routes outside of the AS. After the area is configured as a stub area, it has a default type 3 LSA, which is absent from normal areas. No LSA outside of the AS is displayed.

Switch_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
100.1.1.0	255.255.255.0	1.1.1.2	Network	ASE	

2. After the area of Switch_3 is configured as a stub area, no route outside of the AS is displayed, but a default route destined outside the area is displayed.

Switch_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Network	INTER	
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	

7.3.3.3 Configuring OSPF NSSA

Network Requirements

As shown in Figure 7-6, all devices run OSPF. The AS is divided into 3 areas. Switch_1 and Switch_2 are ABRs that transmit the routes between areas.
After configuration, each device can learn the routes destined for all network segments in the AS.

Network Diagram

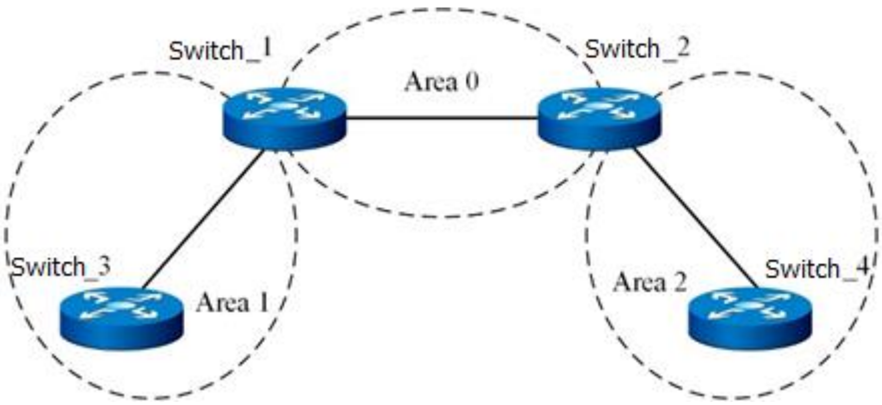


Figure 7-6OSPF NSSA network diagram

Configuration

The basic configuration and topology are the same as those described in 7.3.3.1 Example of Configuring Basic OSPF Functions.
Configure Area 1 as NSSA.
Switch_1:
Switch_1(config)#router ospf
Switch_1(config-ospf-1)#area 1 nssa
Switch_1(config)#
Switch_3:
Switch_3(config)#router ospf
Switch_3(config-ospf-1)# area 1 nssa
Switch_3(config)#

Configuration Verification

1. The database of NSSA has a default LSA of the NSSA type, which is absent from the databases of normal areas.

Switch_3(config-ospf-1)#show ip ospf database

Database of OSPF Process 1

Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	134	0x80000002	0x9934	36
3.1.1.3	3.1.1.3	133	0x80000002	0x6066	36

Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	133	0x80000001	0xe64f	32

SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	178	0x80000001	0x9c4d	28
4.1.1.0	1.1.1.1	178	0x80000001	0x6121	28

NSSA LSA (Area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	178	0x80000001	0xc608	36

2. Import the static route IP address route-static 100.1.1.0 255.255.255.0 3.1.1.1 of interface 100.1.1.1 to Switch_3, and redistribute static routes.

Database:

NSSA LSA (Area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	374	0x80000001	0x7550	36
100.1.1.0	3.1.1.3	0	0x80000001	0x70c4	36

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	1	0x80000001	0xe656	36

Route:

Switch_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.1	255.255.255.255	3.1.1.1	ASBR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Network	ASE2	
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	

3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER

View the following on Switch_4

Database:

Switch_4#

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	412	0x80000001	0x4701	36

Route:

Switch_4# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	4.1.1.2	ABR	INTRA	2
1.1.1.0	255.255.255.0	4.1.1.2	Network	INTER	
3.1.1.0	255.255.255.0	4.1.1.2	Network	INTER	
4.1.1.0	255.255.255.0	4.1.1.4	Network	INTRA	
100.1.1.0	255.255.255.0	4.1.1.2	Network	ASE	

3. Import the static route 200.1.1.1 to Switch_4 and check whether Switch_4 has any external route.

View the database on Switch_4

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	823	0x80000001	0x4701	36
200.1.1.0	4.1.1.4	4	0x80000001	0xb933	36

View the database on Switch_3

Switch_3

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	836	0x80000001	0xe656	36

The external route 200.1.1.0 does not exist.

7.3.3.4 Configuring Redistribution

Network Requirements

As shown in Figure 7-7, two routers run OSPF and are located in Area 0. Assume that Switch_1 needs to import external routes to OSPF. The following requirements are posed on external route import:

1. Receive all direct routes and adopt the default configuration.

2. Receive all static routes and configure overhead 2000 and type 2 for the routes, and configure overhead 100 for the static routes from 10.1.1.0/24.

3. Reject RIP routes from 20.1.1.0/24 and aggregate RIP routes from 30.1.0.0/16.

After configuration, each device can learn the routes destined for all network segments in the AS.

Network Diagram

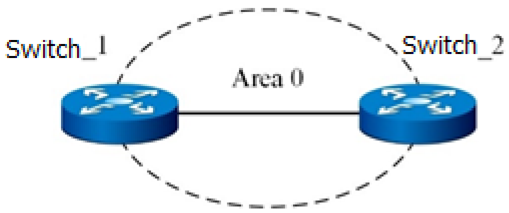


Figure 7-7 OSPF redistribution network diagram

Configuration

1. Basic Configuration

Switch_1:
Switch_1(config)#router ospf
Switch_1(config-ospf-1)#router-id 1.1.1.1
Switch_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Switch_1(config)#
Switch_2:
Switch_2(config)#router ospf
Switch_2(config-ospf-1)#router-id 1.1.1.2
Switch_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Switch_2(config)#

2. Configure redistribution.

```
Switch_2(config-ospf-1)#redistribute connected
Switch_2(config-ospf-1)#redistribute static metric 2000 type 2
Switch_2(config-ospf-1)#redistribute static 10.1.1.0 255.255.255.0    metric 100 type 2
Switch_2(config-ospf-1)#redistribute static
Switch_2(config-ospf-1)#redistribute rip 20.1.1.0 255.255.255.0 not-advertise
Switch_2(config-ospf-1)#redistribute rip
```

Configuration Verification

After configuration is complete, check the database of A to determine whether the imported external LSA meets requirements.

7.3.3.5 Configuring Aggregation

Network Requirements

The network requirements are shown in Figure 7-8:

- Area 1 contains intra-area routes 10.1.1.0/24, 10.1.2.0/24, 20.1.1.0/24, and 20.1.2.0/24. It is required to aggregate 10.1.1.0/24 and 10.1.2.0/24 into 10.1.0.0/16 to be advertised, and not to import 20.1.1.0/24 and 20.1.2.0/24 into other areas.
- Devices in Area 2 have relatively low capabilities and cannot receive many external routes. It is required to advertise external route 30.1.1.0/24 in this area to other areas.
- Area 3 is similar to Area 2 but does not have external routes to be advertised.

Based on the preceding requirements, configure an aggregation entry and a filter entry for Area 1; configure the NSSA attribute for Area 2; and configure the stub attribute for Area 3.

Network Diagram

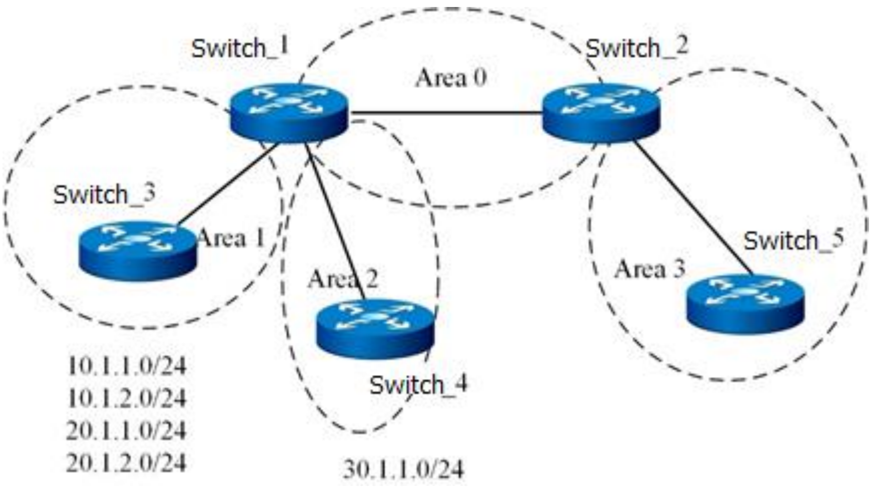


Figure 7-8 OSPF aggregation network diagram

Configuration

For basic OSPF configuration, see 7.3.3.1 Example of Configuring Basic OSPF Functions.
Switch_1:

Switch_1(config-ospf-1)#area 1 range 10.1.0.0 255.255.0.0 advertise

Switch_1(config-ospf-1)#area 1 range 20.1.0.0 255.255.0.0 no-advertise

Switch_1(config-ospf-1)#area 2 nssa

Configure all routers of Area 2 in such way.

Switch_2:

Switch_2(config-ospf-1)#area 3 stub

or

Switch_2(config-ospf-1)#area 3 stub no-summary

Configuration Verification

After configuration is complete, check the database to determine whether the following conditions are met:

1. Area 0 contains summary LSA 10.1.0.0/16.
2. Area 0 does not contain summary LSAs 10.1.1.0, 10.1.2.0, 20.1.1.0, and 20.1.2.0.
3. Area 0 contains type 5 LSA 30.1.1.0/16.
4. Area 2 contains type 7 LSA 30.1.1.0/16.
5. Area 2 contains LSA 0.0.0.0/0.
6. Area 3 contains summary LSA 0.0.0.0/0.
7. If **nosummary** is not specified for Area 3, Area 3 contains summary LSA 10.1.0.0/16; if **nosummary** is specified for Area 3, Area 3 does not contain summary LSA 10.1.0.0/16.

7.3.3.6 Configuring an Authentication Mode

Network Requirements

The configuration requirements are shown in Figure 7-9:

1. Implement simple password authentication between Switch_1 and Switch_2, and set the password to **test**.

2. Establish a virtual link between Switch_1 and Switch_4, implement MD5 authentication between the two routers, and set the password to **aaa** and ID to **100**.

3. Implement MD5 authentication between Switch_2 and Switch_3, and set the password to **ccc** and the ID to **110**.

Network Diagram

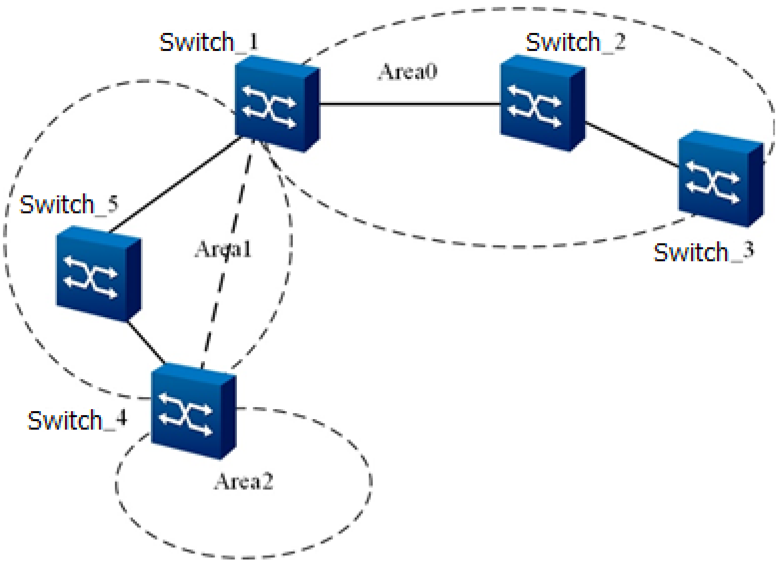


Figure 7-9 OSPF authentication mode network diagram

Configuration

For basic OSPF configuration, see 7.3.3.1 Example of Configuring Basic OSPF Functions.

Switch_1:

Switch_1(config)#interface vlan 1

Switch_1(config-vlan-1)#ip ospf authentication simple-password test

Switch_1(config-vlan-1)#exit

Switch_1(config)#router ospf

Switch_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 authentication md5 aaa 100

Switch_2:

Switch_2(config)#interface vlan 1

Switch_2(config-vlan-1)#ip ospf authentication simple-password test

Switch_2(config-vlan-1)#exit

Switch_2(config)#interface vlan 2

Switch_2(config-vlan-1)#ip ospf authentication md5 110 ccc

Switch_2(config-vlan-1)#exit

Switch_3:

Switch_3(config-vlan-1)#router ospf

Switch_3(config-ospf-1)#area 0 authentication md5 110 ccc

Switch_4:

Switch_4(config)#router ospf

Switch_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 authentication md5 aaa 100

Configuration Verification

After configuration is complete, check that the neighbor relationship is normal.

7.3.3.7 Configuring BFD

Network Requirements

As shown in Figure 7-10, two routers run OSPF and are located in Area 0.

Network Diagram

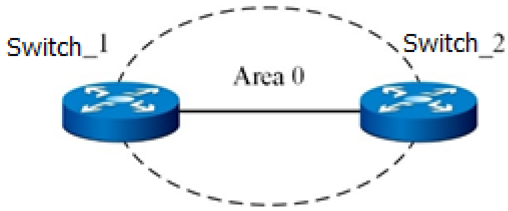


Figure 7-10 OSPF BFD network diagram

Configuration

1. For basic OSPF configuration, see 7.3.3.1 Example of Configuring Basic OSPF Functions.

2. BFD configuration

Switch_1:

Switch_1(config)#interface vlan 4

Switch_1(config-vlan-4)#bfd enable

Switch_1(config-vlan-4)#ip ospf bfd enable

Switch_2:

Switch_2(config)#interface vlan 4

Switch_2(config-vlan-4)#bfd enable

Switch_2(config-vlan-4)#ip ospf bfd enable

Configuration Verification

```
Switch_1(config-vlan-4)#show ip ospf bfd session
 OSPF Process 1
 NeighborAddress      NeighborID          BFDState
 1.1.1.2              1.1.1.2             UP
Switch_2(config-vlan-4)#show ip ospf bfd session
 OSPF Process 1
 NeighborAddress      NeighborID          BFDState
 1.1.1.1              1.1.1.1             UP
```

7.3.3.8 Configuring GR

Network Requirements

As shown in Figure 7-11, two routers run OSPF and are located in Area 0.

Two devices are required by GR testing. One device is GR initiator and the other is GR helper. Testing on the GR initiator uses dual core switch cards and the plugging/unplugging method. There is no limit on the GR helper.

Network Diagram

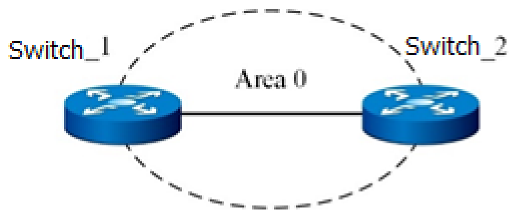


Figure 7-11 OSPF GR network diagram

Configuration

1. For basic OSPF configuration, see 7.3.3.1 Example of Configuring Basic OSPF Functions.
2. GR configuration

Switch_1:

Switch_1(config)#router ospf

Switch_1(config-ospf-1)# graceful-restart

Switch_1(config-ospf-1)# graceful-restart period 60

Switch_2:

Switch_2(config)#router ospf

Switch_2(config-ospf-1)# graceful-restart helper

Configuration Verification

Use the plugging/unplugging method for testing. After the GR initiator and GR helper are configured, unplug the active core switch card of the GR initiator and check that the original traffic between the devices is not interrupted.

7.4 Configuring OSPFv3

7.4.1 OSPFv3 Overview

7.4.1.1 Basic OSPFv3 Concepts

OSPFv3 runs inside an AS. To reduce the routing information size, OSPFv3 divides an AS into different areas. Each area is marked by an area ID, which is in the format of IPv4 address here. Figure 7-12 shows an example of area division.

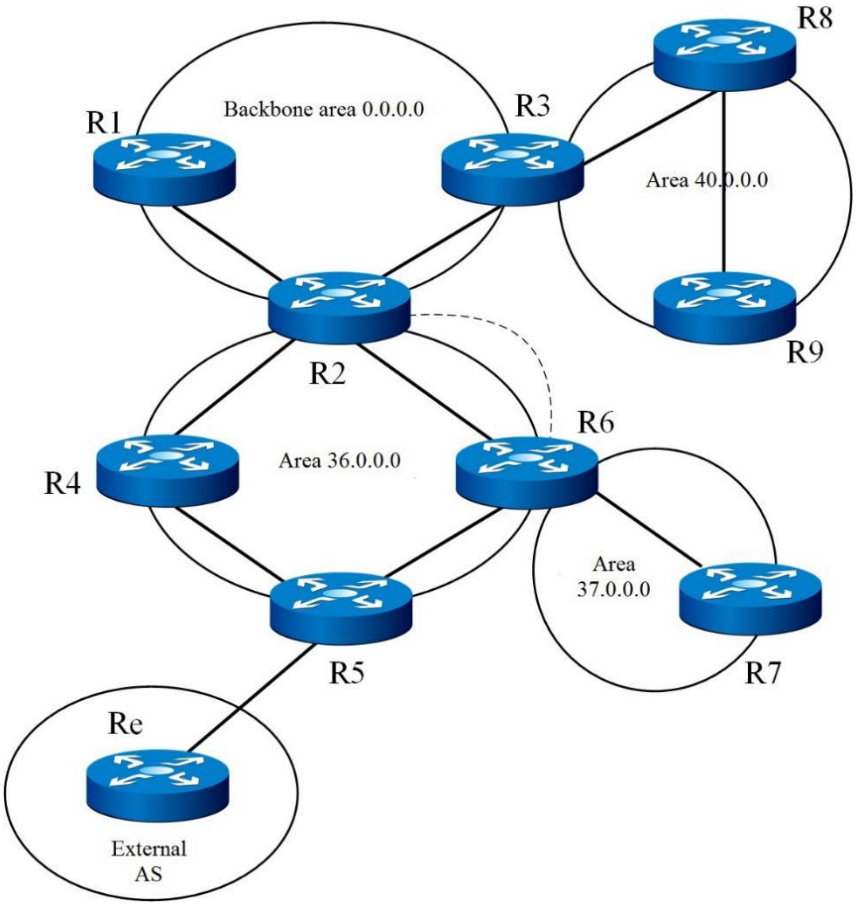


Figure 7-12 OSPFv3 area division

In Figure 7-12, an AS is divided into 4 areas. Some interfaces of R1, R2, and R3 are in the backbone area 0.0.0.0. Some interfaces of R2, R4, R5, and R6 are in the area 36.0.0.0. Some interfaces of R6 and R7 are in the area 37.0.0.0. R3, R8 and R9 form the area 40.0.0.0.

In OSPFv3, the area 0.0.0.0 (an area whose ID is 0.0.0.0, same below) is a special area called as backbone area. To ensure normal operation of OSPFv3, the backbone area must be consecutive. If the backbone area is isolated (some links in the backbone area fail), route calculation cannot be performed.

Other areas must connect with the backbone area. As shown in Figure 7-12, area 36.0.0.0 and area 40.0.0.0 connect with the backbone area through R2 and R3 respectively. In this way, each of R2 and R3 is connected to two areas. In OSPFv3, routers connected to two or more areas are called ABRs. Figure 7-12Router R6 connects with area 36.0.0.0 and area 37.0.0.0, and thus is an ABR. However, area 37.0.0.0 is not connected to the backbone area, causing route loss. To solve this problem, OSPFv3 provides the concept virtual link, which is designated between two routers and belongs to the backbone area. As shown in Figure 7-12, a virtual link is created between R2 and R6. Then, R6 connects three areas: 36.0.0.0, 37.0.0.0, and backbone area. In this way, a connection is created between area 37.0.0.0 and the backbone area. Since this virtual link is created through area 36.0.0.0, area 36.0.0.0 is called as the transmit area of the virtual link.

As shown in Figure 7-12, there is only one link between area 37.0.0.0 and the backbone area, while there are two links between area 36.0.0.0 and the backbone area. In OSPFv3, areas with only one connection to the backbone area can be configured as a stub area to reduce the routing information size. Note that, even there is only one link between area 36.0.0.0 and the backbone area, area 36.0.0.0 cannot be configured as a stub area, because it has served as a transmit area for a virtual link. Stub areas cannot serve as transmit areas.

OSPFv3 runs inside an AS and thus route exchange with other ASs is involved. As shown in Figure 7-12, R5 connects to routers in other ASs and can be called as ASBR. Interaction with routes of other ASs is often performed via BGP.

Each router in OSPFv3 has a router ID which uniquely identifies the router. The router ID is in the format of IPv4 address specified by users. 0.0.0.0 is reserved.

OSPFv3 provides two concepts: neighbor and adjacency. Neighbors are routers that other routers can reach directly through an interface, while adjacencies are logical entities that can exchange protocol messages via OSPFv3. For P2P links (including virtual links), the other end of the links has only one neighbor, and therefore only one adjacency. This is not the case for most of Ethernet broadcast links. A link may have multiple routers. To reduce routing information, OSPFv3 defines Designated Router (DR) and Backup Designated Router (BDR). All routers can only establish adjacency relationship with DR and BDR, while network route is advertised by DR, and BDR replaces the original DR when the DR fails. Figure 7-13 shows an example. Four routers form neighbors on the Ethernet link, where R1 is the DR and R2 is the BDR. The dotted line in the figure represents the actual adjacency relationship. It can be seen that there is no adjacency relationship between R3 and R4. The DR and BDR in OSPFv3 are automatically selected by the protocol process. If you want an interface to become the DR, you can manually specify the DR priority of this interface.

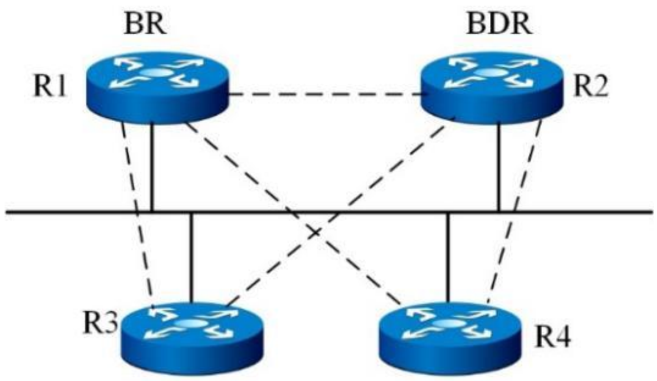


Figure 7-13 Adjacency relationship on an Ethernet link

7.4.1.2 Route Diffusion

The work of OSPFv3 is basically divided into the adjacency establishment process and the subsequent triggered update process. OSPFv3 uses five types of protocol messages to accomplish protocol functions: Hello message, DDP message, LSR message, LACK message, and LSU message. The Hello message checks the status of a neighbor and negotiates adjacency establishment parameters and selection or DR and BDR. The DDP message sends the abstract of route information maintained by a router to its neighbor during OSPFv3 adjacency establishment. The neighbor compares the route information in the DDP message with the route information it maintains and decides which route information to request from its neighbor. Then, the neighbor can send an LSR message to request the corresponding route information. After receiving the request, the router sends an LSU message to advertise the detailed route information. The LACK message is used to acknowledge an LSU message. Acknowledging is necessary because the routing protocol is based on IP, a protocol that does not guarantee arrival. LSU message and LACK message are also used in route change advertisement after an adjacency is established. Figure 7-14 shows the flowchart.

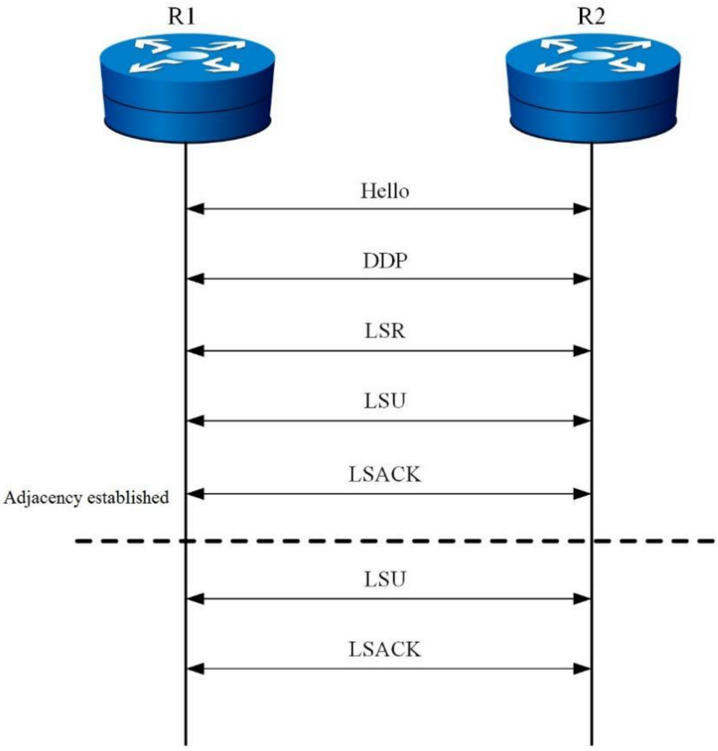


Figure 7-14 Work process of OSPFv3

All OSPFv3 messages except for the Hello message are related to the route information. In OSPFv3, an information unit carrying the route information is called link state advertisement (LSA). There are seven types of LSA: router LSA, network LSA, intra-area prefix LSA, intra-area router LSA, external LSA, link state LSA, and inter-area prefix LSA. These LSAs have different meanings, allowing for flexible route calculation. The external LSA is for the whole AS and does not belong to any area. All other LSAs belong to a specific area. Upon completion of LSA diffusion, routers can perform route calculation and the results are the entries in the route forwarding table.

7.4.1.3 OSPFv3 LSA Types

Router-LSAs

The frame format of Router-LSA is shown in Figure 7-15:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age              |0|0|1|         1               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Advertising Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    LS Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  0  |Nt|x|V|E|B|            Options                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |       0       |          Metric               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Interface ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Neighbor Interface ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Neighbor Router ID                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |       0       |          Metric               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Interface ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Neighbor Interface ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Neighbor Router ID                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             ...                               |
```

Figure 7-15 Frame format of Router-LSA

Differences with OSPFv2:

1. Meaning of the LSID field. OSPFv3 takes fragmentation into consideration. One router can generate one or more Router-LSAs for one area and distinguish these Router-LSAs by LSID. This can avoid the generation of large packets in OSPFv2 due to too many interfaces in the area, resulting in underlying IP fragmentation.

The number of links that a Router-LSA can contain can be designed as (interface MTU - IP header length 40 - LSA header length 16 - Router-LSA header length 24)/Each link length 16 = (1500 - 40 - 20 - 24)/16=88.

Assume that the interface MTU value is 1500.

2. Router-LSA does not contain interfaces in down or loopback state and interfaces without FULL adjacency. In OSPFv3, only interfaces with FULL adjacency can be contained in Router-LSA, while OSPFv2 has no such restriction.

3. When a transit link is added to Router-LSA for broadcast and NBMA links, the neighbor adjacency ID is the interface ID of DR, and the neighbor router ID is the router ID of DR.

Network-LSAs

The frame format of Network-LSA is shown in Figure 7-16 (the advertised overhead is 0):

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age            |0|0|1|          2                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Link State ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Advertising Router                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     LS Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         LS Checksum           |           Length              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0        |                  Options                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Attached Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             ...                               |
```

Figure 7-16 Frame format of Network-LSA

Network-LSA is generated in the same way as that in OSPFv2 but has the following changes:

1. LSID is the interface ID of DR. In OSPFv2, LSID is the interface address of DR.
2. It does not contain the mask and has no Net Mask field.
3. The option field is the logic OR of the option in LINKLSA advertised by the FULL neighbor.

Inter-Area-Prefix-LSAs

The frame format of Inter-Area-Prefix-LSA is shown in Figure 7-17:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age              |0|0|1|          3              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Advertising Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    LS Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |                  Metric                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| PrefixLength  | PrefixOptions |              0                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7-17 Frame format of Inter-Area-Prefix-LSA

This type of LSA equals type 3 LSA in OSPFv2. The prefix generation process is basically the same as that in OSPFv2, but has the following differences:

LSID is not an address and is just used to distinguish LSAs. Therefore, you can add an InterPrefixID to the target area and set its value to 1.

For a new route, increment the sequence number.

For an existing route, use its prefix for searching.

Inter-Area-Router-LSAs

The frame format of Inter-Area-Router-LSA is shown in Figure 7-18:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LS Age             |0|0|1|          4              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Advertising Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    LS Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |                 Options                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       0       |                 Metric                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Router ID                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7-18 Frame format of Inter-Area-Router-LSA

The generation process is basically the same as that in OSPFv2, but has the following differences:

1. LSID does not describe the router ID and is only used to distinguish LSAs. It can be designed in the same way as inter-area prefix LSAs.
2. The ID of the destination router is marked by Destination Router ID in LSA.
3. Compared with OSPFv2, there is an option field, which is the option in Router-LSA of the destination router.

AS-External-LSAs

The frame format of AS-External-LSA is shown in Figure 7-19:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age              |0|1|0|          5              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Advertising Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    LS Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         |E|F|T|              Metric                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| PrefixLength  | PrefixOptions |     Referenced LS Type        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-                                                             -+
|                                                               |
+-                Forwarding Address (optional)                -+
|                                                               |
+-                                                             -+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              External Route Tag (optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Referenced Link State ID (optional)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7-19 Frame format of AS-External-LSA

LSID does not describe the router ID and is only used to distinguish LSAs. The destination ID is marked by the address prefix in LSA body.

NSSA-LSAs

The frame format of NSSA-LSAs is the same as that of type 5 LSA and the generation process is the same as that in OSPFv2.

Link-LSAs

The frame format of Link-LSA is shown in Figure 7-20:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age              |0|0|0|          8              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Link State ID                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Advertising Router                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    LS Sequence Number                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Rtr Priority  |                Options                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-                                                             -+
|                                                               |
+-                Link-local Interface Address                 -+
|                                                               |
+-                                                             -+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         # prefixes                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  PrefixLength | PrefixOptions |             0                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  PrefixLength | PrefixOptions |             0                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7-20 Frame format of Link-LSA

Link-LSA is not available in OSPFv2.

A router generates a Link-LSA for each link. Link-LSAs are generated as long as the interface IP address is available after device startup. Link-LSA is not generated for virtual links. LSID is the interface ID of the router.

Link-LSA is used to:

1. Provide a link local address started with fe80.
2. Provide the IPv6 prefix for local connection.
3. Provide options.

The process for creating a Link-LSA for link L is as follows:

- Set LSID to the interface ID configured by the router for link L.
- Set Link-LSA to contain the priority of link L.
- Set option for the capability of the router. When DR generates a Network-LSA on a broadcast interface, the logic OR operation is performed on options of all FULL neighbors.
- The router adds the link local address of link L in the Link-LSA. This information is used for next hop calculation.
- Contain all IPv6 address prefixes configured for L, and specify the prefix length, option, and prefix.

Add the created LSA to the link database and diffuse it on the link. After receiving the LSA, other nodes on the link store the LSA but do not flood it.

Intra-Area-Prefix-LSAs

The frame format of Intra-Area-Prefix-LSA is shown in Figure 7-21 (LSID does not indicate an address):

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LS Age              |0|0|1|            9            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Link State ID                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Advertising Router                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      LS Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        LS Checksum            |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         # Prefixes            |     Referenced LS Type        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Referenced Link State ID                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Referenced Advertising Router                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  PrefixLength | PrefixOptions |          Metric               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  PrefixLength | PrefixOptions |          Metric               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Address Prefix                         |
|                             ...                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7-21 Frame format of Intra-Area-Prefix-LSA

Intra-area-prefix-LSA is different from type 9 LSA in OSPFv2. Type 9 LSA in OSPFv2 is used for graceful restart, belonging to interface flooding. Intra-area-prefix-LSA describes a prefix of a network or router, belonging to area flooding. LSID is also used to distinguish LSAs.

1. Describe the prefix of a network

Stub interface - the current Router-LSA is referenced. The referenced LSID is 0, and the referenced router ID is the ID of the router itself.

2. Describe the prefix of a router

BCAST interface with a FULL neighbor - Network-LSA is referenced. The referenced LSID is the interface ID of DR on the link L and the referenced router ID is the ID of DR. This is generated only when the router is DR and has a FULL neighbor.

The link DR generates one or multiple LSAs to advertise the link prefix. DR on link L creates an LSA as follows:

- To indicate the correspondence between the prefix and link L, the referenced LS type, LSID, and router ID are set to corresponding fields of Network-LSA of link L. That is, the referenced LS type is 0x2002, the referenced LSID is the interface ID of DR on the link L, and the referenced router ID is the ID of DR.
- Check each Link-LSA on link L. If the advertising router of Link-LSA establishes a FULL neighbor with DR and its LSID is the same as the interface ID of the neighbor, copy the prefix in Link-LSA to the new LSA. If the prefix has the NU bit or LA bit option, the prefix and link local address are not copied. If the prefix length and prefix are the same, logic OR is performed on options to get the final prefix option.

  The overhead of all prefixes is 0.
- "# prefixes" is set to the number of prefixes in LSA. When necessary, prefixes can be distributed across multiple LSAs to reduce the LSA size.

Routers construct intra-area-prefix-LSAs for prefixes on their stub links. Routers construct LSAs as follows:

- Set the reference LS type to 0x2001, referenced LSID to 0, and referenced router ID to the ID of the router itself.
- Check the interface state of its area. If the interface is down, do not contain the interface prefix.

  If the interface is contained in a type 2 link, contain the prefix in the LSA advertised by the interface DR to skip the interface.
  If the LA bit is set for the prefix, contain this prefix.
  Set the prefix overhead to the overhead of the corresponding interface.

- The LSA contains the directly connected host (this is optional).
- If one or more virtual links pass through this area, contain a global IPv6 interface address (if not configured), set the LA bit in the option, and set prefix length to 128 and overhead to 0. This information is used for two ends of a virtual link to learn each other's address.
- "# prefixes" is set to the number of prefixes.

7.4.2 Configuring OSPFv3

7.4.2.1 Configuring Global OSPFv3

7.4.2.1.1 Enabling an OSPFv3 Process

Purpose

This section describes how to enable and disable an OSPFv3 process.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the default OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command.
Enable the designated OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** *process-id* command.
Disable the default OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **no router ipv6 ospf** command.
Disable the designated OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **no router ipv6 ospf** *process-id* command.

7.4.2.1.2 Enabling the VPN Instance Designated by an OSPFv3 Process

Purpose

This section describes how to enable the VPN instance designated by an OSPFv3 process.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the VPN instance designated by an OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** *process-id* **vpn-instance** *name* command.
Enable the VPN instance designated by the default OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf vpn-instance** *name* command.

7.4.2.1.3 Resetting an OSPFv3 Process

Purpose

This section describes how to reset an OSPFv3 process.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Reset an OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **reset ipv6 ospf** command.
Reset the designated OSPFv3 process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **reset ipv6 ospf** *process-id* command.

7.4.2.1.4 Clearing OSPFv3 Statistics

Purpose

This section describes how to clear OSPFv3 statistics.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Clear OSPFv3 statistics	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **reset ipv6 ospf counters** command.

7.4.2.2 Configuring an OSPFv3 Node

7.4.2.2.1 Configuring a Router ID

Purpose

This section describes how to configure a router ID.

Background

The router ID to be configured must be one of the local IP addresses.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a router ID	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **router-id** *router-id* command.

7.4.2.2.2 Configuring a Stub Area

Purpose

This section describes how to configure a stub area.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a common stub area	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **stub** command.
Configure a total stub area	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **stub no-summary** command.
Delete a stub area	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no area** *area-id* **stub** command.
Configure a stub router	1. Access the global configuration view. 2. Access the OSPFv3 configuration view. 3. Run the **stub router** command.
Configure a stub router and set the interval during which a device acts as a stub router when it is restarted or faulty	1. Access the global configuration view. 2. Access the OSPFv3 configuration view. 3. Run the **stub router on-startup** [*on-startup-time* | **default**] command.
Delete a stub router	1. Access the global configuration view. 2. Access the OSPFv3 configuration view. 3. Run the **no stub router** command.

7.4.2.2.3 Configuring an NSSA

Purpose

This section describes how to configure an NSSA.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure an NSSA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **nssa** command.
Configure the no summary NSSA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **nssa no-summary** command.
Configure aggregation advertising/no advertising for an NSSA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **nssa range** *dst-address dst-mask* **{ advertise** | **no-advertise }** command.
Configure the designated conversion router or candidate conversion router for an NSSA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **nssa translator { always | candidate }** command.
Delete an NSSA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no area** *area-id* **nssa** command.
Delete NSSA aggregation	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no area** *area-id* **nssa range** *dst-address dst-mask* command.

7.4.2.2.4 Configuring Area Aggregation

Purpose

This section describes how to configure area aggregation.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure area aggregation	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **no-advertise** } command.
Delete area aggregation	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no area** *area-id* **range** *dst-address dst-mask* command.

7.4.2.2.5 Enabling FRR

Purpose

This section describes how to enable fast route redistribution (FRR).

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable FRR	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **frr** { **enable** | **disable** } command.

7.4.2.2.6 Configuring GR

Purpose

This section describes how to configure graceful restart (GR).

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable GR	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **graceful-restart** command.
Configure a GR period	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **graceful-restart period** *restart-time* command.
Enable the GR helper	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **graceful-restart helper** command.
Disable GR	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no graceful-restart** command.
Disable the GR helper	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no graceful-restart helper** command.
Implement GR	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **graceful-restart begin** command.

7.4.2.2.7 Configuring an Interval for Route Calculation

Purpose

This section describes how to configure an interval of route calculation.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure an interval for route calculation	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the following commands: ● **spf-running-interval** *interval* ● **spf-running-interval default**

7.4.2.2.8 Configuring OSPFv3 Redistribution

Purpose

This section describes how to configure OSPFv3 redistribution.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure OSPFv3 redistribution	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **redistribute { connect | static | rip | bgp | isis | ospf }** command.
Disable OSPFv3 redistribution	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no redistribute { connect | static | rip | bgp | isis | ospf }** command.

Purpose	Procedure
Configure a routing policy of redistribution	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the r**edistribute { connect | static | rip | bgp | isis | ospf } route-policy** *policy-name* command.
Delete a routing policy of redistribution	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **no redistribute { connect | static | rip | bgp | isis | ospf } route-policy** *policy-name* command.

7.4.2.2.9 Enabling the Trap Report Function of OSPFv3

Purpose

This section describes how to enable the trap report function of OSPFv3.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the trap report function of OSPFv3	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the **snmp-trap** { **enable** | **disable** } command.
Enable or disable the detailed trap report function of OSPFv3	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **router ipv6 ospf** command to access the OSPFv3 configuration view. 3. Run the command **snmp-trap { enable | disable } trap-name { ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange | ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa | ospfnbrrestarthelperstatuschange | ospfnbrstatechange | ospfnssatranslatorstatuschange | ospforiginatelsa | ospfrestartstatuschange | ospftxretransmit | ospfvirtifauthfailure | ospfvirtifconfigerror | ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit | ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange }.**

7.4.2.3 Configuring an OSPFv3 Port

7.4.2.3.1 Configuring OSPFv3 Interface Parameters

Purpose

This section describes how to configure the parameters of an OSPFv3 interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Add an interface to a designated area	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the **ipv6 ospf area** *area-id* command.
Add an interface to a designated process	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf area** *area-id* **process** *process-id* ● **ipv6 ospf area** *area-id* **process** *process-id* **instance** *instance-id*
Configure the type of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the **ipv6 ospf if-type** { **broadcast** | **p2p** } command.
Configure the priority of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf priority** *priority* ● **ip ospf priority default**
Configure the overhead of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view.

Purpose	Procedure
	3. Run the following commands: ● **ipv6 ospf cost** *cost* ● **ip ospf cost default**
Configure an interval for sending Hello packets by an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf hello-interval** *hello-interval* ● **ip ospf hello-interval default**
Configure the neighbor timeout time of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf dead-interval** *dead-interval* ● **ip ospf dead-interval default**
Configure the retransmission interval of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf retransmit-interval** *retransmit-interval* ● **ip ospf retransmit-interval default**
Configure the transmission delay of an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the following commands: ● **ipv6 ospf transmit-delay** *transmit-delay* ● **ip ospf transmit-delay default**

7.4.2.3.2 Configuring BFD

Purpose

This section describes how to configure BFD.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure BFD	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the **ipv6 ospf bfd** { **enable** | **disable** } command.

7.4.2.3.3 Configuring an MTU Value for an OSPFv3 Interface

Purpose

This section describes how to configure an MTU value for an OSPFv3 interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure an MTU value for an OSPFv3 interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the **ipv6 ospf mtu** *mtu* **or ip ospf mtu default** command.
Configure MTU detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the **ipv6 ospf mtu-ignore { enable | disable }** command.

7.4.2.3.4 Configuring a Passive Interface

Purpose

This section describes how to configure a passive interface.

Background

A passive interface refers to an OSPFv3 interface that does not send or receive protocol messages and does not establish any neighbor relationship. However, the interface route is included in the Router-LSA for internal route propagation. It can be used for the stub route.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a passive interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the ipv6 ospf passive-interface command.
Delete configuration of a passive interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface vlan** *N* command to access the VLANIF configuration view. 3. Run the no ipv6 ospf passive-interface command.

7.4.2.4 Configuring OSPFv3 Debugging

Purpose

This section describes how to configure OSPFv3 debugging.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable global debugging	1. Access the privileged user view. 2. Run the command **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }.**
Enable debugging for a specified instance	1. Access the privileged user view. 2. Run the command **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process** *process-id*.
Enable debugging for all instances	1. Access the privileged user view. 2. Run the command **debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all.**
Disable global debugging	1. Access the privileged user view. 2. Run the command **no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error }.**
Disable debugging for a specified instance	1. Access the privileged user view. 2. Run the command **no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process** *process-id*.
Disable debugging for all instances	1. Access the privileged user view. 2. Run the **command no debug ospf6 { global | all | lsa | hello | packet | neighbor | interface | ip-route | rtm | spf | syn | graceful-restart | nbrchange | frr | error } process all.**

7.4.2.5 Viewing OSPFv3 Configuration

Purpose

This section describes how to view the OSPFv3 configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display the brief OSPFv3 information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf brief** ● **show ipv6 ospf brief process** *process-id*
Display the OSPFv3 configuration	1. Access the common user view. 2. Run the **show ipv6 ospf config** command.
Display the OSPFv3 interface information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf interface** ● **show ipv6 ospf interface vlan** *vlan-id* ● **show ipv6 ospf interface loopback** *loopback-id* ● **show ipv6 ospf interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show ipv6 ospf interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **show ipv6 ospf interface count** ● **show ipv6 ospf interface process** *process-id*
Display the OSPFv3 neighbor information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf neighbor** ● **show ipv6 ospf neighbor process** *process-id* ● **show ipv6 ospf neighbor** *ip-address* ● **show ipv6 ospf neighbor state statistic**
Display the OSPFv3 area information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf area** ● **show ipv6 ospf area** *area-id* ● **show ipv6 ospf area process** *process-id*

Purpose	Procedure
Display the OSPFv3 database information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf database** ● **show ipv6 ospf database process** *process-id* ● **show ipv6 ospf database area** *area-id* ● **show ipv6 ospf database area** *area-id* **process** *process-id* ● **show ipv6 ospf database count** ● **show ipv6 ospf database count process** *process-id* ● **show ipv6 ospf database total count** ● **show ipv6 ospf database { router | network | inter-prefix | inter-router | external | link | intra-prefix | nssa | te }** ● **show ipv6 ospf database { router | network | inter-prefix | inter-router | intra-prefix | nssa | te }** *LS-id advertise-router-id area-id* ● **show ipv6 ospf database age** *min-age max-age* ● **show ipv6 ospf database area** *area-id* ● **show ipv6 ospf database area** *area-id* **process** *process-id* ● **show ipv6 ospf database external** *LS-id advertise-router-id* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface vlan** *vlan-id* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface loopback** *loopback-id* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.**subinterface**
Display the OSPFv3 routing information	1. Access the common user view. 2. Run the following commands: ● **show ipv6 ospf route** ● **show ipv6 ospf route process** *process-id* ● **show ipv6 ospf route total count**
Display the OSPFv3 BFD information	1. Access the common user view. 2. Run the **show ipv6 ospf bfd session** command.

Purpose	Procedure
Display the OSPFv3 trap information	1. Access the common user view. 2. Run the **show ipv6 ospf trap** command.
Display the OSPF BFD session information	1. Access the common user view. 2. Run the **show ipv6 ospf bfd session** command.

7.4.3 OSPFv3 Configuration Example

7.4.3.1 Configuring Basic OSPFv3 Functions

Network Requirements

This case shows how to configure basic OSPFv3 functions to make you familiar with the OSPFv3 configuration process. The topology is shown in Figure 7-22.

Network Diagram

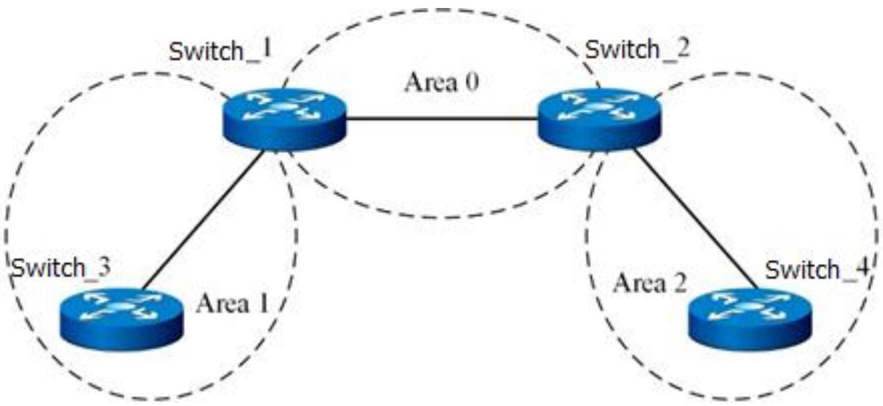


Figure 7-22 OSPFv3 basic configuration topology

Configuration Suggestion

All devices run OSPFv3. The AS is divided into 3 areas. Switch_1 and Switch_2 are ABRs that transmit the routes between areas.

After configuration, each device can learn the routes destined for all network segments in the AS.

Data Preparation

Interface addresses of Switch_1: 2001::1/64 and 2003::1/64

Interface addresses of Switch_2: 2001::2/64 and 2004::2/64

Interface address of Switch_3: 2003::3/64

Interface address of Switch_4: 2004::4/64

Configuration

Switch_1:
Switch_1(config)#router ipv6 ospf
Switch_1(config-ospfv3-1)#router-id 1.1.1.1
Switch_1(config-ospfv3-1)#quit
Switch_1(config)#interface vlan 10
Switch_1(config-if-vlan10)#ipv6 ospf area 0
Switch_1(config-if-vlan10)#quit
Switch_1(config)#
Switch_1(config)#interface vlan 30
Switch_1(config-if-vlan 30)#ipv6 ospf area 0

Switch_2:
Switch_2(config)#router ipv6 ospf
Switch_2(config-ospfv3-1)#router-id 2.1.1.2
Switch_2(config-ospfv3-1)#quit
Switch_2(config)#interface vlan 10
Switch_2(config-if-vlan10)#ipv6 ospf area 0
Switch_1(config-if-vlan10)#quit
Switch_1(config)#
Switch_1(config)#interface vlan 40
Switch_1(config-if-vlan 40)#ipv6 ospf area 0

Switch_3:
Switch_3(config)#router ipv6 ospf
Switch_3(config-ospfv3-1)#router-id 3.1.1.3
Switch_3(config-ospfv3-1)#quit
Switch_3(config)#interface vlan 30
Switch_3(config-if-vlan30)#ipv6 ospf area 0

Switch_4:
Switch_4(config)#router ipv6 ospf
Switch_4(config-ospfv3-1)#router-id 4.1.1.4
Switch_4(config-ospfv3-1)#quit
Switch_4(config)#interface vlan 40
Switch_4(config-if-vlan40)#ipv6 ospf area 0

Configuration Verification

Run the **show ipv6 ospf neighbor** command to view the following OSPFv3 information:

OSPFv3 process 1

NeighborId	Priority	State	Interface	Instance	Aging	UpTime	IpAddress
1.1.1.2	1	Full	vlan10	0	32	0:01:38	fe80::b8:1

Run the **show ip ospf database** command to view the following OSPFv3 information:

Database of OSPFv3 process 1

Router Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	196	0x80000002	0x49f7	40
0.0.0.0	3.1.1.3	197	0x80000002	0x43fc	40

Network Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	3.1.13	197	0x80000001	0x11d1	32

Intra Area Prefix Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.3.232	3.1.1.3	197	0x80000001	0x1a6c	44

Link(Type-8) State(interface vlan1 Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	1.1.1.1	236	0x80000001	0xf91	76
0.0.39.17	3.1.1.3	237	0x80000001	0x6155	76

7.4.3.2 Configuring a Stub Area

Network Requirements

This case shows how to configure an OSPFv3 stub area to make you familiar with the OSPFv3 stub area configuration process. The topology is shown in Figure 7-23.

Network Diagram

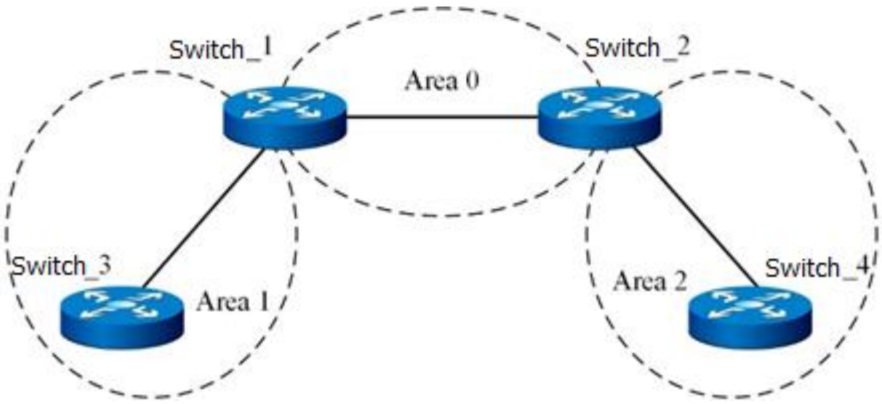


Figure 7-23 Stub area topology

Configuration Suggestion

All devices run OSPFv3. The AS is divided into 3 areas. Switch_1 and Switch_2 are ABRs that transmit the routes between areas.

After configuration, each device can learn the routes destined for all network segments in the AS.

Data Preparation

Interface addresses of Switch_1: 2001::1/64 and 2003::1/64

Interface addresses of Switch_2: 2001::2/64 and 2004::2/64

Interface address of Switch_3: 2003::3/64

Interface address of Switch_4: 2004::4/64

Configuration

The basic configuration and topology are the same as those described in 7.4.3.1 Configuring Basic OSPFv3 Functions.

Configure Area 1 as a stub area.
Switch_1:
Switch_1(config)#router ipv6 ospf
Switch_1(config-ospfv3-1)#area 1 stub
Switch_1(config)#
Switch_3:
Switch_3(config)#router ipv6 ospf
Switch_3(config-ospfv3-1)# area 1 stub
Switch_3(config)#
Introduce a type 5 LSA with the address 2013:0122::1/64 to Switch_4
Switch_4:
Switch_4(config-ospfv3-1)#redistribute static

Configuration Verification

1) When the area of Switch_3 is a normal area, the routing table contains routes outside of the AS. After the area is configured as a stub area, it has a default type 3 Inter-Area-Prefix-LSA, which is absent from normal areas. No LSA outside of the AS is displayed.
2) After the area of Switch_3 is configured as a stub area, no route outside of the AS is displayed, but a default route destined outside the area is displayed.

7.4.3.3 Configuring an NSSA

Network Requirements

This case shows how to configure an OSPFv3 stub area to make you familiar with the OSPFv3 stub area configuration process. The topology is shown in Figure 7-24.

Network Diagram

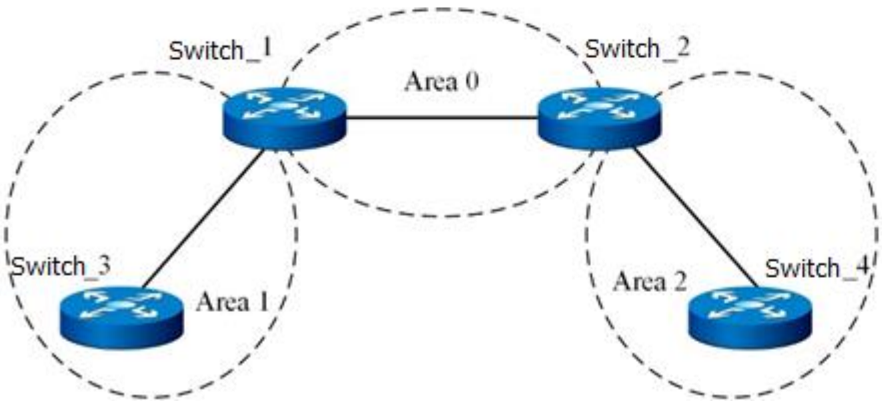


Figure 7-24 NSSA topology

Configuration Suggestion

All devices run OSPFv3. The AS is divided into 3 areas. Switch_1 and Switch_2 are ABRs that transmit the routes between areas.

After configuration, each device can learn the routes destined for all network segments in the AS.

Data Preparation

Interface addresses of Switch_1: 2001::1/64 and 2003::1/64

Interface addresses of Switch_2: 2001::2/64 and 2004::2/64

Interface address of Switch_3: 2003::3/64

Interface address of Switch_4: 2004::4/64

Configuration

The basic configuration and topology are the same as those described in 7.4.3.1 Configuring Basic OSPFv3 Functions.

Configure Area 1 as NSSA.

Switch_1:

```
Switch_1(config)#router ipv6 ospf
Switch_1(config-ospfv3-1)#area 1 nssa
Switch_1(config)#
```

Switch_3:
Switch_3(config)#router ipv6 ospf
Switch_3(config-ospfv3-1)# area 1 nssa
Switch_3(config)#

Configuration Verification

1) The database of NSSA has a default LSA of the NSSA type, which is absent from the databases of normal areas.

2) Import the static route 1111:1011::1/64 to Switch_3, and redistribute static routes.

3) Import the static route 2222:1011::1/64 to Switch_4 and check whether Switch_3 has any external route.

7.4.3.4 Configuring BFD

Network Requirements

This case shows how to configure the OSPFv3 BFD configuration to make you familiar with the OSPFv3 BFD configuration process. The topology is shown in Figure 7-25.

Network Diagram

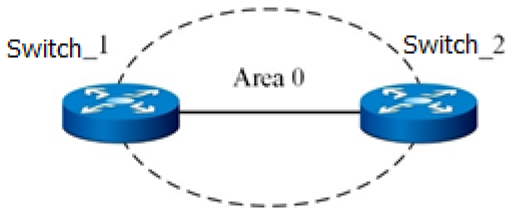


Figure 7-25 BFD function case topology

Configuration Suggestion

Two devices run OSPFv3 and are located in Area 0.

Data Preparation

Interface addresses of Switch_1: 2001::1/64 and 2003::1/64

Interface addresses of Switch_2: 2001::2/64 and 2004::2/64

Interface address of Switch_3: 2003::3/64

Interface address of Switch_4: 2004::4/64

Configuration

1) Basic configuration:

```
Switch_1:
Switch_1(config)#router ipv6 ospf
Switch_1(config-ospfv3-1)#router-id 1.1.1.1
Switch_1(config-ospfv3-1)#quit
Switch_1(config)#interface vlan 10
Switch_1(config-if-vlan10)#ipv6 ospf area 0
Switch_1(config-if-vlan10)#quit

Switch_2:
Switch_2(config)#router ipv6 ospf
Switch_2(config-ospfv3-1)#router-id 2.1.1.2
Switch_2(config-ospfv3-1)#quit
Switch_2(config)#interface vlan 10
Switch_2(config-if-vlan10)#ipv6 ospf area 0
Switch_2(config-if-vlan10)#quit
```

2) BFD configuration:

```
Switch_1:
Switch_1(config)#interface vlan 4
Switch_1(config-vlan-10)#bfd enable
Switch_1(config-vlan-10)#ipv6 ospf bfd enable
Switch_2:
Switch_2(config)#interface vlan 4
Switch_2(config-vlan-10)#bfd enable
Switch_2(config-vlan-10)#ipv6 ospf bfd enable
```

Configuration Verification

```
Switch_1#sho ipv6 ospf bfd session
 OSPF process 1
 NeighborAddress      NeighborID         BFDState
 fe80::b8:2            2.1.1.2            UP
Switch_2#sho ipv6 ospf bfd session
 OSPF process 1
 NeighborAddress      NeighborID         BFDState
 fe80::b8:1            1.1.1.1            UP
```

7.4.3.5 Configuring GR

Network Requirements

This case shows how to configure the OSPFv3 GR configuration to make you familiar with the OSPFv3 GR configuration process. The topology is shown in Figure 7-26.

Network Diagram

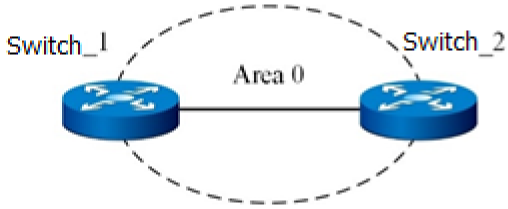


Figure 7-26 GR function case topology

Configuration Suggestion

Two devices run OSPFv3 and are located in Area 0.

Two devices are required by GR testing. One device is GR initiator and the other is GR helper. Testing on the GR initiator uses dual core switch cards and the plugging/unplugging method. There is no limit on the GR helper.

Data Preparation

Interface addresses of Switch_1: 2001::1/64 and 2003::1/64

Interface addresses of Switch_2: 2001::2/64 and 2004::2/64

Interface address of Switch_3: 2003::3/64

Interface address of Switch_4: 2004::4/64

Configuration

1) The topology is the same as shown in Figure 7-26 and the basic configuration is the same as those described in 7.4.3.1 Configuring Basic OSPFv3 Functions.

2) GR configuration

Switch_1:
Switch_1(config)#router ipv6 ospf
Switch_1(config-ospfv3-1)# graceful-restart
Switch_1(config-ospfv3-1)# graceful-restart period 60
Switch_2:
Switch_2(config)#router ipv6 ospf
Switch_2(config-ospfv3-1)# graceful-restart helper

Configuration Verification

Use the plugging/unplugging method for testing. After the GR initiator and GR helper are configured, unplug the active core switch card of the GR initiator and check that the original traffic between the devices is not interrupted.

7.5 Configuring BGP

7.5.1 BGP Overview

7.5.1.1 Background Information

Border Gateway Protocol (BGP) is used to control the propagation of routes and select the best route.
BGP is a dynamic routing protocol used between Autonomous Systems (AS). The earlier versions are BGP-1 (RFC1105), BGP-2 (RFC1163), and BGP-3 (RFC1267). The current version is BGP-4 (RFC4271).
As the de facto Internet external routing protocol standard, BGP-4 is widely used between Internet Service Providers (ISPs).

7.5.1.2 Protocol Features

BGP has the following features:

- Different from interior gateway protocols (IGPs) such as OSPF and RIP, BGP is an exterior gateway protocol (EGP) used to control the propagation of routes and select the best route, instead of discovering and calculating routes.
- BGP uses TCP as its transport layer protocol (port number: 179), which improves protocol reliability.
- BGP supports Classless Inter-Domain Routing (CIDR).
- BGP only sends updated routes, which greatly reduces the bandwidth occupied by BGP for route propagation, and is suitable for sending a large amount of routing information on the Internet.
- BGP routes completely solve the routing loop problem by carrying AS path information.
- BGP provides various routing policies and can flexibly filter and select routes.
- BGP is easy to expand and can adapt to network development.

BGP runs on the switch in the following two ways:

- IBGP (Internal BGP)
- EBGP (External BGP)

BGP running within the same AS is called IBGP. BGP running between different ASs is called EBGP.

7.5.1.3 Basic Concepts

BGP-4 provides a set of new mechanisms to support CIDR, including supporting network prefix broadcast and cancelling the concept "class" in BGP networks. BGP-4 also supports route aggregation, including aggregation of AS paths. These changes provide support for the proposed supernet solution. Main route attributes include:

- Origin
- AS_Path
- Next_Hop
- Multi-Exit-Discriminator
- Local_Pref
- Community

7.5.1.4 BGP4 Technology

7.5.1.4.1 BGP4 Neighbor

BGP neighbors, also known as peers, are of two types. If two peers exchanging BGP packets belong to different ASs, the two peers are EBGP (External BGP) peers. If two peers exchanging BGP packets belong to the same AS, the two peers are IBGP (Internal BGP) peers. BGP connections must also be established between different border routers in an AS. Only in this way can routing information be transmitted throughout the AS.

IBGP peers are not necessarily directly connected physically, but must be fully connected logically. In most cases, there are physical direct links between EBGP peers, but if this is not possible, logical links can also be configured. Figure 7-27 shows an example of BGP neighbors. R1 and R3, and R2 and R3 in AS100 form IBGP neighbors, and R3 in AS100 and R4 in AS200 form EBGP neighbors.

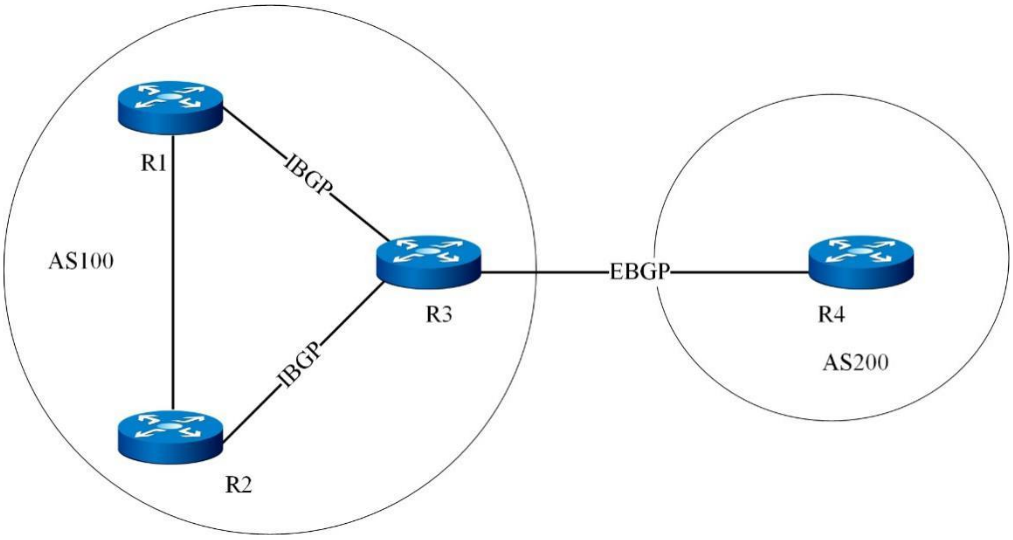


Figure 7-27 BGP neighbors

BGP advertises the routes obtained from EBGP to all its BGP peers, including IBGP and EBGP. It does not advertise the routes obtained from IBGP to its IBGP peers. When advertising routes to EBGP, ensure that BGP waits until IGP propagates the same route in the local AS, and then advertises the route to other ASs. That is, before a route is advertised to other ASs, the routers within the AS must know the route first.

7.5.1.4.2 BGP4 Route Advertisement

A route is generally generated inside an AS, discovered and calculated by an internal routing protocol and transmitted to the border of the AS, and then is propagated to other ASs by an ASBR through an EBGP connection.

The route may pass through several ASs during propagation, and these ASs are called transit ASs. If the AS has multiple border routers, these routers run IBGP to exchange routing information. In this case, internal routers do not need to know these external routes, and they only need to maintain IP connectivity between border routers. After the routes reach the border of the AS, if an internal router needs to know these external routes, the ASBR can import the routes into the internal routing protocol. The number of external routes is very large, which usually exceeds the processing capacity of internal routers. Therefore, when importing external routes, route filtering or aggregation is generally required to reduce the number of routes. In extreme cases, default routes are used.

Figure 7-28 shows how BGP selects the best route. BGP does not calculate routes. Instead, it selects the best route based on specific policies.

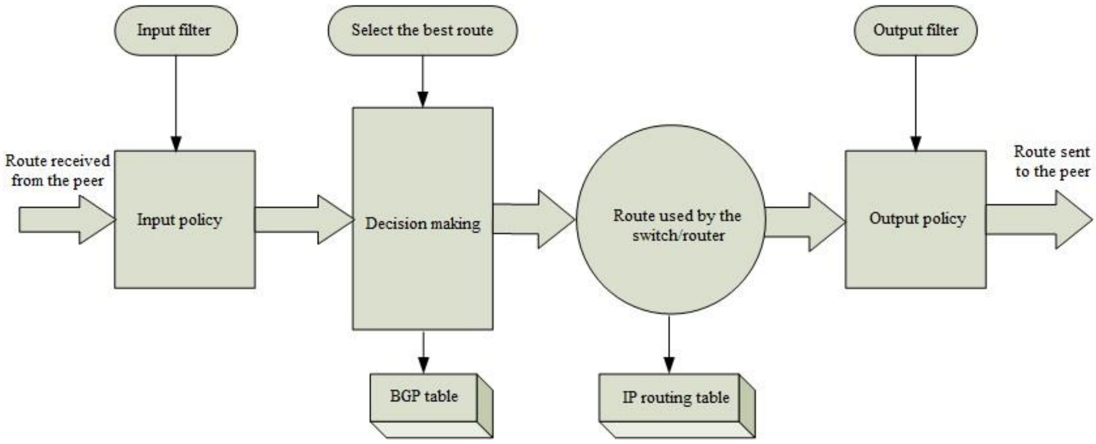


Figure 7-28 BGP route selection flowchart

7.5.1.4.3 BGP4 Messages

BGP supports four types of messages: Open, KeepAlive, Update, and Notification. All these messages are transmitted via TCP.

1. Open message

   The Open message is the first message after TCP connection used by the BGP neighbor is established. It contains the current protocol version, AS, router ID, and some optional parameters. If the peer does not agree on some parameters in the message, the BGP neighbor relationship cannot be established.

2. KeepAlive message

   After the two parties reach an agreement on the content of the Open message, the KeepAlive message will be sent periodically. This message is used to detect the status of the neighbor. If the KeepAlive message sent by the neighbor is not received within a certain period of time, the neighbor is considered to be faulty.

3. Update message

   The Update message carries routing information, including various attributes of the route. BGP uses this message to advertise routing information to neighbors.

4. Notification message

   When an error occurs during BGP operation, a Notification message carrying the error reason is sent.

7.5.1.4.4 BGP4 Attributes

BGP defines a large number of route attributes to describe routes in more detail. During route selection, BGP needs to judge the route attributes to select routes that meet specific policy requirements.

1. ORIGIN

   Specifies the source of a route. It can be set to any of the following values:
   IGP: Network reachability information is inside the original AS
   EGP: Get network reachability information through EGP
   INCOMLETE: Get network reachability information in other means

2. AS-PATH

   AS-PATH consists of AS path fragments. Each AS path fragment consists of a combination of <path fragment type, path fragment length, and path fragment value>. Path fragment type is a 1-byte field with the following specified values:

   (1) AS-SET: A sequence of unordered ASs that a route passes through.

   (2) AS-SEQUENCE: A sequence of ordered ASs that a route passes through.

   Path fragment length is a 1-byte field containing the number of ASs in the path fragment value field. The path fragment value field contains one or more AS numbers, each encapsulated in a 2-byte long field.

3. NEXT-HOP

   NEXT-HOP specifies the IP address of a border router, which is used as the IP address of the next hop in pathfinding.

4. MULTI-EXIT-DISC

   It is a 4-bit non-zero integer. Its value is used by the BGP initiator to perform decision processing to distinguish multiple paths to neighboring ASs.

5. LOCAL-PREF

   It is a 4-bit non-zero integer. It is used by BGP participants to notify other BGP participants in an AS.

6. ATOMIC-AGGREGATE

   It is used by BGP participants to inform other BGP participants that the local system has chosen an ambiguous route rather than an explicit route.

7. AGGREGATOR

   It contains the last AS number (encapsulated in two bytes) that forms the aggregate route, followed by the IP addresses of the BGP participants that form the aggregate route (encapsulated in four bytes).

7.5.1.4.5 BGP4 Route Selection Policies

1. Select the route with the highest Local_Pref first.
2. Select aggregated routes (aggregated routes have higher priority than non-aggregated routes) first.
3. Select the route with the shortest AS_Path first.
4. Select the route whose Origin is IGP first, followed by EGP and then Incomplete.
5. Select the route with the lowest MED value first.
6. Select routes learned from EBGP (EBGP routes have higher priority than IBGP routes) first.
7. Select the route with the lowest Metric of the IGP in the AS first.
8. Select the route advertised by the switch with the smallest Router ID.
9. Select the route learned from the peer with the smaller IP address first.

7.5.1.4.6 BGP4 Route Advertising Policies

1. When there are multiple active routes, the BGP speaker only advertises the optimal route to its peers.
2. The BGP speaker only advertises the routes it uses to its peers.
3. The route obtained by the BGP speaker from EBGP will be advertised to all its BGP peers, but will not be advertised to the peers (including EBGP peers and IBGP peers) that advertise the route.
4. Routes obtained by the BGP speaker from IBGP are not advertised to its IBGP peers.
5. The BGP speaker advertises routes obtained from IBGP to its EBGP peers (when the BGP and IGP synchronization feature is not enabled).
6. After a connection is established, the BGP speaker advertises all its BGP routes to new peers.

7.5.1.4.7 BGP4 Route Aggregation

In a large network, the BGP routing table is very large, and route aggregation can greatly reduce the size of the routing table.

Route aggregation is actually a process of combining multiple routes. In this way, when BGP can only advertise the aggregated route to its peers, instead of advertising all specific routes.

7.5.1.4.8 IBGP-IGP Synchronization in BGP4

IBGP-IGP synchronization can avoid misleading external AS routers.

After synchronization is enabled, the IGP routing table will be checked before IBGP routes are added to the routing table and advertised to EBGP peers. Only when the IGP also knows this IBGP route will it be added to the routing table and advertised to EBGP peers.

Synchronization can be disabled in following situations.

- The local AS is not a transit AS.
- All switches in the AS have established IBGP full connections.

7.5.1.4.9 BGP4 Community

Peers in the same group can share the same policy, and a community enables a group of BGP routers in multiple ASs to share the same policy. Community is a routing attribute that is propagated between BGP peers and is not restricted by the AS scope.

Before advertising a route with the community attribute to other peers, a BGP router can change the original community attribute of the route.

In addition to recognized community attributes, you can also use community attribute filters to filter custom extended community attributes for more flexible control of routing policies.

7.5.1.4.10 BGP4 Route Reflector

To ensure connectivity between IBGP peers, full connections need to be established between IBGP peers. Assuming that there are n switches in an AS, the number of IBGP connections required is n(n-1)/2. When the number of IBGP peers is large, many network resources and CPU resources are consumed.

This problem can be solved by route reflection. In an AS, one switch serves as a route reflector (RR), and other switches serve as clients to establish IBGP connections with the route reflector. The route reflector transfers (reflects) routing information between clients without establishing a BGP connection between clients.

BGP routers that are neither a reflector nor a client are called a non-client. A full connection must be established between non-clients and route reflectors, as well as between all non-clients.

7.5.1.4.11 BGP4 Confederation

Confederation is another method to deal with the surge of IBGP network connections within an AS. It divides an AS into several sub-ASs. A full connection is established between IBGP peers in each sub-AS and an EBGP connection is established between IBGP peers in different sub-ASs.

BGP speakers that do not belong to a confederation treat multiple sub-ASs belonging to the same confederation as a whole, and do not need to know internal sub-ASs. The confederation ID is the AS number that identifies the entire confederation.

Confederation has a disadvantage: When switching from a non-confederation solution to a confederation solution, the switches must be reconfigured and the logical topology must be modified.

In large BGP networks, route reflector and confederation can be used together.

7.5.1.4.12 MP-BGP of BGP4

Traditional BGP-4 only manages routing information of IPv4. For applications using other network layer protocols, there are certain restrictions when spreading routes across ASs.

To support multiple network layer protocols, IETF extended BGP-4 to MP-BGP. The current MP-BGP standard is RFC2858 (Multiprotocol Extensions for BGP-4).

MP-BGP is forward compatible. That is, switches supporting BGP extension can communicate with switches not supporting BGP extension.

1. MP-BGP Extension Attribute

   In the packets used by BGP-4, three pieces of information related to IPv4 are carried by the Update packets. These three pieces of information are NLRI, Next_Hop in the path attribute, and Aggregator in the path attribute (this attribute contains the IP addresses of the BGP speakers that form the aggregated route).

   To support multiple network layer protocols, BGP-4 needs to reflect network layer protocol information to NLRI and Next_Hop. Two new path attributes are introduced in MP-BGP:

   MP_REACH_NLRI: Multiprotocol Reachable NLRI. It is used to advertise reachable routes and the next hop.

   MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI. It is used to cancel unreachable routes.

   Both attributes are optionally non-transitive. Therefore, BGP speakers that do not provide multi-protocol capability will ignore the information of these two attributes and will not pass them to other neighbors.

2. Address Family

   BGP uses address family to distinguish different network layer protocols. For values of address family, see RFC1700 (Assigned Numbers). MP-BGP extension applications, including VPN extension, should be configured in their respective address family views.

7.5.1.4.13 BFD for BGP Features

Bidirectional Forwarding Detection (BFD) is used in IPv4 to accelerate link failure detection for BGP. BFD can quickly detect link failures between BGP peers and report them to BGP, thereby realizing fast convergence of BGP routes.

7.5.1.4.14 BGP GR

When BGP is restarted, the peer relationship is re-established and the forwarding is interrupted. After the graceful restart (GR) function is enabled, traffic interruption can be avoided.

7.5.2 Configuring BGP

7.5.2.1 Configuring Basic BGP4 Functions

Purpose

This section describes how to configure basic BGP4 functions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Access or create a BGP node	1. Access the global configuration view. 2. Run the **router bgp** *as-value* command to access the BGP configuration view.
Specify a router ID for BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **router-id** *router-id* command.
Restore the BGP router ID to the default value	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no router-id** command.
Create a BGP neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **remote-as** *AS-value* command.
Delete a BGP neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no neighbor** *ipv4-address* command.
Shut down a BGP neighbor	1. Access the global configuration view. 2. Run the **router bgp N** command to access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **shutdown** command.
Delete a shutdown BGP neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no neighbor** *ipv4-address* **shutdown** command.
Configure MD5 authentication for a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view.

Purpose	Procedure
	3. Run the **neighbor** *ipv4-address* **password** *password* command.
Delete MD5 authentication for a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no neighbor** *ipv4-address* **password** command.
Configure the maximum keepalive time for a neighbor and an interval for sending keepalive packets to the neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the command **neighbor** *ipv4-address* **keeplive-timer** { *keeplive-timer* | **default** } **hold-timer** { *hold-timer* | **default** }.
Specify the updated source address for a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPN address family view. 3. Run the **neighbor** *ip-address1* **update-source** *ip-address2* command.
Delete the updated source address for a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPN address family view. 3. Run the **no neighbor** *ip-address1* **update-source** command.
Detect the number of valid TTL hops of a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **valid-ttl-hops** { *hops-value* | **default** } command.

7.5.2.2 Configuring BGP4 Route Advertising

Purpose

This section describes how to configure BGP4 route advertising.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable route aggregation and set to send the aggregated route only or send both the aggregated route and non-aggregated routes	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **aggregate** *ipv4-address ipv4mask-length* { **summaryonly** | **all** } command.
Configure the admin status of route aggregation to Up or Down	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **aggregate** *ipv4-address ipv4mask-length* **adminstatus** { **up** | **down** } command.
Delete route aggregation	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no aggregate** *ipv4-address ipv4mask-length* command.
Modify the next hop of the route sent to a neighbor to the local address	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **next-hop-local** command.
Delete the configuration of using the local address as the next hop of the route sent to a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no neighbor** *ipv4-address* **next-hop-local** command.
Enable a neighbor to refresh the routes	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **route-refresh** command
Disable a neighbor from refreshing the routes	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view.

Purpose	Procedure
	3. Run the **no neighbor** *ipv4-address* **route-refresh** command.
Advertise the specified route	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **network** *network-address network-mask* command.
Delete the specified advertised route	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no network** *network-address network-mask* command.
Introduce a static or direct route to BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **redistribute { static | connected | rip | ospf | isis }** command.
Introduce a static or direct route to BGP based on a policy	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **redistribute** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* command.
Modify the MED value of the static or direct route introduced to BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **redistribute** { **static** | **connected** | **rip** | **ospf** | **isis** } **med** *med-value* command.
Delete the route introduced to BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no redistribute { static | connected | rip | ospf | isis }** command.
Delete the route introduced to BGP based on a policy	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no redistribute** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* command.
Enable or disable IGP synchronization	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **synchronization** { **enable** | **disable** } command.

7.5.2.3 Configuring BGP4 Route Attributes

Purpose

This section describes how to configure BGP4 route attributes.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the default MED value	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **default local-med** { *local-med* | **default** } command.
Configure the default local-preference value	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **default local-preference** { *local-preference-value* | **default** } command.
Configure the BGP community attribute	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **community** { *community-value* | **noadvertise** | **noexport** } { **additive** | **replace** | **none** } command.
Delete the BGP community attribute	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no community** command.
Send the community attribute to a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **neighbor** *ipv4-address* **send-community** command.
Cancel sending the community attribute to a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no neighbor** *ipv4-address* **send-community** command.
Configure the loop number of a local AS ID	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **allow-as-loop** { *time-value* | **default** } command.
Set to carry only the public	1. Access the global configuration view. 2. Access the BGP configuration view.

Purpose	Procedure
AS ID, not the private AS ID, in the BGP update packet to be sent	3. Run the **neighbor** *ipv4-address* **public-as-only** command.

7.5.2.4 Configuring BGP4 Route Policies

Purpose

This section describes how to configure BGP4 route policies.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a global import or export filter policy for BGP	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **filter-policy** { **export** | **import** } **route-policy** *route-policy-name* command.
Specify a global export filter policy for BGP based on protocol type	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **filter-policy export { static | connected | rip | ospf | isis } route-policy** *route-policy-name* command.
Delete a global import or export filter policy for BGP	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no filter-policy** { **export** | **import** } **route-policy** *route-policy-name* command.
Delete a global export filter policy for BGP based on protocol type	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no filter-policy export { static | connected | rip | ospf | isis } route-policy** *route-policy-name* command.
Configure an import or export	1. Access the global configuration view. 2. Access the BGP configuration view.

Purpose	Procedure
route policy for a designated neighbor	3. Run the **neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** } command.
Delete an import or export route policy for a designated neighbor	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** } command.

7.5.2.5 Configuring BFD for BGP

Purpose

This section describes how to configure BFD for BGP.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable BFD for a neighbor	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **bfd** { **enable** | **disable** } command.

7.5.2.6 Configuring a BGP4 Route Reflector

Purpose

This section describes how to configure a BGP4 route reflector.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a cluster ID for a route reflector	1. Access the global configuration view. 2. Access the BGP-ipv4 address family configuration view, BGP-vpnv4 address family configuration view, BGP-EVPN address family configuration

Purpose	Procedure
	view, BGP-VPN IPv4 address family configuration view, or BGP-VPN IPv6 address family configuration view. 3. Run the **cluster-id** *router-id* command.
Specify a neighbor as the reflector client	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **neighbor** *ipv4-address* **route-reflector-client** command.
Delete a cluster ID for a route reflector	1. Access the global configuration view. 2. Access the BGP-ipv4 address family configuration view, BGP-vpnv4 address family configuration view, BGP-EVPN address family configuration view, BGP-VPN IPv4 address family configuration view, or BGP-VPN IPv6 address family configuration view. 3. Run the **no cluster-id** command.
Cancel using a neighbor as the reflector client	1. Access the global configuration view. 2. Access the BGP configuration view or BGP-VPNv4 address family view. 3. Run the **no neighbor** *ipv4-address* **route-reflector-client** command.

7.5.2.7 Configuring a BGP4 Confederation

Purpose

This section describes how to configure a BGP4 confederation.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an AS ID for a confederation	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **confederation identifier** { *autonomy-system-number* | *string* } command.
Specify a member for a confederation	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **confederation peer-as** *autonomy-system-number* command.
Delete the AS ID for a confederation	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no confederation identifier** command.

Purpose	Procedure
Delete a designated confederation member	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **no confederation peer-as** *autonomy-system-number* command.

7.5.2.8 Configuring BGP4 GR

Purpose

This section describes how to configure BGP4 GR.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable BGP GR	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **graceful-restart { enable | disable }** command.
Configure the maximum time for recreating a BGP session	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **graceful-restart timer restart** { *restar-timer* | **default** } command.
Configure a time for the restarting speaker and receiving speaker to receive the End-of-RIB message	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **graceful-restart timer selection-deferral {** *select-time* | **default }** command.

7.5.2.9 Configuring a BGP Family Address

Purpose

This section describes how to configure a BGP family address.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enter the IPv4 unicast address family view	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **ipv4-family unicast** command.
Associate a specified VPN instance with the IPv4 address family and access the BGP-VPN instance view	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **ipv4-family vpn-instance** *name* command.
Enable or disable an address group under an address family node	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Access the address family view. 3. Run the **neighbor** *ipv4-address* { **enable** | **disable** } command.

7.5.2.10 Viewing the BGP4 Configuration

Purpose

This section describes how to view the BGP4 configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the BGP aggregation table	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp aggregate** command.

Purpose	Procedure
Display the basic BGP configuration	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp config** command.
Display all BGP peers	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp neighbor** command.
Display the state of a designated BGP peer	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the following commands: ● **show ip bgp neighbor** *ipv4-address* ● **show ip bgp neighbor** *ipv6-address* ● **show ip bgp neighbor orf state** ● **show ipv6 bgp neighbor** *ipv6-address* **error-statistic**
Display statistics about BGP resources	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp resource** command.
Display the BGP routing table	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp route** command.
Display statistics about BGP routes	1. Access the common user view, BGP configuration view, privileged user view, global configuration view, BGP address family configuration view, or BGP-VPNv4 address family view. 2. Run the **show ip bgp summary** command.
Display peers of a BGP VPN instance	1. Access the common user view or privileged user view. 2. Run the **show ip bgp vpn-instance** *name* **neighbor** command.
Display statistics of errors generated in a BGP process	1. Access the global configuration view. 2. Run the following commands: ● **show ip bgp error-statistics** ● **show ip bgp neighbor** *nbr-address* **error-statistics**

7.5.3 BGP Configuration Example

7.5.3.1 Basic BGP4 Configuration

Network Requirements

As shown in Figure 7-29, all switches run BGP. An EBGP connection is created between R1 and R2 and an IBGP full connection is created among R2, R3, and R4.

Network Diagram

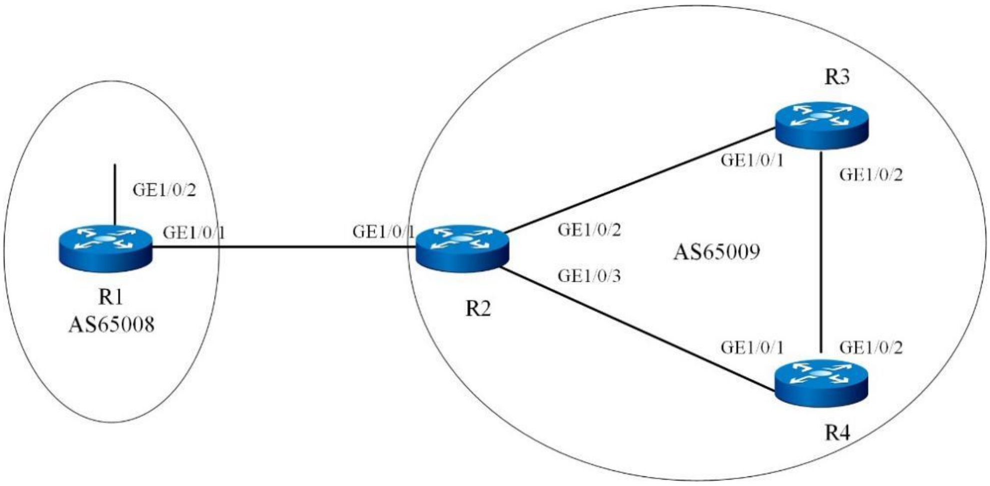


Figure 7-29 Network diagram of basic BGP configuration

Switch	Interface	VLAN	IP Address
R1	Gigaethernet1/0/1	VLAN 10	192.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 50	20.1.1.1/8
R2	Gigaethernet1/0/1	VLAN 10	192.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 20	10.1.3.1/24
R2	Gigaethernet1/0/3	VLAN 30	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	10.1.3.2/24
R3	Gigaethernet1/0/2	VLAN 40	10.1.2.1/24
R4	Gigaethernet1/0/1	VLAN 30	10.1.1.2/24
R4	Gigaethernet1/0/2	VLAN 40	10.1.2.2/24

Configuration Suggestion

Configure basic BGP functions as follows:

1. Create an IBGP connection among R2, R3, and R4.
2. Create an EBGP connection between R1 and R2.
3. Run the **network** command on R1 to advertise the route and view the routing tables of R1, R2, and R3.
4. Introduce a direct route to BGP on R2 and view the routing tables of R1 and R3.

Data Preparation

Prepare the following data to complete the configuration in this example:

VLAN IDs corresponding to the interfaces. See Figure 7-29.

IP addresses of the VLAN interfaces. See Figure 7-29.

The Router ID of R1 is 1.1.1.1 and the AS ID is 65008.

The router IDs of R2, R3, and R4 are 2.2.2.2, 3.3.3.3, and 4.4.4.4, respectively, and their AS ID is 65009.

Configuration

1. Configure an IBGP connection

Configure R2.

R2(config)#router bgp 65009

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 10.1.1.2 remote-as 65009

R2(config-bgp)#neighbor 10.1.3.2 remote-as 65009

Configure R3.

R3(config)#router bgp 65009

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 10.1.3.1 remote-as 65009

R3(config-bgp)#neighbor 10.1.2.2 remote-as 65009

R3(config-bgp)#quit

Configure R4.

R4(config)#router bgp 65009

R4(config-bgp)#router-id 4.4.4.4

R4(config-bgp)#neighbor 10.1.1.1 remote-as 65009

R4(config-bgp)#neighbor 10.1.2.1 remote-as 65009

R4(config-bgp)#quit

2. Configure an EBGP connection

Configure R1.

R1(config)# router bgp 65008

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 192.1.1.1 remote-as 65009

Configure R2.

R2(config-bgp)#neighbor 192.1.1.2 remote-as 65008

R2(config-bgp)#quit

View the connection state of the BGP peer

R1(config)#show ip bgp neighbor

3. Set R1 to advertise the route 20.0.0.0/8

Set R1 to advertise a route.

R1(config-bgp)#network 20.0.0.0 255.0.0.0

R1(config-bgp)#quit

View the R1 routing table.

R1(config)#show ip bgp route

View the R2 routing table.

R2(config)#show ip bgp route

View the R3 routing table.

R1(config)#show ip bgp route

The routing table shows that, R3 has learned the route 20.0.0.0 in AS65008, but the route is invalid since the next hop 192.1.1.2 is not reachable.

4. Introduce a direct route to BGP

Configure R2.

R2(config)#router bgp 65009

R2(config-bgp)#redistribute connect

R2(config-bgp)#quit

View the BGP routing table of R1.

R1(config)#show ip bgp route

View the R3 routing table.

R3(config)#show ip bgp route

The route 20.0.0.0 becomes valid and the next hop is the address of R1.

7.5.3.2 Configuring Interaction Between BGP4 and IGP

Network Requirements

As shown in Figure 7-30, OSPF is used as IGP inside AS65009, an EBGP connection is created between R1 and R2, and R3 runs OSPF, not BGP.

Network Diagram

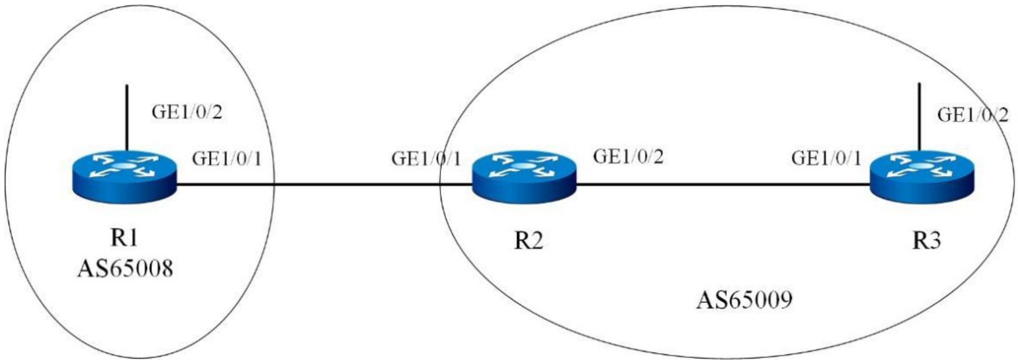


Figure 7-30 Network diagram of configure interaction between BGP and IGP

Switch	Interface	VLAN	IP Address
R1	Gigaethernet1/0/1	VLAN 10	30.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 30	20.1.1.1/24
R2	Gigaethernet1/0/1	VLAN 10	30.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 20	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	10.1.1.2/24
R3	Gigaethernet1/0/2	VLAN 40	10.1.2.1/24

Configuration Suggestion

Configure interaction between BGP and IGP as follows:

1. Enable OSPF for R2 and R3.
2. Create an EBGP connection between R1 and R2.
3. Enable BGP and OSPF to import each other on R2, and check routing information.
4. Enable BGP route aggregation on R2 to simplify the BGP routing table.

Data Preparation

Prepare the following data to complete the configuration in this example:

VLAN IDs corresponding to the interfaces. See Figure 7-30.

IP addresses of the VLAN interfaces. See Figure 7-30.

The Router ID of R1 is 1.1.1.1 and the AS ID is 65008.

The router IDs of R2 and R3 are 2.2.2.2 and 3.3.3.3 respectively, and the AS number is 65009.

Configuration

1. Configure OSPF

Configure R1.

R1(config)#router ospf

R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0

R1(config-ospf-1)#quit

Configure R2.

R1(config)#router ospf

R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0

R1(config-ospf-1)#network 9.1.2.0 255.255.255.0 area 0

R1(config-ospf-1)#quit

2. Configure an EBGP connection

Configure R1.

R1(config)#router bgp 65008

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 3.1.1.1 remote-as 65009

R1(config-bgp)#network 8.1.1.0 255.255.255.0

R1(config-bgp)#quit

Configure R2.

R2(config)#router bgp 65009

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 3.1.1.2 remote-as 65008

3. Configure interaction between BGP and IGP

Enable BGP to import OSPF routes on R2.

R2(config-bgp)#redistribute ospf

R2(config-bgp)#quit

View the R1 routing table.

R1(config)#show ip bgp route

Enable OSPF to import BGP routes on R2.

R2(config)#router ospf

R2(config-ospf-1)#redistribute bgp

R2(config-ospf-1)#quit

View the R3 routing table.

R3(config)#show ip route

4. Enable route aggregation

Configure R2.

R2(config)#router bgp 65009

R2(config-bgp)#aggregate 9.0.0.0 8 summaryonly

R2(config-bgp)#aggregate 9.0.0.0 8 adminstatus up

R2(config-bgp)#quit

View the BGP routing table of R1.

R1(config)#show ip bgp route

7.5.3.3 Configuring a BGP4 Route Reflector

Network Requirements

As shown in Figure 7-31, R1 is a non-client. R2 is the router reflector of Cluster1 and R4 and R5 are its clients. An IBGP connection is created between them, and thus routes do not need to be reflected between clients. R3 is the router reflector of Cluster2, and R6, R7, and R8 are its clients. A peer group is required to simplify configuration and management.

Network Diagram

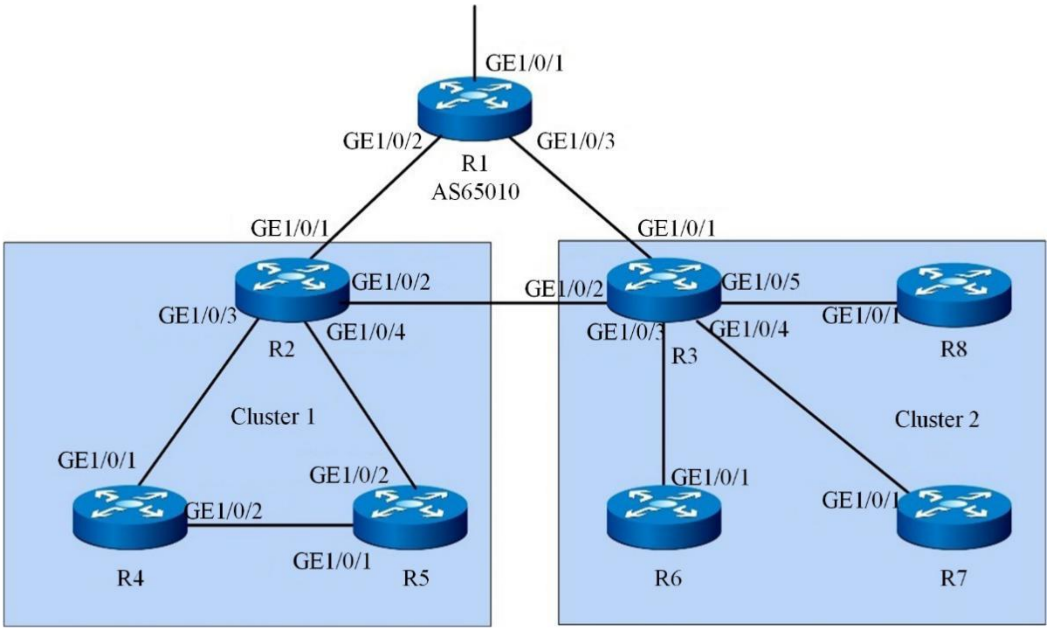


Figure 7-31 Network diagram of configuring a BGP router reflector

Switch	Interface	VLAN	IP Address
R1	Gigaethernet 1/0/1	VLAN 10	10.1.1.2/24
R1	Gigaethernet 1/0/2	VLAN 30	10.1.3.2/24
R1	Gigaethernet 1/0/3	VLAN 100	9.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 10	10.1.1.1/24
R2	Gigaethernet 1/0/2	VLAN 20	10.1.2.1/24
R2	Gigaethernet 1/0/3	VLAN 40	10.1.4.1/24
R2	Gigaethernet 1/0/4	VLAN 50	10.1.5.1/24
R3	Gigaethernet 1/0/1	VLAN 30	10.1.3.1/24
R3	Gigaethernet 1/0/2	VLAN 20	10.1.2.2/24

R3	Gigaethernet 1/0/3	VLAN 70	10.1.7.1/24
R3	Gigaethernet 1/0/4	VLAN 80	10.1.8.1/24
R3	Gigaethernet 1/0/5	VLAN 90	10.1.9.1/24
R4	Gigaethernet 1/0/1	VLAN 40	10.1.4.2/24
R4	Gigaethernet 1/0/2	VLAN 60	10.1.6.1/24
R5	Gigaethernet 1/0/1	VLAN 50	10.1.5.2/24
R5	Gigaethernet 1/0/2	VLAN 60	10.1.6.2/24
R6	Gigaethernet 1/0/1	VLAN 70	10.1.7.2/24
R7	Gigaethernet 1/0/1	VLAN 80	10.1.8.2/24
R8	Gigaethernet 1/0/1	VLAN 90	10.1.9.2/24

Configuration Suggestion

Configure a BGP router reflector as follows:

1. Create an IBGP connection between clients and the router reflectors and between non-clients and router reflectors.
2. Set R2 and R3 to router reflectors, specify clients, and view the routing information.

Data Preparation

Prepare the following data to complete the configuration in this example:

VLAN IDs corresponding to the interfaces. See Figure 7-31.

IP addresses of the VLANIF interfaces. See Figure 7-31.

The AS ID of all switches is AS10.

The router IDs of R1 to R8 are 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4, 5.5.5.5, 6.6.6.6, 7.7.7.7, and 8.8.8.8, respectively.

The cluster IDs of R2 and R3 are 1 and 2 respectively.

Configuration

1. Create an IBGP connection between clients the router reflectors and between non-clients and router reflectors (omitted).
2. Set R1 to advertise the local network route 9.1.1.0/24 (omitted).
3. Configure router reflectors.

Configure R2.

R2(config)#router bgp 65010

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 10.1.4.2 route-reflector-client

R2(config-bgp)#neighbor 10.1.5.2 route-reflector-client

R2(config-bgp)#cluster-id 10.10.10.10

R2(config-bgp)#quit

Configure R3.

R3(config)#router bgp 65010

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 10.1.7.2 route-reflector-client

R3(config-bgp)#neighbor 10.1.8.2 route-reflector-client

R3(config-bgp)#neighbor 10.1.9.2 route-reflector-client

R3(config-bgp)#cluster-id 20.20.20.20

R3(config-bgp)#quit

View the R4 routing table.

R4(config)#show ip bgp route

As shown in the routing table, R4 has learned from R2 the router advertised by R1.

7.5.3.4 Configuring a BGP4 Confederation

Network Requirements

As shown in Figure 7-32, multiple devices in the network run BGP. To reduce the number of IBGP connections, divide these devices into three sub-ASs: AS6500, AS65002, and AS65003. An IBGP full connection is created among three devices in AS65001.

Network Diagram

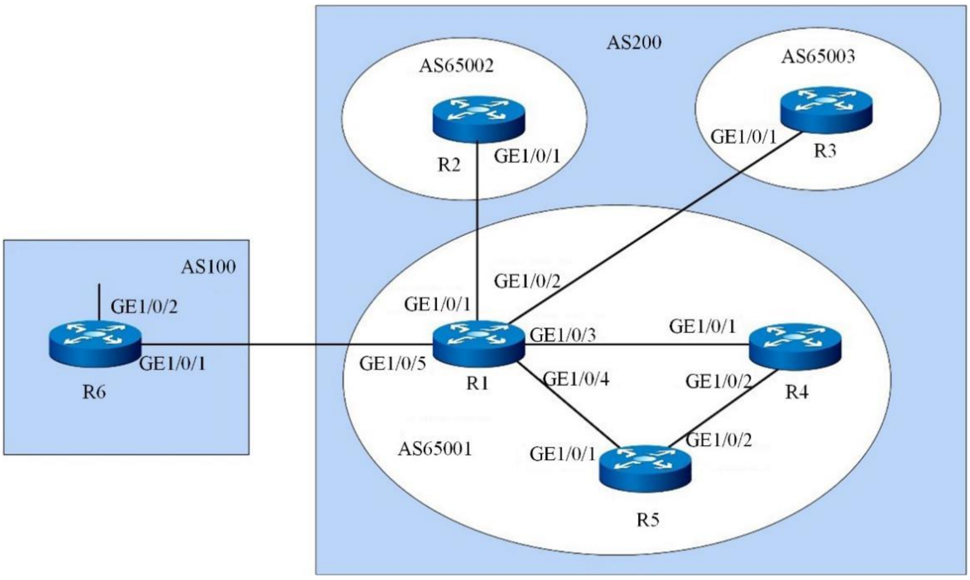


Figure 7-32 Network diagram of configuring a confederation

Switch	Interface	VLAN	IP Address
R1	Gigaethernet 1/0/1	VLAN 10	10.1.1.1/24
R1	Gigaethernet 1/0/2	VLAN 20	10.1.2.1/24
R1	Gigaethernet 1/0/3	VLAN 30	10.1.3.1/24
R1	Gigaethernet 1/0/4	VLAN 40	10.1.4.1/24
R1	Gigaethernet 1/0/5	VLAN 60	200.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 10	10.1.1.2/24
R3	Gigaethernet 1/0/1	VLAN 20	10.1.2.2/24
R4	Gigaethernet 1/0/1	VLAN 30	10.1.3.2/24
R4	Gigaethernet 1/0/2	VLAN 50	10.1.5.1/24
R5	Gigaethernet 1/0/1	VLAN 40	10.1.4.2/24
R5	Gigaethernet 1/0/2	VLAN 50	10.1.5.2/24
R6	Gigaethernet 1/0/1	VLAN 60	200.1.1.2/24
R6	Gigaethernet 1/0/2	VLAN 70	9.1.1.1/24

Configuration Suggestion

Configure a BGP confederation as follows:

1. Configure a BGP confederation for switches in AS200.
2. Create an IBGP connection in AS65001.
3. Create an EBGP connection between AS100 and AS200, and view the routing information.

Data Preparation

Prepare the following data to complete the configuration in this example:

VLAN IDs corresponding to the interfaces. See Figure 7-32.

IP addresses of the VLANIF interfaces. See Figure 7-32.

The router IDs of R1 to R6 are 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4, 5.5.5.5, and 6.6.6.6, respectively.

The IDs of two ASs are AS100 and AS200. AS200 is divided into 3 sub-ASs: AS65001, AS65002, and AS65003.

Configuration

1. Configure a BGP confederation.

Configure R1.

R1(config)#router bgp 65001

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#confederation identifier 200

R1(config-bgp)#confederation peer-as 65002

R1(config-bgp)#confederation peer-as 65003

R1(config-bgp)#neighbor 10.1.1.2 remote-as 65002

R1(config-bgp)#neighbor 10.1.2.2 remote-as 65003

R1(config-bgp)#neighbor 10.1.1.2 next-hop-local

R1(config-bgp)#neighbor 10.1.2.2 next-hop-local

R1(config-bgp)#quit

Configure R2.

R2(config)#router bgp 65002

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#confederation identifier 200

R2(config-bgp)#confederation peer-as 65001

R2(config-bgp)#confederation peer-as 65003

R2(config-bgp)#neighbor 10.1.1.1 remote-as 65001

R2(config-bgp)#quit

Configure R3.

R3(config)#router bgp 65003

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#confederation identifier 200

R3(config-bgp)#confederation peer-as 65001

R3(config-bgp)#confederation peer-as 65002

R3(config-bgp)#neighbor 10.1.2.1 remote-as 65001

R3(config-bgp)#quit

2. Create an IBGP connection inside AS65001.

Configure R1.

R1(config)#router bgp 65001

R1(config-bgp)#neighbor 10.1.3.2 remote-as 65001

R1(config-bgp)#neighbor 10.1.4.2 remote-as 65001

R1(config-bgp)#neighbor 10.1.3.2 next-hop-local

R1(config-bgp)#neighbor 10.1.4.2 next-hop-local

R1(config-bgp)#quit

Configure R4.

R4(config)#router bgp 65001

R4(config-bgp)#router-id 4.4.4.4

R4(config-bgp)#neighbor 10.1.3.1 remote-as 65001

R4(config-bgp)#neighbor 10.1.5.2 remote-as 65001

R4(config-bgp)#quit

Configure R5.

R5(config)#router bgp 65001

R5(config-bgp)#router-id 5.5.5.5

R5(config-bgp)#neighbor 10.1.4.1 remote-as 65001

R5(config-bgp)#neighbor 10.1.5.1 remote-as 65001

R5(config-bgp)#quit

3. Create an EBGP connection between AS100 and AS200.

Configure R1.

R1(config)#router bgp 65001

R1(config-bgp)#neighbor 200.1.1.2 remote-as 100

R1(config-bgp)#quit

Configure R6.

R6(config)#router bgp 100

R6(config-bgp)#router-id 6.6.6.6

R6(config-bgp)#neighbor 200.1.1.1 remote-as 200

R6(config-bgp)#network 9.1.1.0 255.255.255.0

R6(config-bgp)#quit

4. View the configuration result.

View the BGP routing table of R2.

R2(config)#show ip bgp route

View the BGP routing table of R4.

R4(config)#show ip bgp route

7.5.3.5 Configuring BFD for BGP

Network Requirements

As shown in Figure 7-33, R1 belongs to AS100, R2 and R3 belong to AS200, and an EBGP connection is created between R1 and R2 and between R1 and R3. The service traffic is transmitted on the primary link (R1 > R2). The link R1 > R3 > R2 is a backup link. BFD is enabled to detect the BGP neighbor relationship between R1 and R2. When the link between R1 and R2 fails, BFD can quickly detect the fault and notify it to BGP, and then the service traffic is transmitted on the backup link.

Network Diagram

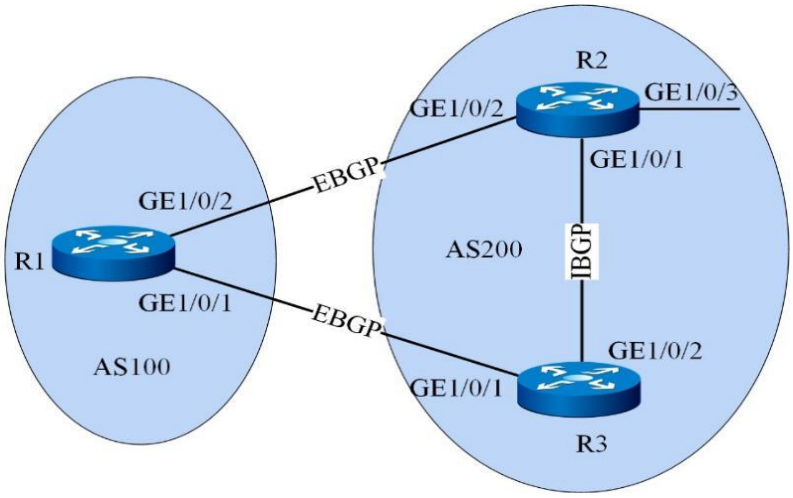


Figure 7-33 Network diagram of configuring BFD for BGP

Switch	Interface	VLAN	IP Address
R1	Gigaethernet 1/0/1	VLAN 10	200.1.2.1/24
R1	Gigaethernet 1/0/2	VLAN 20	200.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 30	9.1.1.1/24
R2	Gigaethernet 1/0/2	VLAN 20	200.1.1.2/24
R2	Gigaethernet 1/0/3	VLAN 40	192.1.1.1/24
R3	Gigaethernet 1/0/1	VLAN 10	200.1.2.2/24
R3	Gigaethernet 1/0/2	VLAN 30	9.1.1.2/24

Configuration Suggestion

Configure BFD for BGP as follows:

1. Configure basic BGP functions on each switch.
2. Configure a MED value to control route selection.
3. Enable BFD on R1 and R2.

Data Preparation

Prepare the following data to complete the configuration in this example:

Router IDs and AS IDs of R1, R2, and R3.

Peer IP address detected by BFD.

Minimum sending interval and minimum receiving interval of BFD control packets, and local detection multiple.

Configuration

1. Configure basic BGP functions, create an EBGP connection between R1 and R2 and between R1 and R3, and create an IBGP connection between R2 and R3.

Configure R1.

```
R1(config)#router bgp 100
R1(config-bgp)#router-id 1.1.1.1
R1(config-bgp)#neighbor 200.1.1.2 remote-as 200
R1(config-bgp)#neighbor 200.1.2.2 remote-as 200
R1(config-bgp)#quit
```

Configure R2.

```
R2(config)#router bgp 200
R2(config-bgp)#router-id 2.2.2.2
R2(config-bgp)#neighbor 200.1.1.1 remote-as 100
R2(config-bgp)#neighbor 9.1.1.2 remote-as 200
```

R2(config-bgp)#network 9.1.1.0 255.255.255.0
R2(config-bgp)#quit
Configure R3.
R3(config)#router bgp 200
R3(config-bgp)#router-id 3.3.3.3
R3(config-bgp)#neighbor 200.1.2.1 remote-as 100
R3(config-bgp)#neighbor 9.1.1.1 remote-as 200
R3(config-bgp)#network 9.1.1.0 255.255.255.0
R3(config-bgp)#network 192.1.1.0 255.255.255.0
R3(config-bgp)#quit
On R1, check whether a BGP neighbor is established.
R1(config-bgp)#show ip bgp neighbor

2. Configure the MED value.
Configure the MED values sent by R2 and R3 to R1 according to the policy.
Configure R2.
R2(config)#route-policy 10 permit node 10
R2(config-route-policy)#apply cost 100
R2(config-route-policy)#quit
R2(config)#router bgp 200
R2(config-bgp)#neighbor 200.1.1.2 route-policy 10 export
Configure R3.
R3(config)#route-policy 10 permit node 10
R3(config-route-policy)#apply cost 150
R3(config-route-policy)#quit
R3(config)#router bgp 200
R3(config-bgp)#neighbor 200.1.2.2 route-policy 10 export
View all BGP routes on R1.
R1(config-bgp)#show ip bgp route
As shown in the BGP routing table, the next hop address of the route destined to 192.1.1.0/24 is 200.1.1.2.
The traffic is transmitted on the primary link R1 > R2.

3. Enable BFD and configure the sending and receiving intervals, and local detection multiple.

Enable BFD for R1.

R1(config)#bfd enable

R1(config)#router bgp 100

R1(config-bgp)#neighbor 200.1.1.2 bfd enable

Enable BFD for R2.

R2(config)#bfd enable

R2(config)#router bgp 200

R2(config-bgp)#neighbor 200.1.1.1 bfd enable

Display all BFD sessions established by BGP on R1.

R1(config)#show ip bfd session

4. View the configuration result.

Run the **shutdown** command for VLAN20 of R2 to simulate a primary link fault.

R2(config)#interface vlan 20

R2(config-vlan-20)#shutdown

View the BGP routing table on R1.

R1(config)#show ip bgp route

As shown in the BGP routing table, after the primary link fails, the backup link R1 > R3 > R2 becomes valid. The next hop address of the route destined to 192.1.1.0/24 is 200.1.2.2.

7.6 Configuring ISIS

7.6.1 ISIS Overview

7.6.1.1 Background Information

Internet is developing quickly and used by more and more users with different needs, and thousands of network terminals communicate with each other via Internet. Therefore, dynamic routing protocols are required by intermediate devices (routers and L3 switches) on networks to guide packet forwarding and provide accurate and effective routing information for packet forwarding. The Intermediate System-to-Intermediate System intra-domain routing information exchange protocol (ISIS) ensures good scalability and supports IP network layer protocols.

ISIS is a dynamic routing protocol designed by the International Organization for Standardization (ISO) for the Connectionless Network Protocol (CLNP). To support IP routes, IETF extended and modified ISIS in RFC 1195, so that ISIS can be applied in both TCP/IP and OSI environments, which is called Integrated ISIS or Dual ISIS.

7.6.1.2 Introduction

ISIS belongs to Interior Gateway Protocol (IGP) and is used inside ASs. ISIS is a link state protocol that uses Shortest Path First (SPF) algorithm for route calculation. The following are basic ISIS concepts:

1. IS: Intermediate System. Equivalent to a router in TCP/IP, it is a basic unit for generating routes and transmitting routing information in ISIS. In the following text, IS and router have the same meaning.
2. RD: Routing Domain. A group of ISs in a routing domain exchange routing information through the same routing protocol.
3. Area: a sub-unit of a routing domain. ISIS allows users to divide a routing domain into multiple areas.
4. LSDB: Link State Database. All the connection states in a network form a link state database, and there is at least one LSDB in each IS. An IS uses the SPF algorithm and uses the LSDB to generate its own routes.
5. LSP: Link State Protocol Data Unit. In ISIS, each IS generates at least one LSP that contains all link state information of the IS. Each IS collects all LSPs in the area and locally generated LSPs to form its own LSDB.

7.6.1.3 Functions and Features

ISIS runs directly on the link layer. Its working process consists of establishing a neighbor relationship, synchronizing LSDBs, and calculating routes.
The process of forming a neighbor relationship varies with the type of network, and the conditions for establishing adjacency are:

- Only neighboring routers at the same layer can become neighboring routers.
- For Level-1 routers, the area addresses must be the same.
- They must be in the same network segment.

Link state database synchronization is implemented through LSP, CSNP, and PSNP packets. A router must be elected as DIS in a LAN, and DIS is responsible for creating and updating pseudo nodes in the broadcast network and maintaining a link state database in the LAN.
For Level-1-2 devices, both Level-1 and Level-2 databases are maintained, and Level-1 and Level-2 devices run the same SPF algorithm. Based on the link state database, ISIS uses the SPF algorithm to calculate the shortest path to other devices in the network topology, and create a routing table based on the shortest path tree.

7.6.1.4 Protocol Description

ISIS can run on point-to-point links (such as PPP and HDLC) or broadcast links (such as Ethernet and Token-Ring). Links on Non-Broadcast Multi-Access (NBMA) networks such as ATM are also treated as P2P links. For such links, users can only run the **CLNS MAP** command to configure a PVC. ISIS cannot run on point to multipoint links.
To support large routing networks, ISIS adopts a two-level hierarchical structure in the routing domain. A large routing domain is divided into one or more areas. Intra-area routes are managed by Level-1 routers, and inter-area routes are managed by Level-2 routers.

1. Level-1 router: A Level-1 router is responsible for routing within an area. It only forms an adjacency relationship with other Level-1 routers in the same area, and maintains a Level-1 LSDB which contains routing information in this area. Packets destined to devices outside the area are forwarded to the nearest Level-1-2 router.

2. Level-2 router: A Level-2 router is responsible for routing between areas. It can form an adjacency relationship with Level-2 routers in another area, and maintains a Level-2 LSDB which contains routing information between areas. All Level-2 routers and Level-1-2 routers form the backbone network of a routing domain and are responsible for communication between different areas. Level-2 routers in a routing domain must be physically continuous to ensure the continuity of the backbone network.
3. Level-1-2 router: A router belonging to both Level-1 and Level-2 is called a Level-1-2 router. Each area has at least one Level-1-2 router to connect the area to the backbone network. It maintains two LSDBs, of which the Level-1 LSDB is used for intra-area routing, and the Level-2 LSDB is used for inter-area routing.

Figure 7-34 shows a classic ISIS-based network topology, where Area5 is the backbone area and all routers in this area are Level-2 routers. The other four areas are non-backbone areas, and they are all connected to the backbone router through Level-1-2 routers.

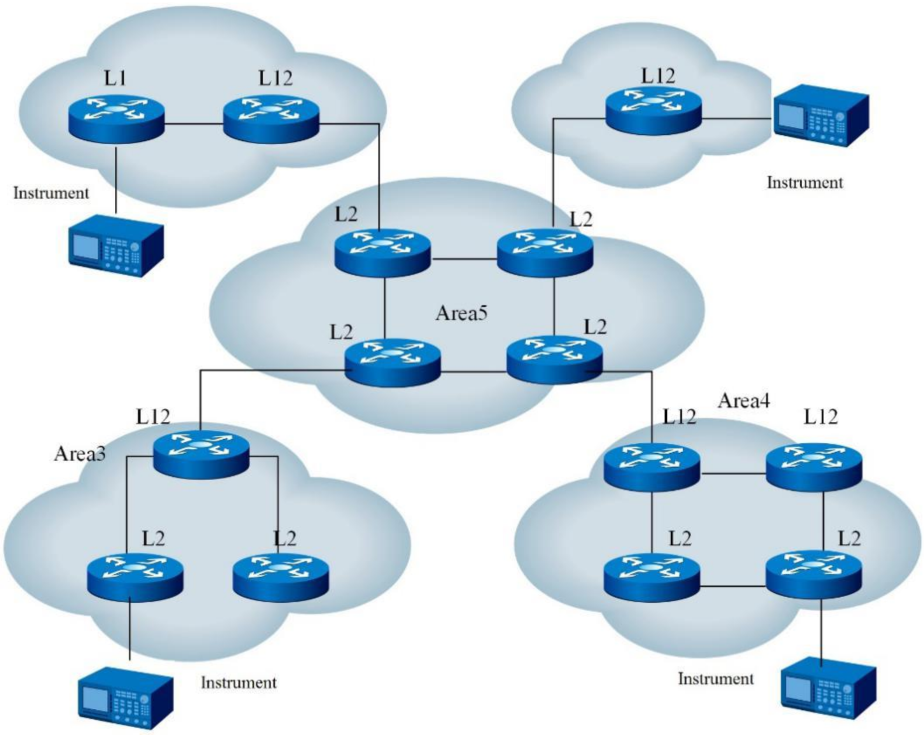


Figure 7-34 Typical ISIS network topology

ISIS packets are directly encapsulated in data link frames, and are divided into three categories:

1. Hello packet: used to establish and maintain adjacencies, also known as IIH (IS-to-IS Hello PDUs). Level-1 routers in a broadcast network use Level-1 LAN IIH, Level-2 routers in a broadcast network use Level-2 LAN IIH, and the routers in a P2P network use P2P IIH.
2. LSP (Link State PDUs) packet: used to exchange link state information. LSPs are divided into Level-1 LSP and Level-2 LSP. Level-1 routers transmit Level-1 LSP, Level-2 routers transmit Level-2 LSP, and Level-1-2 routers transmit both Level-1 LSP and Level-2 LSP.
3. SNP (Sequence Number PDUs) packet: used to confirm the latest received LSP between neighbors, similar to the acknowledge packet, but more effective. SNPs include CSNP (Complete SNP) and PSNP (Partial SNP), which can be further divided into Level-1 CSNP, Level-2 CSNP, Level-1 PSNP, and Level-2 PSNP. CSNP carries summary information of all LSPs in the LSDBs, so that the synchronization of the LSDBs can be maintained between adjacent routers. On a broadcast network, CSNP is sent periodically by DIS (the default interval is 10 seconds). On a P2P link, CSNP is sent only when an adjacency is established for the first time. PSNP only enumerates the sequence numbers of one or more LSPs recently received, and it can confirm multiple LSPs at a time. When LSDBs are not synchronized, PSNP is also used to request the neighbor to send a new LSP.

According to RFC1195, Integrated ISIS can run in an environment in which both OSI and IP are enabled. It can not only dynamically discover and generate IP routes, but also discover and generate CLNS routes. ISISv6 can run in an IPv4 environment and can dynamically discover and generate IPv4 routes.

ISIS uses Hello packets to discover neighboring routers on the same link and establish adjacencies. The ISIS-enabled router periodically sends Hello packets from each ISIS-enabled interface. If an ISIS Hello packet is received by a router on the same link, and the Hello packet sent by the peer router passes the protocol check and interface address check, an adjacency relationship will be established with the peer. Figure 7-35 and Figure 7-36 show how a LAN and a P2P interface establish a neighboring relationship, respectively. After the neighbor relationship is established, Hello packets are sent periodically to maintain the neighbor relationship. An IPv4 adjacency can be established between ISs.

1. If an IPv4 adjacency (IPv4-only) needs to be established between ISs, both interfaces need to be enabled with ISIS and configured with valid IPv4 addresses and be in the same network segment (for a P2P network, the IP addresses of routers at two ends can be in different network segments when the following function is enabled: do not check the peer IP address when a PPP interface is allowed to receive Hello packets).

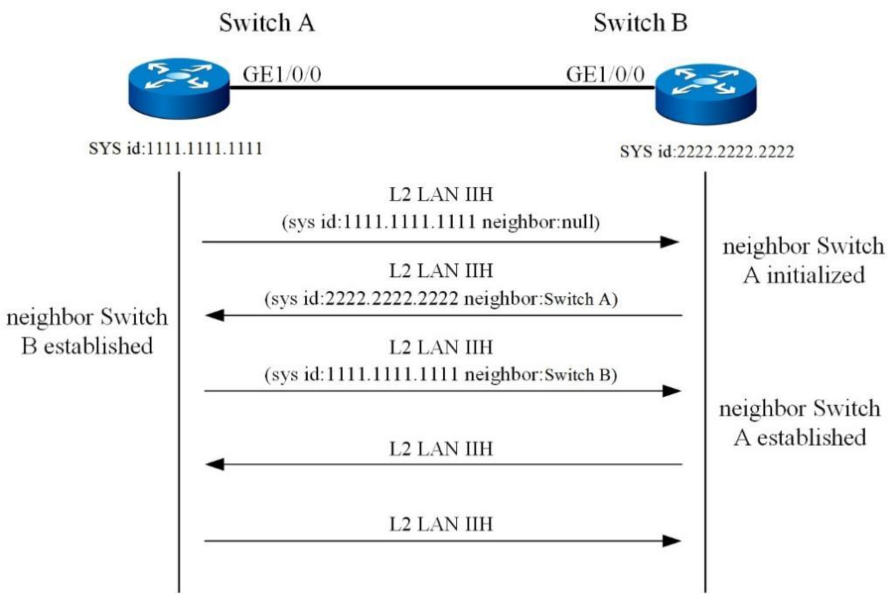


Figure 7-35 Flowchart of establishing a neighbor relationship on a broadcast link

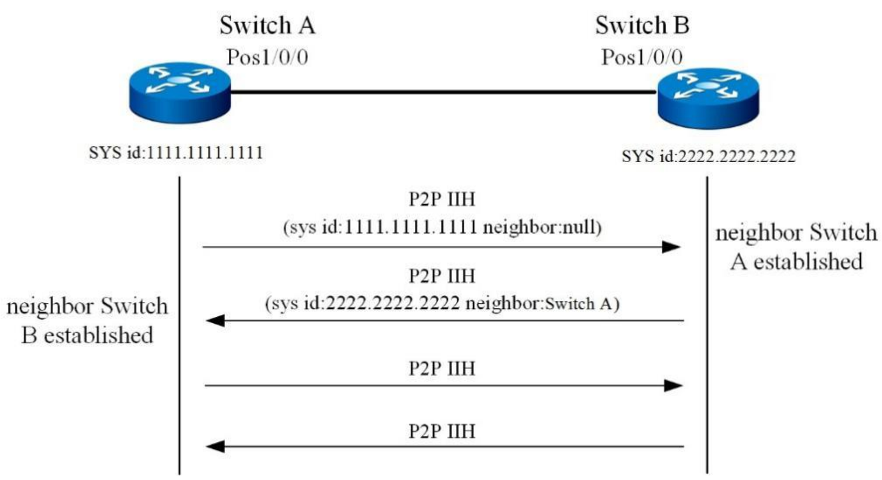


Figure 7-36 Flowchart of establishing a neighbor relationship on a P2P link

After ISIS establishes a neighbor relationship, for broadcast links, it selects a DIS for maintaining database updates and uses LSP flooding and SNP packets to synchronize databases. For P2P link, it directly uses CSNP and PSNP for database synchronization. LSP packet flooding means that, after a router advertises its own LSP to its neighboring routers, the neighboring routers transmit the same LSP packet to other neighbors except for the router that sent the LSP. In this way, the LSP is transmitted via the entire hierarchy. By flooding, every router in the entire hierarchy can have the same LSP and keep LSDBs synchronized. Figure 7-37 And Figure 7-38 show how ISIS synchronizes databases on a broadcast link and a P2P link respectively

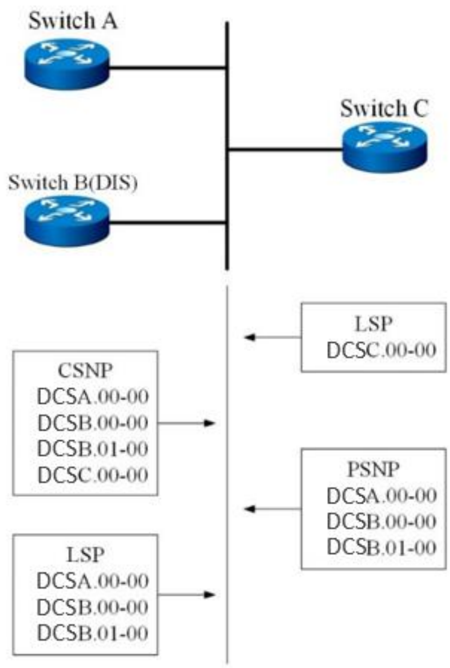


Figure 7-37 Flowchart of synchronizing databases on a broadcast link

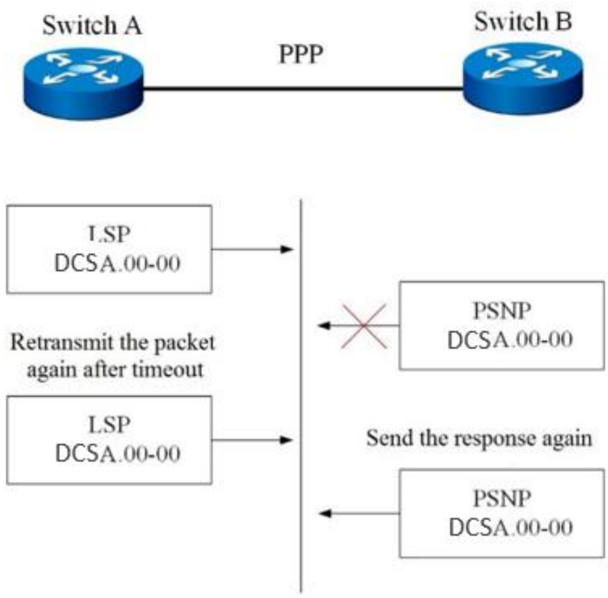


Figure 7-38 Flowchart of synchronizing databases on a P2P link

After synchronizing databases, ISIS uses the SPF algorithm to calculate the loop-free SPF tree according to the link state information in the databases, and restricts the route calculation type according to the type of the adjacency relationship established with neighbors:

When an IPv4 adjacency relationship is established with a neighbor, only IPv4 routes are calculated and generated.

7.6.2 Configuring ISIS

7.6.2.1 Basic ISIS Configuration

Purpose

This section describes basic ISIS configuration, including enabling all ISIS interfaces, enabling ISIS for an interface and starting an ISIS process, configuring a network entity title, and setting a global ISIS overload bit.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable an ISIS instance	1. Access the global configuration view. 2. Run the **router isis** command to access the ISIS configuration view. 3. Run the **router isis** *isis-instance-id* command to start an ISIS instance with the designated ID.
Disable an ISIS instance	1. Access the global configuration view. 2. Run the **no router isis** *isis-instance-id* command to disable an ISIS instance with the designated ID.
Enable ISIS for an interface and specify the ISIS process ID to be associated	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **ip router isis** [*instance-ID*] command.
Disable ISIS for an interface and specify the ISIS process ID to be disassociated	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **no ip router isis** command.
Configure an ISIS network entity title	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **net** *network-entity-title* command.
Delete an ISIS network entity title	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **no net** *network-entity-title* command.
Set a global ISIS overload bit	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **set-overload-bit** command.
Cancel a configured global ISIS overload bit	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **no set-overload-bit** command.

7.6.2.2 Configuring Basic ISIS Parameters

Purpose

This section describes how to configure basic ISIS parameters, including the interface link, interface priority, and packet interval.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an interval for ISIS to send CSNP packets on a broadcast unit or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis csnp-interval { level-1 | level-2 | ppp }** *interval-value* ● **no isis csnp-interval { level-1 | level-2 | ppp }**
Enable an interface to send ISIS packets or disable the function	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, or interface group configuration view. 3. Run the **isis passive-interface or no isis passive-interface** command.
Configure an interval for an ISIS interface to send Hello packets or cancel the configuration	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Access the VLANIF configuration view, interface group configuration view, or loopback interface configuration view. 3. Run the following commands: ● **isis hello-interval { level-1 | level-2 | ppp }** *hello-interval-time* ● **no isis hello-interval { level-1 | level-2 | ppp }**
Configure a multiplier of ISIS hello packet retention interval or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view or interface group configuration view. 3. Run the following commands: ● **isis hello-multiplier { level-1 | level-2 | ppp }** *multiple-value* ● **no isis hello-multiplier { level-1 | level-2 | ppp }**
Configure an overhead for	1. Access the global configuration view.

Purpose	Procedure
links under an ISIS interface or cancel the configuration	2. Access the VLANIF configuration view or interface group configuration view. 3. Run the following commands: ● **isis default-metric { level-1 | level-2 | ppp }** *default-metric* ● **no isis default-metric { level-1 | level-2 | ppp }**
Configure a wide overhead for an interface or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis wide-metric { level-1 | level-2 | ppp }** *metric* ● **no isis wide-metric { level-1 | level-2 | ppp }**
Configure a priority for an ISIS interface for DIS election, or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis priority { level-1 | level-2 }** *priority-value* ● **no isis priority { level-1 | level-2 }**
Enable or disable the three-way handshake function for an ISIS interface, for P2P interfaces only	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis three-way-handshake** ● **no isis three-way-handshake**
Configure an interval for an ISIS interface to send PSNP packets, or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis psnp-interval { level-1 | level-2 | ppp }** *interval-value* ● **no isis psnp-interval { level-1 | level-2 | ppp }**
Configure a circuit type for an ISIS interface	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, or interface group configuration view. 3. Run the **isis circuit-type { broadcast | ppp }** command.
Enable or disable the automatic	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, or interface group configuration view.

Purpose	Procedure
padding function for Hello packets sent by an ISIS interface	3. Run the following commands: ● **isis hello padding** ● **no isis hello padding**
Add an ISIS interface to a designated mesh group or cancel the configuration	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, or interface group configuration view. 3. Run the following commands: ● **isis mesh-group** *group-value* ● **no isis mesh-group**
Enable the mesh group blocking function for an ISIS interface	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, or interface group configuration view. 3. Run the **isis mesh-group blocked** command.

7.6.2.3 Configuring an ISIS Circuit Level

Purpose

The section describes how to configure an ISIS circuit layer, including configuring a global system level, interface level, and level import and export overhead type.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a circuit level for an ISIS interface or restore its circuit level to the default value	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis circuit-level { level-1 | level-1-2 | level-2 }** ● **no isis circuit-level**
Configure a global ISIS system level	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **is-type { level-1 | level-1-2 | level-2 }** command.

7.6.2.4 Configuring ISIS LSP

Purpose

This section describes how to configure ISIS LSP, including configuring an LSP refresh interval, and maximum lifetime, enabling checking checksum of the received LSP packets globally, and enabling receiving MTU values of LSP packets globally.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an LSP refresh interval for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **lsp-refresh-interval** *interval-value* command.
Configure a maximum LSP lifetime for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **max-lsp-lifetime** *lifetime* command.
Enable or disable checking the checksum of the received LSP packets for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **ignore-lsp-errors { level-1 | level-2 }** ● **no ignore-lsp-errors { level-1 | level-2 }**

7.6.2.5 Configuring ISIS Redistribution

Purpose

This section describes how to configure ISIS redistribution, including enabling or disabling route redistribution, and enabling or disabling redirecting a Level-2 ISIS route to a level-1 route.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable route redistribution and introduce routing information of other routing protocols	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **redistribute { connect | static | rip | bgp | ospf | isis } { level-1 | level-2 | level-1-2 }** ● **no redistribute { connect | static | rip | bgp | ospf | isis }**
Enable or disable redirecting a Level-2 ISIS route to a level-1 route	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **redistribute level-2 to level-1** ● **no redistribute level-2 to level-1**

7.6.2.6 Configuring ISIS Route Aggregation

Purpose

This section describes how to configure ISIS route aggregation, including enabling or disabling an ISIS aggregated route.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable an ISIS aggregated route	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **summary-address** *(A.B.C.D) (A.B.C.D)* **{ level-1 | level-2 }** ● **no summary-address** *(A.B.C.D) (A.B.C.D)* **{ level-1 | level-2 }**

7.6.2.7 Configuring ISIS Authentication

Purpose

This section describes how to configure ISIS authentication, including enabling or disabling area authentication or domain authentication for all ISIS interfaces, and enabling or disabling an ISIS interface to authenticate Hello packets in a designated manner and with a designated password.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable area authentication for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **area-password { simple | md5 }** *password* ● **no area-password**
Enable or disable domain authentication for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **domain-password { simple | md5 }** *password* ● **no domain-password**
Enable an ISIS interface to authenticate Hello packets in a designated manner and with a designated password or disable the function	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the following commands: ● **isis password { simple | md5 }** *password* **{ level-1 | level-2 | ppp }** ● **no isis password { level-1 | level-2 | ppp }**

7.6.2.8 Configuring ISIS BFD

Purpose

This section describes how to configure ISIS BFD, including enabling or disabling BFD for an ISIS interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable BFD for an ISIS interface	1. Access the global configuration view. 2. Access the VLANIF configuration view or loopback interface configuration view. 3. Run the **isis bfd** { **enable** | **disable** } command.

7.6.2.9 Configuring ISIS GR

Purpose

This section describes how to configure ISIS GR, including enabling or disabling GR for all ISIS interfaces.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable GR for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **graceful-restart enable** ● **graceful-restart disable**

7.6.2.10 Enabling Other ISIS Function Modules

Purpose

This section describes how to enable or disable other ISIS function modules, including enabling or disabling TE, FRR, and SNMP alarm for all interfaces.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable TE for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **traffic-engineer { enable | disable } { level-1 | level-2 }** command.
Enable or disable FRR for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the **frr** { **enable** | **disable** } command.
Enable or disable SNMP alarm for all ISIS interfaces	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **snmp-trap enable** ● **snmp-trap disable**
Enable ISIS to identify the hostname in an LSP packet, configure a dynamic hostname for an ISIS system on the local switch, and advertise the hostname as an LSP packet, or disable the function	1. Access the global configuration view. 2. Access the ISIS configuration view. 3. Run the following commands: ● **hostname** *host-name* ● **no hostname**

7.6.2.11 Viewing the ISIS Configuration

Purpose

This section describes how to view the ISIS configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display information about an ISIS database of a designated level	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis database** { **level-1** | **level-2** } *instance-id* command.
Display information about an LSDB.	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the following commands: ● **show ip isis database** ● **show ip isis database verbose** ● **show ip isis database verbose** *lsp-index*
Display statistics of an LSDB.	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis database count** command.
Display details about an ISIS neighbor	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis neighbor verbose** command.
Display information about an ISIS neighbor	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis neighbor** command.
Display the basic ISIS configuration	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis config** command.

Purpose	Procedure
Display mapping of the ISIS dynamic host	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis hostname** command.
Display information about an ISIS interface	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis interface** command.
Display details about an ISIS interface	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis interface verbose** command.
Display information about an ISIS instance	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis** *instance-id* command.
Display information about routes learned by ISIS	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the following commands: ● **show ip isis route** ● **show ip isis route { level-1 | level-2 }** ● **show ip isis route** *dst-ip-address* ● **show ip isis route all**
Display the ISIS FRR information	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, loopback interface configuration view, or ISIS configuration view. 2. Run the **show ip isis frr route** command.

7.6.3 ISIS Configuration Example

7.6.3.1 Configuring Basic ISIS Functions

Network Requirements

This task is to complete basic ISIS configuration to make you familiar with the ISIS configuration process and the roles of AREA, LEVEL, and SYSID in ISIS configuration. The topology is shown in Figure 7-39.

Network Diagram

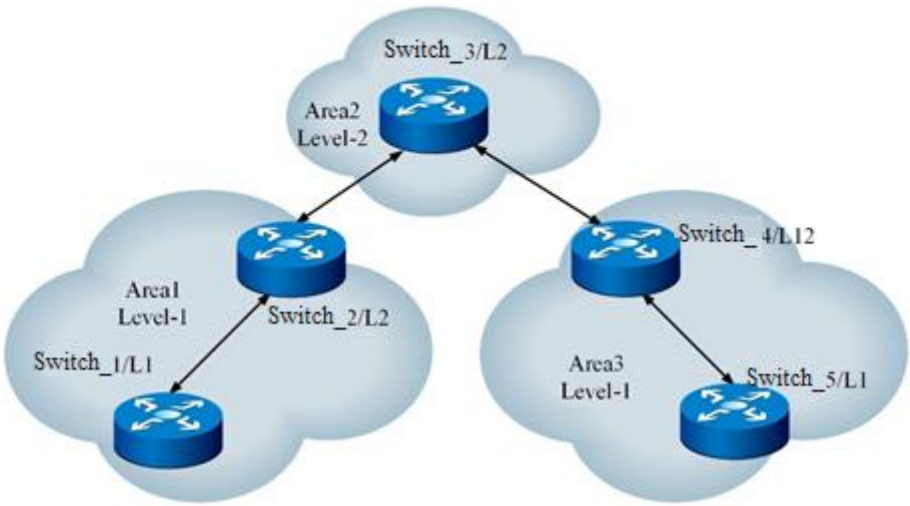


Figure 7-39 Basic ISIS configuration topology

Configuration Suggestion

All devices run ISIS. The AS is divided into 3 areas. Switch_2 and Switch_4 are DISs that transmit the routes between areas.

After configuration, each Level-1 device can only learn all routes in its area, and both Level-1-2 and Level-2 devices can learn routes to all network segments in the AS.

Data Preparation

Area1 and Area3 are Level-1 areas and Area2 is a Level-2 area.

The addresses of Area1, Area2, and Area3 are 10, 20, and 30, respectively.

Switch_1 NET is 10.0001.0001.0001.00 and its interface address is 1.1.1.1/24.

Switch_2 NET is 10.0002.0002.0002.00, and addresses of its two interfaces are 1.1.1.2/24 and 2.1.1.2/24.

Switch_3 NET is 20.0003.0003.0003.00, and addresses of its two interfaces are 2.1.1.1/24 and 3.1.1.1/24.

Switch_4 NET is 30.0004.0004.0004.00, and addresses of its two interfaces are 3.1.1.2/24 and 4.1.1.2/24.

Switch_5 NET is 30.0005.0005.0005.00 and its interface address is 4.1.1.1/24.

Configuration

Switch_1:
Switch_1(config)#router isis
Switch_1(config-isis-1)#net 10.0001.0001.0001.00
Switch_1(config-isis-1)#is-type level-1
Switch_1(config-isis-1)#exit
Switch_1(config)#interface vlan 1
Switch_1(config-vlan-1)#ip router isis

Switch_2:
Switch_2 (config)#router isis
Switch_2 (config-isis-1)#net 10.0002.0002.0002.00
Switch_2 (config-isis-1)#is-type level-1-2
Switch_2 (config-isis-1)#exit
Switch_2 (config)#int vlan 1
Switch_2 (config-vlan-1)#ip router isis
Switch_2 (config-vlan-1)#exit
Switch_2 (config)#int vlan 2
Switch_2 (config-vlan-2)#ip router isis

Switch_3:
Switch_3 (config)#router isis
Switch_3 (config-isis-2)#net 20.0003.0003.0003.00
Switch_3 (config-isis-2)#is-type level-2
Switch_3 (config-isis-2)#exit
Switch_3 (config)#int vlan 2
Switch_3 (config-vlan-2)#ip router isis
Switch_3 (config-vlan-2)#exit
Switch_3 (config)#int vlan 3
Switch_3 (config-vlan-3)#ip router isis

Switch_4:
Switch_4 (config)#router isis
Switch_4 (config-isis-2)#net 30.0004.0004.0004.00
Switch_4 (config-isis-2)#is-type level-1-2
Switch_4 (config-isis-2)#exit
Switch_4 (config)#int vlan 3
Switch_4 (config-vlan-3)#ip router isis
Switch_4 (config-vlan-1)#exit
Switch_4 (config)#int vlan 4
Switch_4 (config-vlan-4)#ip router isis

Switch_5:
Switch_5 (config)#router isis
Switch_5 (config-isis-1)#net 30.0005.0005.0005.00
Switch_5 (config-isis-1)#is-type level-1
Switch_5 (config-isis-1)#exit
Switch_5 (config)#int vlan 4
Switch_5 (config-vlan-4)#ip router isis

Configuration Verification

Run the commands **show ip isis neighbor**, **show ip isis database**, and **show ip isis route** to verify the running results.

7.6.3.2 Configuring ISIS Redistribution

Network Requirements

This case shows how to configure ISIS redistribution to make you familiar with the ISIS redistribution configuration process. The topology is shown in Figure 7-40.

Network Diagram

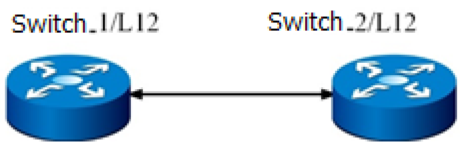


Figure 7-40 ISIS redistribution topology

Configuration Suggestion

Two devices run ISIS and are located in the same area. Assume that Switch_1 has external routes that are learned through other routing protocols and need to be imported to ISIS, but the requirements for external routes are as follows:

1) Receiving all direct routes and redistributing them to level-1 devices.

2) Receiving all RIP routes and redistributing them to level-2 devices.

After configuration, each device can learn the routes destined for all network segments in the AS.

Configuration

Refer to basic ISIS configuration and enable redistribution on Switch_1:

```
Switch_1(config-isis-1)#redistribute connect level-1
Switch_1(config-isis-1)#redistribute rip level-2
```

Configuration Verification

Run the commands **show ip isis database** and **show ip isis route** to verify the running results.

7.6.3.3 Configuring ISIS Route Aggregation

Network Requirements

This case shows how to configure ISIS route aggregation to make you familiar with the ISIS route aggregation configuration process. The topology is shown in Figure 7-41.

Network Diagram

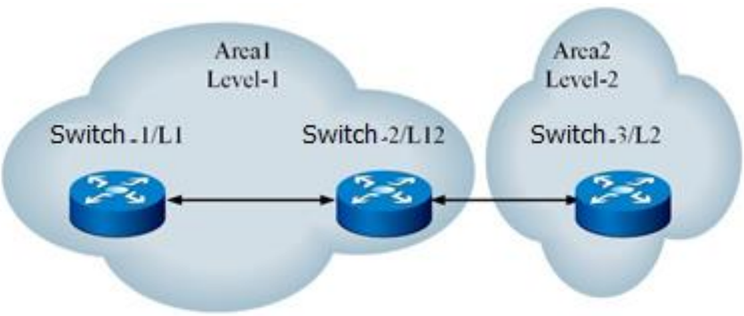


Figure 7-41 ISIS route aggregation topology

Configuration Suggestion

Switch_1 has 10 routes: 10.1.1.0/24 to 10.1.10.0/24. It is hoped to reduce the routing table size of Switch_3, so that when Switch_2 advertises Area1's routes to Area2, the routes are aggregated to 10.1.0.0/16. For this purpose, you can run the route aggregation command on Switch_2. After the configuration, Switch_3 only learns 10.1.0.0/16 from Area1.

Configuration

Refer to basic ISIS configuration and enable route aggregation on Switch_2:
Switch_2(config)# router isis
Switch_2(config-isis-1)#summary-address 10.1.0.0 16

Configuration Verification

Run the commands **show ip isis database** and **show ip isis route** to verify the running results.

7.6.3.4 Configuring ISIS Authentication

Network Requirements

This case shows how to configure ISIS authentication to make you familiar with the process of configuration authentication modes for Level-1 and Level-2 Hello and LSP packets. The topology is shown in Figure 7-42.

Network Diagram

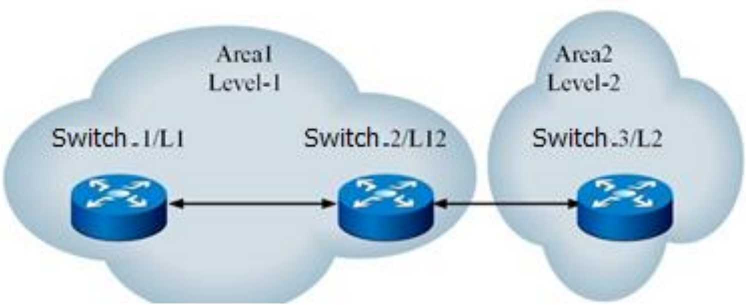


Figure 7-42 ISIS authentication topology

Configuration Suggestion

Meet the following rules for packets between Switch_1 and Switch_2:

Configure simple password authentication for Level-1 Hello packets. The password is **123456**.

Configure MD5 authentication for Level-2 Hello packets. The password is **fhn**.

Configure simple password authentication for Level-1 LSP packets. The password is **12345**.

Configure MD5 authentication for Level-2 LSP packets. The password is **cmcc**.

After configuration, Level-1 and Level-2 neighbors are established between Switch_1 and Switch_2 and Level-1 and Level-2 routes can be advertised.

Configuration

Refer to ISIS basic configuration and configure an authentication mode:

Switch_1:

```
Switch_1(config)#router isis
Switch_1(config-isis-1)#area-password simple 12345
Switch_1(config-isis-1)#domain-password md5 cmcc
Switch_1(config-isis-1)#quit
Switch_1(config)#interface vlan 1
Switch_1(config- vlan-1)#isis password simple 123456 level-1
Switch_1(config- vlan-1)#isis password md5 fhn level-2
```

Switch_2:

```
Switch_2(config)# router isis
Switch_2(config-isis-1)#area-password simple 12345
Switch_2(config-isis-1)#domain-password md5 cmcc
Switch_2(config-isis-1)#quit
Switch_2(config)#interface vlan 1
Switch_2(config- vlan-1)#isis password simple 123456 level-1
Switch_2(config- vlan-1)#isis password md5 fhn level-2
```

Configuration Verification

Run the commands **show ip isis neighbor**, **show ip isis database**, and **show ip isis route** to verify the running results.

7.6.3.5 Configuring ISIS BFD

Network Requirements

This case shows how to configure ISIS BFD to make you familiar with the ISIS BFD configuration process. The topology is shown in Figure 7-43.

Network Diagram

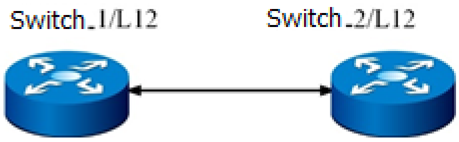


Figure 7-43 ISIS BFD topology

Configuration Suggestion

Both devices run ISIS, BFD is enabled globally, and BFD is enabled for ISIS interfaces. After configuration, neighbors are bound with BFD and quickly time out after disconnection.

Configuration

Refer to ISIS basic configuration and enable BFD:
Switch_1:
Switch_1(config)#interface vlan 2
Switch_1(config-vlan-2)#bfd enable
Switch_1(config-vlan-2)# isis bfd enable

Switch_2:
Switch_2(config)#interface vlan 2
Switch_2(config-vlan-2)#bfd enable
Switch_2(config-vlan-2)#isis bfd enable

Configuration Verification

Run the commands **show ip isis neighbor**, **show ip isis database**, **show ip isis route**, and **show ip isis bfd session** to verify the running results.

7.6.3.6 Configuring ISIS GR

Network Requirements

This case shows how to configure ISIS GR to make you familiar with the ISIS GR configuration process. The topology is shown in Figure 7-44.

Network Diagram

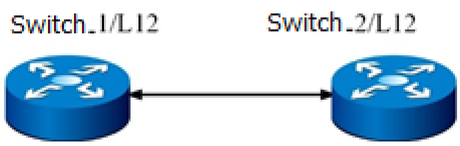


Figure 7-44 ISIS GR topology

Configuration Suggestion

Both devices run ISIS and are located in the same area. Both Switch_1 and Switch_2 are enabled with GR and send bidirectional traffic to each other. Start GR testing when the databases and traffic become stable.

Two devices are required by GR testing. One device is GR initiator and the other is GR helper. Testing on the GR initiator uses dual core switch cards and the plugging/unplugging method. There is no limit on the GR helper.

Configuration

Refer to ISIS basic configuration and enable GR:

Switch_1:

Switch_1(config)#router isis

Switch_1(config-isis-1)#graceful-restart enable

Switch_2:

Switch_2(config)#router isis

Switch_2(config-isis-1)#graceful-restart enable

Configuration Verification

Use the plugging/unplugging method for testing. After the GR initiator and GR helper are configured, unplug the active core switch card of the GR initiator and check that the original traffic between the devices is not interrupted within the period from this time to the time when new backup core switch card is restarted.

7.7 Configuring a Routing Policy

7.7.1 Overview of Routing Policy

Routing Policy

A routing policy is used to change the path of transmitting network traffic.

In order to implement a routing policy, you can define a group of match rules and configuration rules and then apply them to the routing policies for route advertisement, reception, and import.

Routing Policy Modes Supported by Switch

When configuring a routing policy, you can use address prefix lists.

The function of an address prefix list is similar to the ACL but it is more flexible and easier to understand. When an address prefix list is used to filter routing information, its matched object is the destination address information field in routing information. Besides, you can specify the router option to only receive routing information advertised by some routers.

7.7.2 Configuring an Address Prefix List

Purpose

This section describes how to configure an address prefix list to filter routing information. The matched object is the destination address field in routing information.

Procedure

Caution

- Tables are differentiated based on the list-name and IP address type.
- Directly return after any rule is matched.
- The matching is implemented based on the index in ascending order. If the index is not set, the maximum index in the table - index%10 + 10 is automatically adopted.
- The logical entry relation conflict is not detected. You need to independently arrange the detection.
- The original rule is overwritten when a rule is configured for an existing index.

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a filter rule to fully match network segment addresses with length of MASKLEN	1. Access the global configuration view. 2. Run the **ip prefix-list** *listname* [**index** *index-number*] { **permit | deny** } *ipv4-address mask-length* command.
Create a filter rule (with the route address mask length greater than or equal to the specified minimum value) to fully match network segment addresses of prefix mask length	1. Access the global configuration view. 2. Run the command **ip prefix-list** *listname* [**index** *index-number*] { **permit | deny** } *ipv4-address/mask-length* **greater-equal** *prefix-length*.
Create a filter rule (with the route address mask length smaller than or equal to the specified maximum value) to fully match network segment addresses of prefix mask length	1. Access the global configuration view. 2. Run the command **ip prefix-list** *listname* [**index** *index-number*] { **permit | deny** } *ipv4-address/mask-length* **less-equal** *prefix-length*.
Create a filter rule (with the route address mask length smaller than or equal to the specified maximum and minimum value range) to fully match network segment addresses of prefix mask length	1. Access the global configuration view. 2. Run the command **ip prefix-list** *listname* [**index** *index-number*] { **permit | deny** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*.

7.7.3 Configuring a Routing Policy

Prerequisite

Before configuring a routing policy, you need to configure ACL filter rules. For details, see 0 Configuring an L3 ACL.

Purpose

This section describes how to configure a routing policy to match given routing information or some attributes of routing information and change these attributes in some conditions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a routing policy and access the routing policy configuration view	1. Access the global configuration view. 2. Run the **route-policy** *policy-name* { **permit** | **deny** } **node** *node-number* command.
(Optional) Configure a MATCH clause	1. Access the global configuration view. 2. Access the routing policy configuration view. 3. Run the following commands: ● **match cost** *cost-value* ● **match ip filter-list** *ipv4-filter-list-number* ● **match ip { next-hop | route-source } filter-list** *ipv4-filter-list-number* ● **match ip-prefix** *prefix-name* ● **match ip { next-hop | route-source } ip-prefix** *prefix-name* ● **match route-type { internal | external-type1 | external-type2 | external-type1or2 | nssa-external-type1 | nssa-external-type2 | nssa-external-type1or2 }** ● **match tag** *tag-value*
(Optional) Configure an APPLY clause	1. Access the global configuration view. 2. Access the routing policy configuration view. 3. Run the following commands: ● **apply cost** *cost-value* ● **apply cost** { **plus** | **minus** } *cost-value* ● **apply cost-type { type-1 | type-2 }** ● **apply local-preference** *local-priority* ● **apply origin { igp | incomplete }** ● **apply isis { level-1 | level-2 | level-1-2 }** ● **apply origin egp** *as-number* ● **apply ospf { translate | not-translate }** ● **apply preferred-value** *preferred-value* ● **apply tag** *tag-value*

7.7.4 Applying a Routing Policy to OSPF

Purpose

This section describes how to apply a routing policy in OSPF to reference the ACL or address prefix list to filter received routes. Only the routes satisfying the conditions are accepted.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Apply a routing policy to the routes advertised by OSPF	1. Access the global configuration view. 2. Access the OSPFv2 configuration view. 3. Run the **filter route-policy** *route-policy-name* command to configure a filter policy of the routing protocol. Only the filtered route is added to the update packet for advertisement.
Apply a routing policy to OSPF when external routes are imported	1. Access the global configuration view. 2. Access the OSPF configuration view. 3. Run the **redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** } **route-policy** *policy-name* command to configure a policy for importing different routes.

7.7.5 Applying a Routing Policy to BGP

Purpose

This section describes how to apply a routing policy to BGP to reference the ACL or address prefix list to filter received routes. Only the routes satisfying the conditions are accepted.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Apply a routing policy to the routes received by BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **filter-policy import route-policy** *route-policy-name* command.

Purpose	Procedure
Apply a routing policy to routes received by the BGP neighbor	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **neighbor** *ipv4-address* **route-policy** *route-policy-name* **import** command.
Apply a routing policy to routes advertised by BGP	1. Access the global configuration view. 2. Access the BGP configuration view. (Perform Step 3 or 4 according to the actual condition.) 3. Run the **filter-policy export route-policy** *policy-name* command to configure a route filter policy. 4. Run the **filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* command to configure a route filter policy.
Apply a routing policy to routes advertised by the BGP neighbor	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **neighbor** *ipv4-address* **route-policy** *route-policy-name* **export** command to configure a route filter policy.
Apply a routing policy when external routes are imported by BGP	1. Access the global configuration view. 2. Access the BGP configuration view. 3. Run the **redistribute** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* command to configure a policy for importing different routes.

7.7.6 Applying a Routing Policy to ISIS

Purpose

This section describes how to apply a routing policy to ISIS to reference the ACL or address prefix list to filter received routes. Only the routes satisfying the conditions are accepted.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Apply a routing policy when external routes are imported by ISIS	1. Access the global configuration view. 2. Access the ISIS routing configuration view. 3. Run the **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy** *policy-name* command.

7.7.7 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the routing policy function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the global information of a routing policy	1. Access the privileged user view, global configuration view, or routing policy configuration view. 2. Run the **show route-policy information** command.
View the configured routing policy information	1. Access the privileged user view, global configuration view, or routing policy configuration view. 2. Run the following commands: ● **show route-policy config** ● **show route-policy** *policy-name* ● **show route-policy** *policy-name* **node** *node-number*

7.7.8 Configuration Example

7.7.8.1 Example of Configuring BGP4 ECMP and a Routing Policy

Network Requirements

BGP is configured on all switches. R1 is in AS65008. R2 and R3 are in AS65009. EBGP runs on R1, R2, and R3. IBGP runs on R2 and R3.

Network Diagram

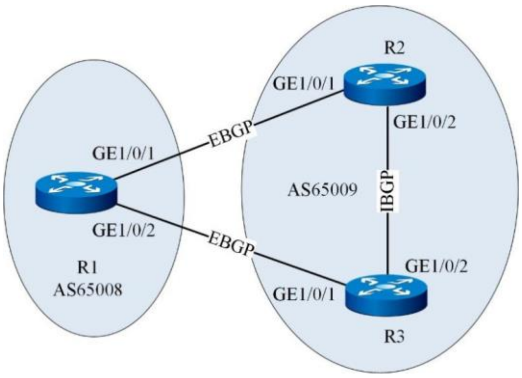


Figure 7-45 Network diagram of configuring BGP path selection

Switch	Interface	VLAN	IP Address
R1	10Gigaethernet1/0/1	VLAN 10	200.1.1.2/24
R1	10Gigaethernet1/0/2	VLAN 20	200.1.2.2/24
R2	10Gigaethernet1/0/1	VLAN 10	200.1.1.1/24
R2	10Gigaethernet1/0/2	VLAN 30	10.1.1.1/24
R3	10Gigaethernet1/0/1	VLAN 20	200.1.2.1/24
R3	10Gigaethernet1/0/2	VLAN 30	10.1.1.2/24

Configuration Suggestion

Configure BGP load sharing and apply a routing policy to modify MED attributes as follows:

1. Configure an EBGP connection between R1 and R2 and between R1 and R3; configure an IBGP connection between R2 and R3.
2. Apply the routing policy to R1 to change the MED value; check the routing information.

Data Preparation

Prepare the following data to complete the configuration in this example:

VLAN IDs corresponding to the interfaces. See Figure 7-45.

IP addresses of the VLANIF interfaces. See Figure 7-45.

The router ID of R1 is 1.1.1.1, its AS number is 65008, and the load sharing quantity is 2.

The router IDs of R2 and R3 are 2.2.2.2 and 3.3.3.3 respectively, the AS number is 65009, and the default MED value of R2 is 100.

Configuration

1. Configure the BGP connection.

Configure R1.

```
R1(config)#router bgp 65008
R1(config-bgp)#router-id 1.1.1.1
R1(config-bgp)#neighbor 200.1.1.1 remote-as 65009
R1(config-bgp)#neighbor 200.1.2.1 remote-as 65009
R1(config-bgp)#quit
```

Configure R2.

```
R2(config)#router bgp 65009
R2(config-bgp)#router-id 2.2.2.2
R2(config-bgp)#neighbor 200.1.1.2 remote-as 65008
R2(config-bgp)#neighbor 10.1.1.2 remote-as 65009
R2(config-bgp)#network 10.1.1.0 255.255.255.0
R2(config-bgp)#quit
```

Configure R3.
R3(config)#router bgp 65009
R3(config-bgp)#router-id 3.3.3.3
R3(config-bgp)#neighbor 200.1.2.2 remote-as 65008
R3(config-bgp)#neighbor 10.1.1.1 remote-as 65009
R3(config-bgp)#network 10.1.1.0 255.255.255.0
R3(config-bgp)#quit
View the R1 routing table. As shown in the routing table, there are two next hops for the BGP route 10.1.1.0/24, namely 200.1.1.1 and 200.1.2.1, both of which are the optimal routes.
R1(config)#show ip bgp route
2. Configure the MED attribute.
Configure the MED value sent by R2 to R1 according to the policy.
R2(config)#route-policy 10 permit node 10
R2(config-route-policy)#apply cost 100
R2(config-route-policy)#quit
R2(config)#router bgp 65009
R2(config-bgp)#neighbor 200.1.1.2 route-policy 10 export
View the R1 routing table. As shown in the routing table, the next hop is 200.1.1.1, the route MED value of R2 is 100, while the MED value of next hop 200.1.2.1 is 0; therefore, BGP preferentially selects the route with the smaller MED value.
R1(config)#show ip bgp route

7.7.8.2 Configuring an OSPF Routing Policy

Network Requirements

OSPF is configured for all switches and all the interfaces are set to Area 0. Switch_1 and Switch_2 are ABRs for transmitting routes among areas. The route calculated by OSPF based on LSDB must reference the routing policy before being sent to the local routing table.

Network Diagram

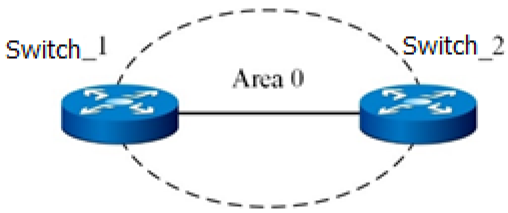


Figure 7-46 Network diagram of configuring an OSPF routing policy

Interface addresses of Switch_1: 1.1.1.1/24 and 3.1.1.1/24

Interface addresses of Switch_2: 1.1.1.2/24 and 4.1.1.2/24

Configuration

1. Configure Switch_1.

```
Switch_1(config)#router ospf
Switch_1(config-ospf-1)#router-id 1.1.1.1
Switch_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Switch_1(config)#
```

2. Configure Switch_2.

```
Switch_2(config)#router ospf
Switch_2(config-ospf-1)#router-id 1.1.1.2
Switch_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Switch_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Switch_2(config)#
```

3. Configure a routing policy.

```
Switch_1(config)#filter-list 1001
Switch_1(configure-filter-ipv4-1001)#filter 1 ip 18.1.1.0/24 any
Switch_1(configure-filter-ipv4-1001)#filter 1 action permit
Switch_1(configure-filter-ipv4-1001)#quit
Switch_1(config)#route-policy fhn deny node 1
Switch_1(configure-route-policy)#match ip filter-list 1001
Switch_1(configure-route-policy)#quit
Switch_1(config)#route-policy fhn permit node 2
Switch_1(configure-route-policy)#quit
```

4. Apply the routing policy to OSPF.

```
Switch_1(config)#router ospf
Switch_1(config-ospf-1)#filter route-policy fhn
```

7.8 Configuring Policy Routes

7.8.1 Policy Route Overview

Policy Route Protocol Overview

Traditionally, ordinary packets are forwarded by querying the forwarding table based on the destination address of packets. When it is necessary to forward packets by source IP address, packet length, or other packet attributes, a new routing mechanism is required, that is, the policy route.

A policy route forwards packets according to a certain policy. Therefore, policy route is a more flexible routing mechanism than destination routing. When a router forwards a data packet, it first filters the packet according to the configured rules, and forwards the packet according to a certain forwarding policy if a rule is matched. These rules can be based on standard and extended ACLs, or based on the packet length. The forwarding policy is to control the packet to be forwarded according to the specified policy routing table, and it can also modify the IP priority field of the packet. Therefore, policy route is an effective enhancement to the traditional IP routing mechanism.

About Policy Route Protocol

Policy route can select routes based on source IP addresses, destination IP addresses, protocol fields, source and destination TCP and UDP ports, or even a combination of these options. As long as an IP standard/extended ACL can be set, it can be forwarded as a matching rule of policy route.

Policy route determines the next-hop forwarding address or the next-hop default IP address of an IP packet not simply based on the destination IP address, but based on multiple factors. For example, it selects a route for data packets according to the DSCP (Differentiated Services Code Point) field, source and destination port numbers, or source IP address. Policy route can implement traffic engineering to a certain extent, so that streams with different quality of service or data of different natures (voice or FTP) take different routes.

Policy route provides network managers with stronger control over packet forwarding and storage than traditional routing protocols. Traditionally, routers use routing tables derived from routing protocols to forward packets based on destination addresses. Compared with traditional routing, policy-based routing is more powerful and flexible. It enables network managers to select forwarding paths not only based on destination addresses but also based on protocol types, packet sizes, applications or IP source addresses. Policies can be defined as load balancing through multiple routers or quality of service (QoS) for packet forwarding across wires based on total traffic.

Policy route is implemented based on chips. It converts software entries into hardware entries and stores them on chips through command lines or other configuration interfaces. When traffic passes a chip, the chip will filter the packets according to the policy routing hardware table.

7.8.2 Configuring the Policy Route Function

Purpose

This section describes how to configure the policy route function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create or modify a policy route and a policy node, and access the policy route configuration view	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route** ***name*** **{ permit | deny } node** *node-id* command,
Delete a policy route	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **no policy-based-route** *name* ● **no policy-based-route** *name* **node** *node-id*
Configure the priority of an IP packet to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node node-id** command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **apply ip-precedence** *value* command.
Cancel the priority configured for an IP packet to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **no apply ip-precedence** command.
Configure the next hop IP address of a packet to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the following commands: ● a**pply ip-address next-hop** *ip-address1* ● **apply ip-address next-hop** *ip-address1 ip-address2*

Purpose	Procedure
Configure the next hop IP address configured for a packet to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **no apply ip-address next-hop** command.
Configure the next hop IP address for redirection	1. Run the **configure** command to access the global configuration view. 2. Run the policy-based-route name { permit | deny } node node-id command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the apply load-balance ip-address next-hop *next-hop-address* command.
Configure the outbound interface to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run **the apply outgoing-interface { gigaethernet | xgigaethernet }** *interface-number* command.
Cancel the configured the outbound interface to which a policy route is applied	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **no apply outgoing-interface** command.
Configure an ACL match rule based on an ACL policy route	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **if-match acl** *acl-number* command.
Cancel an ACL match rule based on an ACL policy route	1. Run the **configure** command to access the global configuration view. 2. Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 3. Run the **no if-match acl** command.

Purpose	Procedure
Delete a policy route applied to an interface	1. Run the **configure** command to access the global configuration view. 2. Run the corresponding command to access the interface configuration view (Trunk or Ethernet). 3. Run the **no ip policy-based-route** *policyname* command.

7.8.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the policy route function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display the policy route information	1. Access any of the following views: ● Remain in the current privileged user view. ● Run the **configure** command to access the global configuration view. ● Run the **disable** command to return to the common user view. ● Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 2. Run the following commands: ● **show ip policy-based-route** ● **show ip policy-based-route** *policy-name*
Display the policy route configuration	1. Access any of the following views: ● Remain in the current privileged user view. ● Run the **configure** command to access the global configuration view. ● Run the **disable** command to return to the common user view. ● Run the **policy-based-route name { permit | deny } node** *node-id* command to create or modify a policy-based route and a node, and access the policy route configuration view. 2. Run the **show ip policy-based-route config** command.

7.8.4 Configuration Example

7.8.4.1 Configuring an ACL-based Policy Route

Network Requirements

As shown in Figure 7-47, define a policy route **aaa**. All IP packets received by 10GE1/1/2 are sent through 10GE1/1/3 to the next hop 1.1.2.2. Other packets are still forwarded according to the routing table.

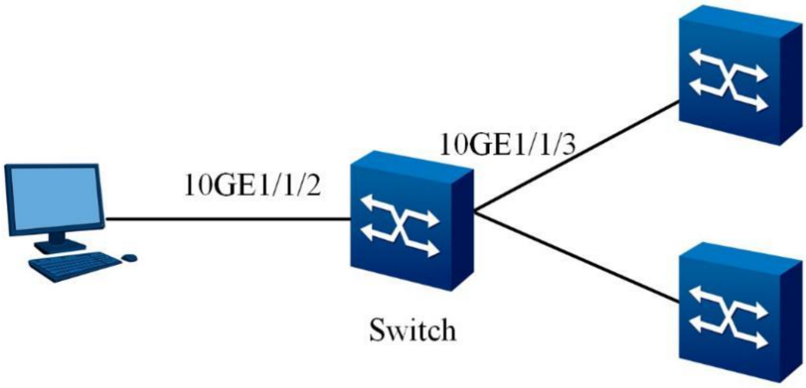


Figure 7-47 ACL-based policy route

Configuration Suggestion

Configure an ACL-based policy route as follows:

- Define an ACL.
- Define rule and action for the policy route.
- Enable the policy route for an interface

Data Preparation

To perform the configuration, prepare the following data:

- ACL No. and rule
- Policy route name
- Next hop IP address for the policy route action

Configuration

1. Configure an ACL and match IP packets based on ACL filter 1.

```
Switch(config)#filter-list 1001
Switch(configure-filter-ipv4-1001)#filter 1 ip any any
Switch(configure-filter-ipv4-1001)#filter 1 action permit
```

2. Define the policy rule and action.

```
Switch (config) policy-based-route aaa permit node 5
Switch (config -policy-based-route-aaa-5) if-match acl 1001
Switch (config -policy-based-route-aaa-5) apply ip-address next-hop 1.1.2.2
Switch (config -policy-based-route-aaa-5) quit
```

3. Enable the policy route for an interface.

```
Switch (config) interface 10gigaethernet 1/1/2
Switch (config-10ge1/1/2) ip policy-based-route aaa
```

7.9 Configuring Hwroute

7.9.1 Hwroute Overview

The Hwroute module is applied for command diagnosis and debugging only.

7.9.2 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when routing entries fail to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable hardware debugging for a route	1. Remain in the current privileged user view. 2. Run the following commands: ● **debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }**

Purpose	Procedure
	• **no debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }**
View an IPv4 routing entry	1. Run the **disable** command to return to the common user view. 2. Run the following commands: • **show hwroute hardware route4** • **show hwroute hardware arp** • **show hwroute hardware ilm**
View an IPv6 routing entry	1. Run the **disable** command to return to the common user view. 2. Run the following commands: • **show hwroute hardware route6** • **show hwroute hardware nd**
View an IPv4 routing entry with unreachable next hop	1. Run the **disable** command to return to the common user view. 2. Run the **show hwroute hardware route4 pend** command.
View an IPv6 routing entry with unreachable next hop	1. Run the **disable** command to return to the common user view. 2. Run the **show hwroute hardware route6 pend** command.
View the information of an IPv4 or IPv6 ECMP group	1. Run the **disable** command to return to the common user view. 2. Run the following commands: • **show hwroute ecmp-group** • **show hwroute ecmp-group6**
View the IPv4 or IPv6 next hop ID	1. Run the **disable** command to return to the common user view. 2. Run the following commands: • **show hwroute nexthop** *route-id* • **show hwroute nexthop6** *route-id*
View statistics on route messages received by an HwRoute module	1. Run the **disable** command to return to the common user view. 2. Run the **show hwroute statistic rtm** command.
View statistics on route messages of an HwRoute module	1. Run the **disable** command to return to the common user view. 2. Run the **show hwroute statistic route { v4 | v6 | all }** command.

Chapter 8 Configuring QoS

This chapter describes the basic content, configuration procedure, and configuration examples of the QoS function of the Switch.

8.1 Configuring DiffServ

8.1.1 DiffServ Overview

In traditional IP networks, each router makes its best effort to send all packets in the principle of first-in-first-out (FIFO) to the destination address, but does not ensure the packet transmission reliability, transmission delay, and other performance.

With emerging new applications on IP networks, new requirements are imposed on the service quality of IP networks. For example, real-time services such as Voice over IP (VoIP) require shorter transmission delay of packets (Email and FTP services are not sensitive to the delay). To support services such as voice, video, and data with different service requirements, the network must be able to distinguish different communications and provide corresponding services for them. The best-effort service of traditional IP networks cannot identify and distinguish communication categories in the networks, and the ability to distinguish communication categories is the premise of providing different services for different communications. Therefore, the best-effort service mode of traditional networks can no longer satisfy the application needs. The Quality of Service (QoS) technology is designed to solve this problem.

To achieve scale adaptability in QoS mode, the IP backbone network generally must have a Differentiated Service (DiffServ) architecture, while IP edge networks can use either the DiffServ architecture or the IntServ architecture. There is no consensus on which QoS architecture that an IP edge network should use yet. These two architectures may coexist in an IP edge network. If an IP edge network uses the DiffServ architecture, it can communicate with an IP backbone network. If an IP edge network uses the IntServ architecture, the communication between DiffServ and IntServ must be solved, including mapping between IntServ-supported services and DiffServ Per-Hop Behaviors (PHBs).

Switch allows users to perform simple traffic classification on packets based on the mapping between packet priority defined in the DiffServ domain and PHB. For packets from upstream devices, the DiffServ domain is bound to the inbound interface of the packets, and map the priority information carried in the packets to the corresponding PHB and color in the DiffServ domain. Inside the device, congestion management is performed according to PHB of the packets, and congestion avoidance is performed according to the color of the packets. For packets destined to downstream devices, the outbound interface of the packets is bound to the DiffServ domain. In the DiffServ domain, the PHB and color of packets are mapped to corresponding priorities, and downstream devices provide corresponding QoS according to the priorities of the packets.

Simple traffic classification is based on the following factors:

- 802.1p priority in VLAN packets
- DSCP priority in IP packets
- EXP priority in MPLS packets

8.1.2 Configuring DiffServ

8.1.2.1 Creating a Configuration Task

Purpose

This section describes how to create a configuration task to configure DiffServ. Users can classify packets from upstream devices by the 802.1p or DSCP priority carried in the packets. In the DiffServ domain, map the priority to PHB and color and take the mapping as a basis for classification. Bind the DiffServ domain to the outbound interface of packets. Then, QoS can perform congestion management and avoidance on this outbound interface based on the packet PHB and color.

Users can classify packets destined to downstream devices by PHB or color. In the DiffServ domain, map PHB and color and priority and take the mapping as a basis for classification. Bind the DiffServ domain to the outbound interface of packets. Then, the downstream devices can provide QoS based on the packet priority.

8.1.2.2 Creating a DiffServ Domain and Configuring Priority Mapping

Purpose

This section describes how to create a DiffServ domain and configure priority mapping. A DiffServ domain consists of a group of connected DiffServ nodes, which adopt the same service providing strategy and implement the same set of PHB groups.

When Switch serves as a boundary node between a DiffServ domain and other networks, users must configure the mutual mapping between internal priority (expressed by DiffServ service level and color) and external priority (such as 802.1p and DSCP).

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a DiffServ domain	1. Access the global configuration view. 2. Run the **diffserv domain** *name* command to create a DiffServ domain and access the DiffServ domain view.
Delete a DiffServ domain	1. Access the global configuration view. 2. Run the **no diffserv domain** *name* command.
At the outbound interface, map the 802.1p priority of a VLAN packet to PHB and mark the packet color	1. Access the global configuration view. 2. Run the **diffserv domain** *name* command to create a DiffServ domain and access the DiffServ domain view. 3. Run the command **8021p-inbound** *8021p-priority-range* **default phb** { **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** | **cs7** } { **green** | **yellow** | **red** }.
At the outbound interface, map the PHB and color to the 802.1p priority of a VLAN packet	1. Access the global configuration view. 2. Run the **diffserv domain** *name* command to create a DiffServ domain and access the DiffServ domain view. 3. Run the following commands: ● **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map** *8021p-priority-range* ● **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**
At the inbound interface, map the SDCP priority of	1. Access the global configuration view. 2. Run the **diffserv domain** *name* command to create a DiffServ domain and access the DiffServ domain view.

Purpose	Procedure
an IP packet to PHB and mark the packet color	3. Run the command **ip-dscp-inbound** *dscp-priority* **default phb { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red }.**
At the outbound interface, map the PHB and color to the DSCP priority of an IP packet	1. Access the global configuration view. 2. Run the **diffserv domain** *name* command to create a DiffServ domain and access the DiffServ domain view. 3. Run the following commands: ● **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map** *dscp priority* ● **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**

8.1.2.3 Configuring Priority of Packets Trusted by a Port

Purpose

This section describes how to configure priority of packets trusted by a port.
Switch provides two priority trusting modes:

1. 802.1p priority of trusted packets.

For packets with a VLAN tag, the switch queries the mapping between their 802.1p priority and the internal priority and then marks the internal priority in packets. For packets without a VLAN tag, Switch queries the mapping between the default 802.1p priority of the port and the internal priority and then marks the internal priority in packets.

2. DSCP priority in trusted packets.

The switch queries the mapping between the DSCP priority of packets and the internal priority and then marks the internal priority in packets.
Note that the internal priority is represented by the service level and color of the DiffServ model.
If the same trusted packet priority needs to be configured for multiple interfaces, configure it in the form of port group to reduce the workload.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure priority of packets trusted by a port	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **trust { 8021p | diffserv | dscp | none } { inner | outer }** command.

8.1.2.4 Applying a DiffServ Domain

Purpose

This section describes how to apply a DiffServ domain.

You can bind a DiffServ domain to the inbound interface of packets so that the system can map the priorities of packets from the upstream device to certain PHBs and colors based on mappings configured in the DiffServ domain.

You can bind a DiffServ domain to the outbound interface of packets so that the system can map the PHBs and colors of packets sent to the downstream device to certain priorities based on mappings configured in the DiffServ domain.

If the **trust diffServ domain recover** command is run at the interface, the system restores the default priority mapping for packets sent to or from this interface. By default, no DiffServ domain is bound to the interface. The system uses the default priority mapping to map priorities of packets sent to or from the interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Bind a DiffServ domain to an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **trust diffserv domain** { *name* | **default** } command.
Cancel the type of the priority to be mapped in packets	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **trust none** command.

8.1.2.5 Checking the Configuration Result

Purpose

This section describes how to check the configuration result.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Check the configuration result	1. Access the common user view, privileged user view, global configuration view, DiffServ configuration view, interface configuration view (Ethernet or Trunk), batch interface configuration view, or interface group configuration view. 2. Run the following commands: ● **show diffserv domain** ● **show diffserv domain config** ● **show diffserv domain interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show diffserv domain** *name*

8.1.3 Configuration Example

Network Requirements

Switch is interconnected with the router through interface 10GE1/0/1, and the enterprise user and residential user can access the network through Switch and the router. The VLAN ID of the enterprise user and residential user are 100 and 200 respectively. The enterprise user needs better QoS guarantee, so the priority of data packets from the enterprise user is mapped to 4, and the priority of data packets from the residential user is mapped to 2 to provide DiffServ.

Network Diagram

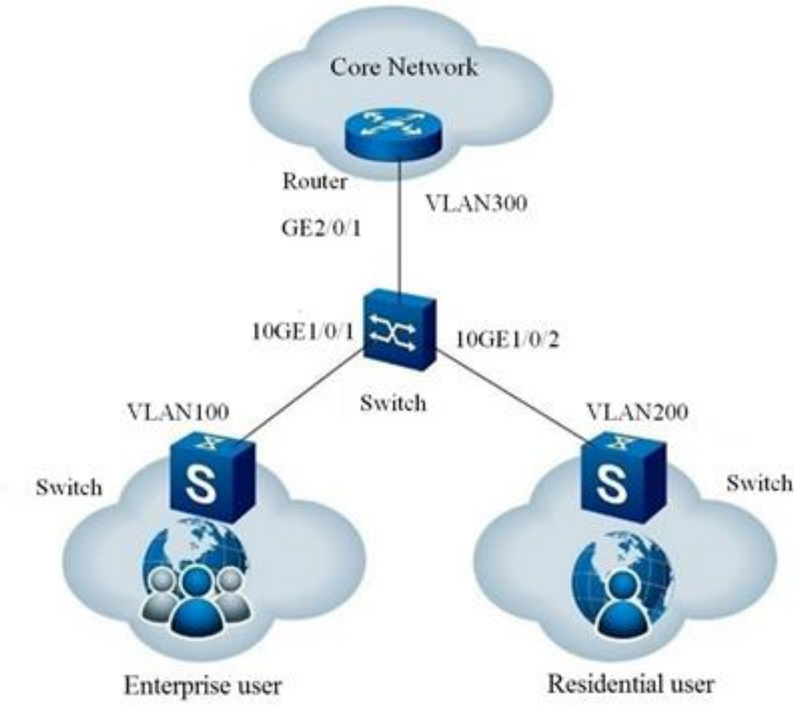


Figure 8-1 DiffServ configuration network diagram

Configuration Suggestion

Configure priority mapping based on simple flow classification as follows

1. Create VLANs and interfaces so that the enterprise user and residential user can access the network through Switch.
2. Create a DiffServ domain and map the 802.1p priority to the PHB and color.
3. Configure the trusted packet priority at inbound interfaces 10GE1/0/1 and 10GE1/0/2 of Switch.
4. Bind the DiffServ domain to inbound interfaces 10GE1/0/1 and 10GE1/0/2 of Switch.

Data Preparation

Prepare the following data to complete the configuration in this example:

- DiffServ domain name.
- The 802.1p priority of packets of the enterprise user and residential.
- The service level of the enterprise user and residential user.

Configuration

1. Create VLANs and interfaces.

2. Create DiffServ domains. On Switch, configure DiffServ domains ds1 and ds2, and map the 802.1p priority of the enterprise user and residential user to the service level.

Switch(config)#diffserv domain ds1

Switch(config-dsdomain-ds1)#8021p-inbound 0 phb af4 green

Switch(config-dsdomain-ds1)#quit

Switch(config)#diffserv domain ds2

Switch(config-dsdomain-ds2)#8021p-inbound 0 phb af2 green

Switch(config-dsdomain-ds2)#quit

3. Bind DiffServ domains to interfaces.

Bind ds1 and ds2 to 10GE1/0/1 and 10GE1/0/2 respectively.

Switch(config)#interface 10gigaethernet 1/0/1

Switch(config-10ge1/0/1)#trust diffServ domain ds1

Switch(config-10ge1/0/1)#quit

Switch(config)#interface 10gigaethernet 1/0/2

Switch(config-10ge1/0/2)#trust diffServ domain ds2

Switch(config-10ge1/0/2)#quit

4. Configure priority of packets trusted by interfaces.

Switch(config)#interface 10gigaethernet 1/0/1

Switch(config-10ge1/0/1)#trust 8021p outer

Switch(config-10ge1/0/1)#quit

Switch(config)#interface 10gigaethernet 1/0/2

Switch(config-10ge1/0/2)#trust 8021p outer

Switch(config-10ge1/0/2)#quit

Description

By default, the mappings between 802.1p priorities, PHBs, and colors of ingress VLAN packets in a DiffServ domain are as follows.

802.1p Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green

802.1p Priority	PHB	Color
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

By default, the mappings between PHBs, colors, and 802.1p priorities of egress VLAN packets in a DiffServ domain are as follows.

PHB	Color	802.1p Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

By default, the mappings between DSCP priorities, PHBs, and colors of ingress IP packets in a DiffServ domain are as follows.

DSCP	PHB	Color	DSCP	PHB	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

By default, the mappings between PHBs, colors, and DSCP priorities of egress IP packets in a DiffServ domain are as follows.

PHB	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

8.2 Configuring Traffic Policing and Traffic Shaping

Purpose

Traffic-based traffic policing enables a switch to limit the rate of traffic in compliance with the traffic classification rules. By policing the traffic rate, the switch discards traffic beyond the rate limiting, so that traffic entering the switch is limited within a reasonable range, thereby protecting network resources and carrier's interests. The traffic-based traffic policing adopts the dual leaky bucket algorithm.

Designate the rate limiting rules (CIR, CBS, PIR, and PBS) via meter, designate the flow type using ACL, and then associate with meter. ACL can be used on either physical interfaces (including Trunk interfaces) or VLAN interfaces.

The Switch supports two kinds of traffic shaping: port shaping and port queue shaping, which can be selected as required. When both traffic shaping modes co-exist, ensure that the CIR of port shaping is equal to or larger than the sum of CIR of port queue shaping. Otherwise, traffic shaping is abnormal (for example, traffic in a queue with a lower priority preempts for bandwidth for traffic in a queue with a higher priority).

This command is used to configure the QoS CAR profile (CIR, CBS, PIR, and PBS), and is applied in the ingress and egress directions of the port. After the QoS CAR applies to the physical interface or Eth-Trunk interface, the system limits the rate of all upstream packets transmitted over the physical interface or Eth-Trunk interface.

The priority of QoS CAR applied to the interface is higher than the QoS CAR of the VLAN. If the QoS CAR is enabled for both interface and VLAN, the QoS CAR of the interface shall prevail.

The cir-value specifies the committed information rate (CIR) that ensures a mean rate of packets passing through an interface. The value is an integer ranging from 64 to 4294967295, in kbit/s.

The cbs-value specifies the size of the committed burst traffic that can pass through an interface. The value is an integer ranging from 10000 to 4294967295, in bytes.

The pir-value specifies the designated peak information rate. The value is an integer ranging from 64 to 4294967295, in kbit/s. The pir-value must be not less than cir-value. The pir-value must be equal to or larger than cir-value. By default, pir-value is equal to cir-value. If the pir-value is equal to cir-value, the pbs-value is 0 byte by default. Otherwise, pbs-value is 125 times the pir-value by default.

The pbs-value specifies the size of the peak burst. The value is an integer ranging from 10000 to 4294967295, in bytes. The pbs-value must be equal to or larger than cbs-value.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Bind a meter	1. Access the global configuration view. 2. Access the filter configuration view. 3. Run the **filter** *rule-number* **meter** *meter-number* command.
Unbind a filter from a meter	1. Access the global configuration view. 2. Access the filter configuration view. 3. Run the **no filter** *rule-number* **meter** command.
Configure the external processing action of a filter entry bound to a meter	1. Access the global configuration view. 2. Access the filter configuration view. 3. Run the following commands: ● **filter** *rule-number* **outaction { red | yellow } { drop | remark-cfi | remark-dot1p | remark-dscp }** ● **filter** *rule-number* **outaction** { **red** | **yellow** } **remark-dscp** *dscp*
Cancel the external processing action configured for a filter entry bound to a meter	1. Access the global configuration view. 2. Access the filter configuration view. 3. Run the **no filter** *rule-number* **outaction** command.
Designate the rate limiting rules (including CIR, CBS, PIR, EBS, and PBS) using a meter	1. Access the global configuration view. 2. Run the following commands: ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* { **aware | blind** } ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* { **aware| blind** } ● **no meter** *meter-number*

8.3 Configuring Queue Scheduling and Congestion Control

8.3.1 Introduction to Queue Scheduling and Congestion Control

Impact of Congestion

Congestion is a type of additional delay caused by decreased forwarding rate due to insufficient resources.

The bottleneck of link bandwidth causes congestion, which results from the shortage of resources that are used for data forwarding and processing (such as allocable processor time, buffer, and memory resource). Under the current complex network environment with a variety of service applications, congestion is very common.

Congestion may bring about a series of adverse impact.

- Congestion increases delay and jitter of packet transmission. Excessive delay causes retransmission of packets.
- Congestion decreases the effective throughput of network and the utilization rate of network resources.
- Serious congestion consumes a large number of network resources (especially storage resources). Improper resource allocation may even lead to system crash because of resource deadlock.

Queue Technology

The main content of congestion management is to develop a resource scheduling policy when congestion occurs to determine the processing order of packet forwarding. For congestion management, queue technology is usually used. A queue algorithm is used to classify traffic and then a priority algorithm is used to send the traffic. Each queue algorithm is used to address a specific network traffic problem and has significant impact on bandwidth resource allocation, delay, and jitter.

8.3.2 Configuring Queue Scheduling and Congestion Control

Purpose

This section describes how to configure queue scheduling and congestion control.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the scheduling mode for queues on an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the following commands: ● **cos scheduling { sp | rr | wrr | drr }** ● **cos scheduling { sp+rr | sp+wrr | sp+drr }** *queue-list*
(Optional) Configure the weight of a port queue	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the following commands: ● **cos queue** *queue-number* **weight** *weight* ● **cos queue** *queue-lis* **weight** *weight*
(Optional) Configure the priority of a specified port queue	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **cos queue** *queue-index* **priority** *priority-value* command.
(Optional) Configure the valid bandwidth of a queue	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the command **cos queue** { *queue-index* | *queue-list* } { **min-bandwidth** | **max-bandwidth** } { **kbps** | **mbps** | **gbps** } *bandwidth-value*.
Create a WRED drop profile and access its view or access the view of an existing WRED drop profile	1. Access the global configuration view. 2. Run the **drop-profile** { *drop-profile-name* | **default** } command.

Purpose	Procedure
Delete a designated WRED drop profile	1. Access the global configuration view. 2. Run the **no drop-profile** *drop-profile-name* command.
Enable the COS ECN function	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the following commands: ● **qos ecn** *name* ● **qos queue** *queue-index* **ecn** *name*
Apply a WRED drop profile to an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **qos wred** *name* command.
Apply a WRED drop profile to an interface queue	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **qos queue** *queen-index* **wred** *name* command.
Configure ECN parameters	1. Access the global configuration view. 2. Run the **drop-profile** { *drop-profile-name* | **default** } command to access the view of an existing WRED drop profile. 3. Run the command **ecn low-limit** { *low-limit* | **default** } **high-limit** { *high-limit* | **default** } **discard-percent** { *discard-percent* | **default** }.
Enable or disable ECN	1. Access the global configuration view. 2. Run the **drop-profile** { *drop-profile-name* | **default** } command to access the view of an existing WRED drop profile. 3. Run the **qos ecn** { **enable** | **disable** } command.

8.3.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the queue scheduling and congestion control functions fail to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the CoS configuration on an interface	1. Access the common user view. 2. Run the following commands: ● **show cos interface** ● **show cos interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
View the CoS configuration	1. Access the common user view. 2. Run the **show cos config** command.
View summary information about all WRED drop profiles on the switch	1. Access the common user view. 2. Run the following commands: ● **show drop-profile** ● **show drop-profile** *drop-profile-name* ● **show drop-profile all**
View all WRED configurations on an interface or a VLAN	1. Access the common user view. 2. Run the **show wred config** command.
Enable or disable WRED debugging	1. Access the privileged user view. 2. Run the **debug wred** or **no debug wred** command.
Reset the CoS statistics	1. Access the global configuration view. 2. Run the command **reset cos statistics all or reset cos statistics interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
View the CoS statistics	1. Access the common user view. 2. Run the following commands: ● **show cos statistics all** ● **show cos statistics interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*

8.3.4 Configuration Example

8.3.4.1 Example of Configuring SP Scheduling

Network Requirements

After traffic is transmitted from interfaces 10GE1/0/1, 10GE1/0/2, and 10GE1/0/3 from Site 1 to Site 2, congestion occurs on interface 10GE1/0/1. It is required to apply the SP scheduling algorithm.

Network Diagram

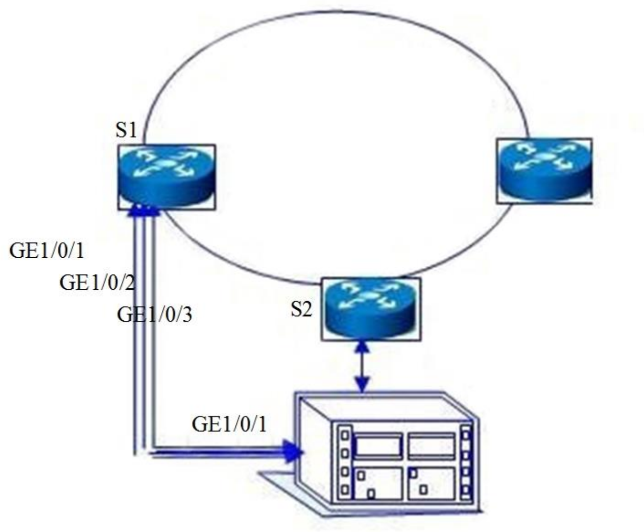


Figure8-2 Network diagram of port queue priority scheduling

Configuration

1. Configure Site 1.

Configure interface 10GE1/0/1.

S1#configure

S1(config)#interface 10gigaethernet 1/0/1

S1(config-10ge1/0/1)#priority 1

S1(config-10ge1/0/1)#quit

Exit the configuration of interface 10GE1/0/1.

Configure interface 10GE1/0/2.

S1#configure

S1(config)#interface 10gigaethernet 1/0/2

S1(config-10ge1/0/2)#priority 2

S1(config-10ge1/0/2)#quit

Exit the configuration of interface GE1/0/2.

Configure interface 10GE1/0/3.
S1#configure
S1(config)#interface 10gigaethernet 1/0/3
S1(config-10ge1/0/3)#priority 3
S1(config-10ge1/0/3#quit
Exit the configuration of interface 10GE1/0/3.
2. Configure Site 2.
Configure an ACL rule.
S2#configure
S2(config)#filter-list 1001
S2(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32
S2(config-filter1)#filter 1 action cos 7
Configure interface 10GE1/0/1.
S2#configure
S2(config)#interface 10ge 1/0/1
S2(config-10ge1/0/1)#cos schedule sp
S2(config-10ge1/0/1)#filter-list in 1001

Chapter 9 Configuring Multicast Service

This chapter describes how to configure the multicast service of the Switch.

9.1 Configuring IGMP Snooping

9.1.1 Overview of IGMP Snooping

Basic Principle of IGMP Snooping

IGMP snooping is the abbreviation of Internet Group Management Protocol snooping. It is the multicast restriction mechanism running on L2 devices. IGMP establishes a mapping relationship for ports and multicast MAC addresses by snooping the IGMP packets transferred between user host and router in the network and analyzing the received IGMP packets. It forwards the multicast data according to this mapping relationship to manage and control multicast groups.

When IGMP snooping does not run on L2 devices, multicast data is broadcast at L2. When IGMP snooping runs on L2 devices, multicast data of known multicast groups is not broadcast at L2 but is multicast to the designated receiver at L2.

Advantages of IGMP Snooping

IGMP snooping has the following advantages:

- Enhances the security of multicast information.
- Reduces the broadcast packets of L2 networks and saves bandwidth.
- Provides convenience for separate accounting for each user host.

IGMP Snooping Features Supported by the Switch

- Support for static L2 multicast

  When a multicast packet is transmitted over the Ethernet, the destination of the packet is not a specified receiver but a group with uncertain members. Therefore, when the multicast packet is forwarded to the link layer from the network layer, no multicast forwarding table entry is generated, causing the multicast packet to be transmitted in broadcast mode at the link layer. When the Switch is deployed between router and user host and applies Layer-2 forwarding features, you can configure static Layer-2 multicast (manually configure forwarding table entries) to transmit multicast data to the user that has the long-term requirement for receiving the data.

Static L2 multicast has the following features:

Configure interfaces to join a multicast group statically to avoid protocol packet attack.

Use the mechanism of directly searching the multicast packet forwarding table to reduce network delay.

Prevent unregistered users from receiving multicast packets and provide paid services.

- Support for multicast VLAN copy

  In traditional multicast forwarding mode, when users that belong to different VLANs join/leave the same multicast source, the switch needs to copy a set of multicast data for each VLAN and then transmit the data to every VLAN. After configuring multicast VLAN copy, when users belonging to different VLANs join/leave the same multicast source, the switch configures one multicast VLAN for all these VLANs. In this way, the upper-layer router only needs to transmit one set of data to this multicast VLAN but does not need to copy a set of multicast data for each VLAN.

  The multicast VLAN copy function facilitates managing and controlling the multicast source and multicast group members and also reduces the waste of bandwidth and extra network burden.

- Support for VLAN-based IGMP snooping
  - The IGMP version can be configured as v1, v2, or v3.
  - The multicast forwarding mode can be configured.
  - Static router interfaces are supported.
  - IGMP query is supported.
  - IGMP packet suppression is supported.
  - The interface fast leave function is supported.
  - The aging time of router interfaces can be configured.
  - The maximum response time of group members can be configured.
  - Multicast policies can be configured.
  - The Router Alert option can be configured.
  - The source IP address for sending IGMP packets can be configured.
  - IGMP proxy is supported.

9.1.2 Configuring Static L2 Multicast

Background

In Metro Ethernet, when a user host has the long-term requirement for receiving multicast data flows from a multicast group, an interface can be configured to join the multicast group in a static way.

Purpose

After configuring this function, users can receive registered multicast data flows stably and timely for a long time.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable IGMP snooping globally	1. Access the global configuration view. 2. Run the **igmp-snooping start** command.
Create a multicast VLAN	1. Access the global configuration view. 2. Run the *vlan vlan-list* command to create a VLAN for which IGMP snooping needs to be enabled. 3. Run the **igmp-snooping mvlan** *vlan-id* command to create the corresponding multicast VLAN and access the multicast VLAN configuration view.
(Optional) Configure the multicast data forwarding mode for a multicast VLAN	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping forwarding-mode { ip | mac }** command.
Configure an interface to join the VLAN and enable IGMP snooping on the interface	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } command to configure the type of VLANs for the Hybrid port. 4. Run the **igmp-snooping enable** command to enable multicast snooping for the interface.
Configure a static multicast group on an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* command.

Purpose	Procedure
Create the multicast group pre-join function	1. Access the global configuration view. 2. Run the **igmp-snooping group-address** *group-address* **mvlan** *vlan-id* command.

9.1.3 Configuring Multicast VLAN Copy

Background

The multicast VLAN copy function can be used to manage and control the multicast source and multicast group members, enable users in different VLANs to receive the same multicast stream, and reduce waste of bandwidth.

VLANs in the multicast VLAN copy function are classified into multicast VLAN and user VLAN. The multicast VLAN is the VLAN to which the interface connecting switch and multicast source belongs and it is used for aggregating multicast streams. The user VLAN is the VLAN to which the interface connecting multicast group member hosts belongs and it is used for receiving data flows from the multicast VLAN.

Purpose

This section describes how to configure parameters to meet the requirements in different application scenarios.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable IGMP snooping globally	1. Access the global configuration view. 2. Run the **igmp-snooping start** command.
Create a multicast VLAN	1. Access the global configuration view. 2. Run the **vlan** *vlan-list* command to create a VLAN for which IGMP snooping needs to be enabled. 3. Run the **igmp-snooping mvlan** *vlan-id* command to create the corresponding multicast VLAN and access the multicast VLAN configuration view.
Configure the IP multicast data	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping forwarding-mode ip** command.

Purpose	Procedure
forwarding mode for a multicast VLAN	
Enable the multicast copy function for a multicast VLAN	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping multicast-vlan enable** command.
Configure an uplink interface for IGMP snooping	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the command **igmp-snooping uplink-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** ***interface-number*** **or igmp-snooping uplink-port eth-trunk** *trunk-number*.
Configure user VLANs for multicast copy	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping multicast user-vlan** *vlan-list* command.
Configure an interface to join the VLAN and enable IGMP snooping on the interface	1. Access the global configuration view. 2. Access the interface group configuration view (Ethernet or Trunk). 3. Run the **port hybrid vlan** *vlan-list* { **tagged** | **untagged** } command to configure the type of VLANs for the Hybrid port. 4. Run the **igmp-snooping enable** command to enable multicast snooping for the interface.

9.1.4 Configuring IGMP Snooping

Background

VLAN-based IGMP snooping runs on the switch between router and user host. By snooping the multicast protocol packets transmitted between upper-layer router and host, IGMP snooping can maintain the multicast packet forwarding table entry to manage and control multicast packet forwarding and to implement L2 multicast.

Purpose

This section describes how to configure parameters to meet the requirements in different application scenarios.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable IGMP snooping globally	1. Access the global configuration view. 2. Run the **igmp-snooping start** command.
Create a multicast VLAN	1. Access the global configuration view. 2. Run the **vlan** *vlan-list* command to create a VLAN for which IGMP snooping needs to be enabled. 3. Run the **igmp-snooping mvlan** *vlan-id* command to create the corresponding multicast VLAN and access the multicast VLAN configuration view.
Enable or disable consistency check between the multicast destination MAC address and destination IP address	1. Access the global configuration view. 2. Run the **hwmc mac-ip-check { enable | disable }** command.
(Optional) Configure the multicast data forwarding mode for a multicast VLAN	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping forwarding-mode { ip | mac }** command.
(Optional) Configure the IGMP version	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping version { v1 | v2 | v3 }** command.
(Optional) Configure a static router interface	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the command **igmp-snooping uplink-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
Configure a query interval for a specific group	1. Access the global configuration view. 2. Access the MVLAN configuration view. 3. Run the **igmp-snooping lastmember-queryinterval {** *query-interval* | **default }** command.
Configure the number of specific queries	1. Access the global configuration view. 2. Access the MVLAN configuration view. 3. Run the **igmp-snooping lastmember-querynumber {** *query-number* | **default }** command.
(Optional) Configure a querier	1. Access the global configuration view.

Purpose	Procedure
	2. Run the **igmp-snooping query-interval** { *query-interval* | **default** } command to configure the query packet sending interval for the querier. (The parameter is shared among multicast VLANs.) 3. Run the **igmp-snooping robust-count** { *robust-count* | **default** } command to configure the IGMP robust count for the querier. (The parameter is shared among multicast VLANs.) 4. Access the multicast VLAN configuration view. 5. Run the **igmp-snooping querier** { **enable** | **disable** } command to configure the enabled state of the IGMP snooping querier. 6. Run the **igmp-snooping max-response-time** { *max-response-time* | **default** } command to configure a maximum response time for common query packets.
(Optional) Configure a multicast policy	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping group-policy filter-list** *acl-number* **version** *version-list* command.
(Optional) Configure protocol packet suppression	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping report-suppress { enable | disable** } command to enable packet suppression for a VLAN.
(Optional) Configure a multicast proxy IP address	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping proxy-ip** *ip-address* command to configure the source IP address of a query packet. This configuration is valid only when packet suppression is enabled or the working mode is proxy.
(Optional) Configure the Router-Alert checking function for a multicast VLAN	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping require-router-alert** { **enable** | **disable** } command to configure the Router-Alert option. Only IGMP packets with the Router-Alert option are processed after the Router-Alert option is enabled.
(Optional) Configure the IGMP snooping working mode	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping workmode { igmp-snooping | igmp-proxy }** command to configure the IGMP snooping working mode to snooping or proxy.
Enable or disable fast switchover	1. Access the global configuration view. 2. Access the multicast VLAN configuration view.

Purpose	Procedure
when the STP snooping changes	3. Run the **igmp-snooping fast-switch { enable | disable }** command.
Enable or disable sending the general query function when fast switchover is triggered due to changes of the STP snooping	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping fast-switch query { enable | disable }** command.
Enable or disable sending IGMP query packets to an interface	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping proxy-uplink-port { enable | disable }** command.
Configure the source IP address for a query packet in snooping mode.	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the following commands: ● **igmp-snooping send-query source-address** *src-address* ● **igmp-snooping send-query source-address default**
Enable or disable multicast entry learning prohibition on an uplink interface.	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping uplink-port drop-report { enable | disable }** command.
Limit the uplink interface number	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping uplink-port-limit** { *uplink-port-limit* | **default** } command,
Configure the 802.1p priority for the IGMP snooping protocol	1. Access the global configuration view. 2. Access the multicast VLAN configuration view. 3. Run the **igmp-snooping 8021p priority {** *value* | **default }** command.
(Optional) Configure the fast leave function on an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **igmp-snooping fast-leave { enable | disable }** command.
Configure controllable	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view.

Purpose	Procedure
multicast on an interface	3. Run the **igmp-snooping ctrlmode { enable | disable }** command.
Configure the global aging time for router interfaces	1. Access the global configuration view. 2. Run the **igmp-snooping router-aging-time** { *router-aging-time* | **default** } command.
Configure static user VLANs for multicast copy	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the command i**gmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*.
Delete specified or all static user VLANs for multicast copy	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the following commands: ● **no igmp-snooping static-group** ● **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list* ● **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan all** ● **no igmp-snooping static-group mvlan** *vlan-id*
Create an uplink interface for a multicast VLAN	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **igmp-snooping mvlan** *vlan-id* **uplink-port** command.
Delete an uplink interface of a multicast VLAN	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **no igmp-snooping mvlan** *vlan-id* **uplink-port** command.
Enable or disable the query packet duplication suppression function	1. Access the global configuration view. 2. Access the interface configuration view (Trunk), Ethernet bridge interface configuration view, or Ethernet routing interface configuration view. 3. Run the **igmp-snooping query-duplicate-suppress { enable | disable }** command.

9.1.5 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the IGMP snooping function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the IGMP snooping configuration file	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping config** command.
View the IGMP snooping interface configuration file	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping interface** command.
View the multicast VLAN configuration information in IGMP snooping configuration mode	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the s**how igmp-snooping mvlan** command.
View the multicast uplink port configuration information in IGMP snooping configuration mode	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping uplinkport** command.
View the egress port table entry information of all interfaces or designated interfaces or the specified VLAN of IGMP snooping	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the following commands: ● s**how igmp-snooping egress-port** ● **show igmp-snooping egress-port mvlan** *mvlan-id*

Purpose	Procedure
	● **show igmp-snooping egress-port interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
View the multicast group table entry information of IGMP snooping	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping group** command.
View the multicast source table entry information of IGMP snooping (valid for version 3)	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping source-address** command.
Clear the dynamic multicast table for IGMP snooping	1. Access the MVLAN configuration view or global configuration view. 2. Run the **reset igmp-snooping group** command to clear the dynamic multicast table (including group and egress-port) for IGMP snooping.
Display and view the global configuration information	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), MVLAN configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show igmp-snooping** command.
Display and view the IGMP snooping statistics	1. Access the common user view. 2. Run the following commands: ● **show igmp-snooping statistic** ● **show igmp-snooping statistic interface** ● **show igmp-snooping statistic interface { ethernet | xgigaethernet |10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show igmp-snooping statistic interface eth-trunk** *trunk-number*
Clear IGMP-snooping statistics	1. Access the global configuration view. 2. Run the **reset igmp-snooping statistic** command.

9.1.6 Configuration Example

9.1.6.1 Example of Configuring Static L2 Multicast

Network Requirements

Switch interface 10GE1/0/1 connects to the router at the multicast source side. Interface 10GE1/0/2 connects to the user host. It is required that, by configuring the static L2 multicast function, all hosts in VLAN 100 receive the multicast data with group address 225.1.1.1 for a long time, as shown in Figure 9-1.

Network Diagram

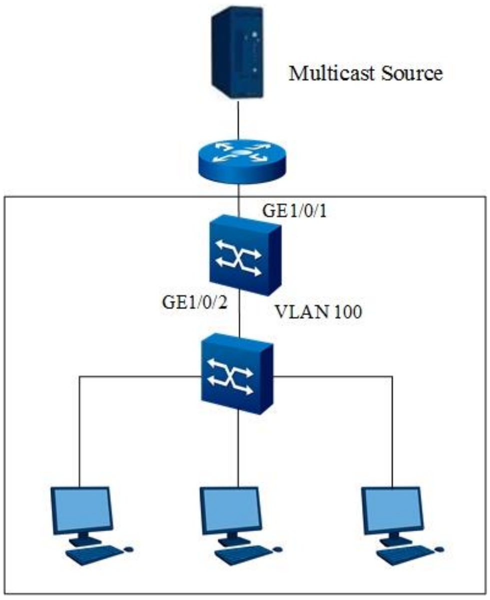


Figure 9-1 Network diagram of static L2 multicast

Configuration

1. Enable the IGMP snooping protocol globally.

Switch#configure
Switch(config)# igmp-snooping start;
Switch(config)#

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.

Switch(config)#vlan 100
Switch(vlan-100)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/2)#quit
Switch(config)# igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#

3. Enable IGMP snooping for the interface.

Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping enable
Switch(config-10ge1/0/2)#quit
Switch(config)#

4. Configure GE1/0/1 as a static router interface.

Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigaethernet 1/0/1
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#

5. Configure the static multicast group.

Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100
Switch(config-10ge1/0/2)#quit
Switch(config)#

6. Check the multicast group table and egress port table after the configuration is complete.

```
Switch#show igmp-snooping group
  Total Entry(s) : 1
  Group Address     MVlan    Pre-join    MemNum    V3FilterMode
  225.1.1.1           100       disable      1            invalid

Switch#show igmp-snooping egress-port
Total Entry(s) : 1

Group Address : 225.1.1.1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :       100
    V3 Mode : invalid
```

9.1.6.2 Example of Configuring IGMP Snooping

Network Requirements

Switch interface 10GE1/0/1 connects to the router at the multicast source side. Interface 10GE1/0/2 connects to the user host. It is required that, by configuring the IGMP snooping function, all the three hosts in VLAN 100 receive the multicast data with group addresses 225.1.1.1 and 225.1.1.2 for a long time, as shown in Figure 9-2.

Network Diagram

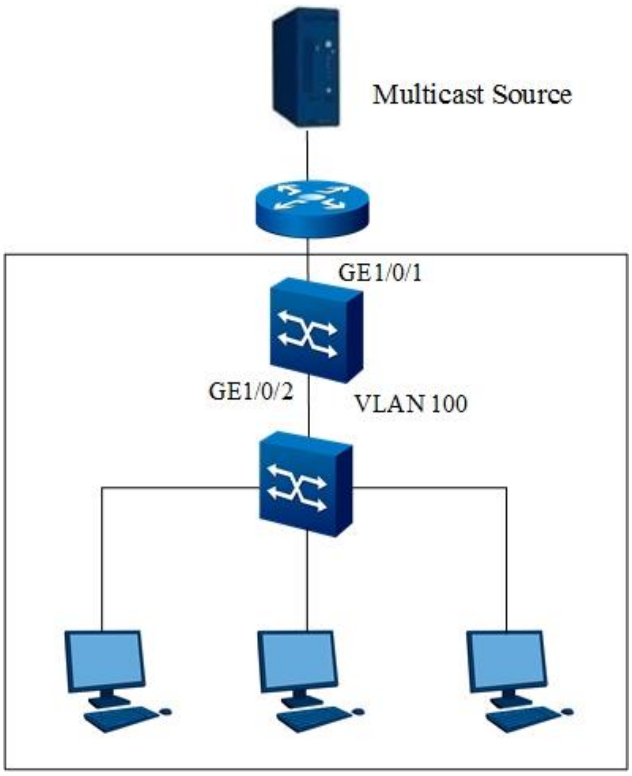


Figure 9-2 Network diagram of IGMP snooping configuration

Configuration

1. Enable the IGMP snooping protocol globally.

Switch#configure
Switch(config)#igmp-snooping start;
Switch(config)#

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.
Switch(config)#vlan 100
Switch(vlan-100)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#port hybrid vlan 100 tagged
Switch(config-10ge1/0/2)#quit
Switch(config)# igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#
3. Enable IGMP snooping for the interface.
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping enable
Switch(config-10ge1/0/2)#quit
Switch(config)#
4. Configure GE1/0/1 as a static router interface.
Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigaethernet 1/0/1
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#
5. Configure the static multicast group.
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.2 mvlan 100
Switch(config-10ge1/0/2)#quit
Switch(config)#
6. Check the multicast group table and egress port table after the configuration is complete.
Switch#show igmp-snooping group

```
Total Entry(s) : 2
Group Address     MVlan    Pre-join    MemNum    V3FilterMode
225.1.1.1         100      disable     1         invalid
225.1.1.2         100      disable     1         invalid
```

```
Switch#show igmp-snooping egress-port
Total Entry(s) : 2

Group Address : 225.1.1.1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :      100
    V3 Mode : invalid
Group Address : 225.1.1.2
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :      100
    V3 Mode : invalid
```

9.1.6.3 Example of Configuring Multicast VLAN Copy

Network Requirements

Switch interface 10GE1/0/1 connects to the router at the multicast source side and belongs to VLAN 100. Interfaces 10GE1/0/2 and 10GE10/3 connect to the user host and respectively belong to VLAN 2 and VLAN 3. It is required that the four hosts connecting to the switch receive the multicast data within group address range 225.0.0.1 to 225.0.0.3. VLAN 100 is a multicast VLAN. VLAN 2 and VLAN 3 are user VLANs, as shown in Figure 9-3.

Network Diagram

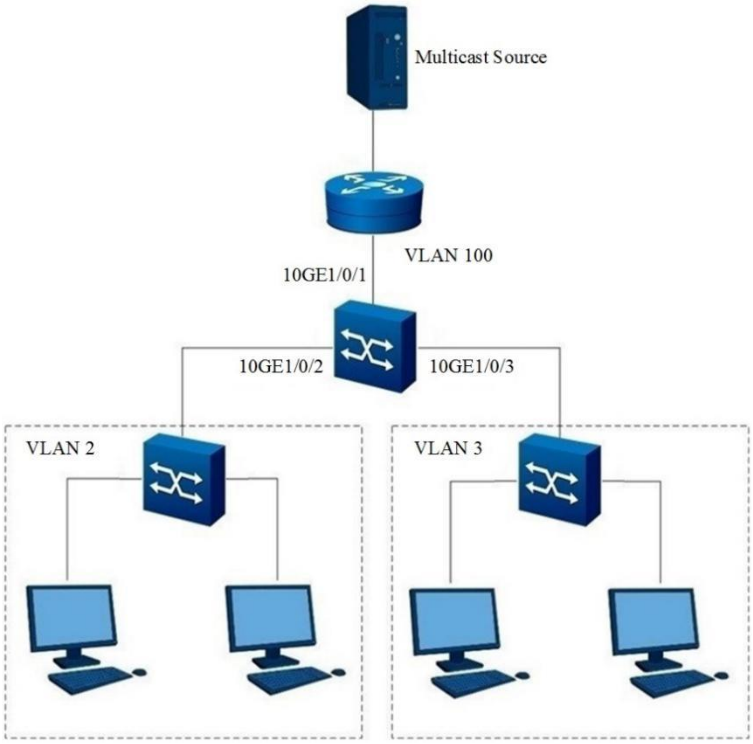


Figure 9-3 Multicast copy topology

Configuration

1. Enable the IGMP snooping protocol globally.

```
Switch#configure
Switch(config)#igmp-snooping start
Switch(config)#
```

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.

```
Switch(config)#vlan 2,3,100
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#port hybrid vlan 2 tagged
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)#port hybrid vlan 3 tagged
Switch(config-10ge1/0/3)#quit
Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#
```

3. Enable IGMP snooping for the interface.
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#igmp-snooping enable
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping enable
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)#igmp-snooping enable
Switch(config-10ge1/0/3)#quit
Switch(config)#
4. Enable the multicast copy function for the multicast VLAN and configure user VLANs.
Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#igmp-snooping forwarding-mode ip
Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable
Switch(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 2,3
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#
5. Configure 10GE1/0/1 as a static router interface.
Switch(config)#igmp-snooping mvlan 100
Switch(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port xgigaethernet 1/0/1
Switch(config-igmpsnoop-mvlan100)#quit
Switch(config)#
6. Configure the static multicast group.
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 3
Switch(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 3
Switch(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 3
Switch(config-10ge1/0/3)#quit
7. Check the multicast group table and egress port table after the configuration is complete.
Switch#show igmp-snooping group

```
Total Entry(s) : 3
Group Address     MVlan    Pre-join    MemNum    V3FilterMode
225.0.0.1         100      disable     2         invalid
225.0.0.2         100      disable     2         invalid
225.0.0.3         100      disable     2         invalid
```

```
Switch#show igmp-snooping egress-port
Total Entry(s) : 6

Group Address : 225.0.0.1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :       2
    V3 Mode : invalid
Group Address : 225.0.0.1
MVlan : 100
Source Address : *
Interface : xge-1/0/3
    Type : static
    Expires : ---
    OutVlan :       3
    V3 Mode : invalid
Group Address : 225.0.0.2
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :       2
    V3 Mode : invalid
Group Address : 225.0.0.2
MVlan : 100
Source Address : *
Interface : xge-1/0/3
    Type : static
    Expires : ---
    OutVlan :       3
    V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
```

Expires : ---
OutVlan : 2
V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
Interface : xge-1/0/3
Type : static
Expires : ---
OutVlan : 3
V3 Mode : invalid

9.2 Configuring IGMP

9.2.1 Introduction to IGMP

IGMP Overview

Internet Group Management Protocol (version 3) (IGMP) is used by IPv4 routers to discover multicast members on their directly connected network segments. Multicast members are host nodes that want to receive multicast data.

Through the IGMP protocol, routers can know whether there are members of IPv4 multicast group on their directly connected network segment, and establish and maintain the membership of multicast group. Routers also maintain timer information related to these IPv4 multicast addresses.

IGMP routers use IPv4 addresses as source addresses to send IGMP packets. The protocol number of IGMP is 2, which can be used to identify whether packets are IGMP packets.

Supported IGMP Versions

There are three IGMP versions:

- IGMPv1 (defined by RFC1112)
- IGMPv2 (defined by RFC2236)
- IGMP (defined by RFC3376)

All these versions are based on the query and response mechanism to manage the members of IPv4 multicast groups, and IGMPv3 is added with the function of filtering multicast sources based on IGMPv1 and IGMPv2.

All IGMP versions support the Any-Source Multicast (ASM) model, and IGMPv3 can be directly applied to the Source-Specific Multicast (SSM) model.

IGMP Features Supported by Switch

- Basic IGMP functions
  - Supports IGMPv1, IGMPv2, and IGMPv3.
  - Supports static multicast groups and multicast sources.
- The Router-Alert option can be configured.

  IGMPv2 and IGMPv3 contain query packets of specified groups or specified sources/groups, and these groups are ever-changing, so Switch cannot join all groups, so IGMP sends the group packets sent to the local host but not joining the upper layer protocol for processing through the Router-Alert option.

Received IGMP packets not carrying this option will be dropped. You can configure whether the Router-Alert option must be included in the header of received or sent IGMP packets as needed.

- IGMP query controller

  You can set performance parameters such as sending interval and robust count of General Query packets as needed.

- IGMP Limit

  You can limit the number of single-instance IGMP global entries and the number of IGMP multicast group members on an interface.

9.2.2 IGMP Working Principle

The working principle of IGMP includes the following five aspects.

9.2.2.1 Querier Election

When there are multiple IPv4 multicast routers in a network segment, all the routers can receive the IGMP membership report from the host, so only one of them needs to send the IGMP query message. For this purpose, the system must elect a router as the IGMP querier, and the election process is as follows.

(1) All IGMP routers consider themselves as queriers first, and send an IGMP general query packet (the destination address is 224.0.0.1) to all hosts and routers in the local network segment.

(2) After receiving the packet, other IGMP routers in the local network segment compare the source IPv4 address of the packet with their own interface address. Then, the router with the smallest IPv4 address serves as the querier, and other routers are non-queriers.

(3) The Other Querier Present Timer will be started on all non-queriers. Before the timer expires, if an IGMP query packet from the querier is received, the timer is reset. Otherwise, the original querier is considered invalid, and a new querier election process is initiated.

9.2.2.2 Joining an IPv4 Multicast Group

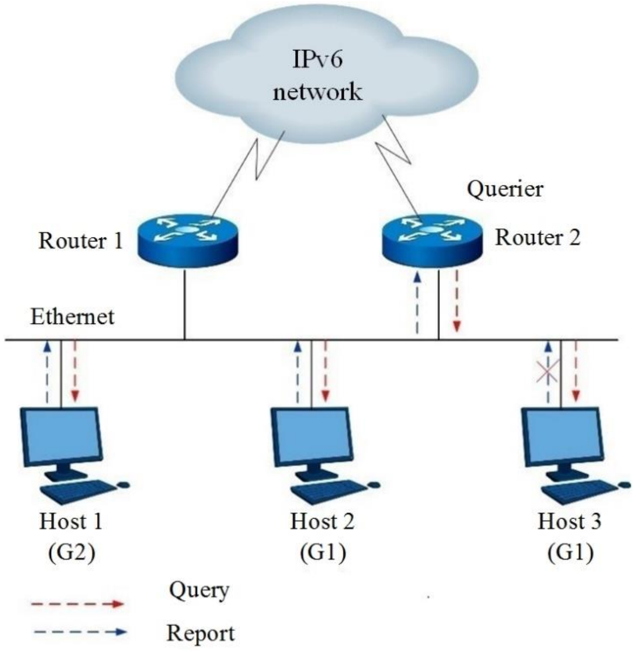


Figure 9-4 IGMP query response

As shown in Figure 9-4, assume that Host 1 and Host 3 want to receive IPv4 multicast data sent to IPv4 multicast group G1, and Host 1 wants to receive IPv4 multicast data sent to IPv4 multicast group G2. The process for the host to join IPv4 multicast group and for the IGMP querier (Router B) to maintain IPv4 multicast group membership is as follows.

(1) The host actively sends the IGMP member report packet to the IPv4 multicast group it wants to join to declare its joining, without waiting for the IGMP query packet sent by the IGMP querier

(2) The IGMP querier (Router B) periodically sends a General Query packet (the destination address is 224.0.0.1) to all hosts and routers in the local network segment by multicast.

(3) After receiving the query packet, pay attention to one of Host 2 and Host 3 of G1 (depending on whose delay timer expires first). For example, Host 2 will first send an IGMP member report packet to G1 by multicast to announce that it belongs to G1. All hosts in the local network segment can receive the report packet sent by Host 2 to G1, so when Host 3 receives the report packet, it will no longer send the same report packet to G1, because IGMP routers (Router 1 and Router 2) already know that there are hosts interested in G1 in the local network segment. This mechanism is called IGMP member report suppression mechanism on the hosts, which helps to reduce the information flow of the local network segment.

(4) However, because Host 1 is concerned about G2, it will still send a report packet to G2 by multicast to announce that it belongs to G2.

(5) After the above query and response process, IGMP routers know that there are members of G1 and G2 in the local network segment, so the IPv4 multicast routing protocol (such as IPv4 PIM) generates (*, G1) and (*, G2) multicast forwarding items as the forwarding basis of IPv4 multicast data, where "*" represents any IPv4 multicast source.

(6) When IPv4 multicast data sent to G1 or G2 by an IPv4 multicast source arrives at IGMP routers through a multicast route, because there are (*, G1) and (*, G2) multicast forwarding items on IGMP routers, the IPv4 multicast data is forwarded to the local network segment, and the recipient host can receive the IPv4 multicast data.

9.2.2.3 Leaving an IPv4 Multicast Group

When a host leaves an IPv4 multicast group:

(1) The host sends a Done packet to all IPv4 multicast routers in the local network segment (the destination address is 224.0.0.2).

(2) After receiving the packet, the querier sends a Multicast-Address-Specific Query packet to the IPv4 multicast group that the host declared to leave (the destination address field and the group address field are filled with the IPv4 multicast group address to be queried).

(3) If there are other members of the IPv4 multicast group in the network segment, these members will send a member report packet within the Maximum Response Delay set in the packet after receiving the Multicast-Address-Specific Query packet.

(4) If the member report packet sent by other members of the IPv4 multicast group is received within the Maximum Response Delay, the querier will continue to maintain the membership of the IPv4 multicast group. Otherwise, the querier will think that there is no member of this IPv4 multicast group in this network segment, so it will not maintain the membership of this IPv4 multicast group.

9.2.2.4 Filtering Multicast Sources

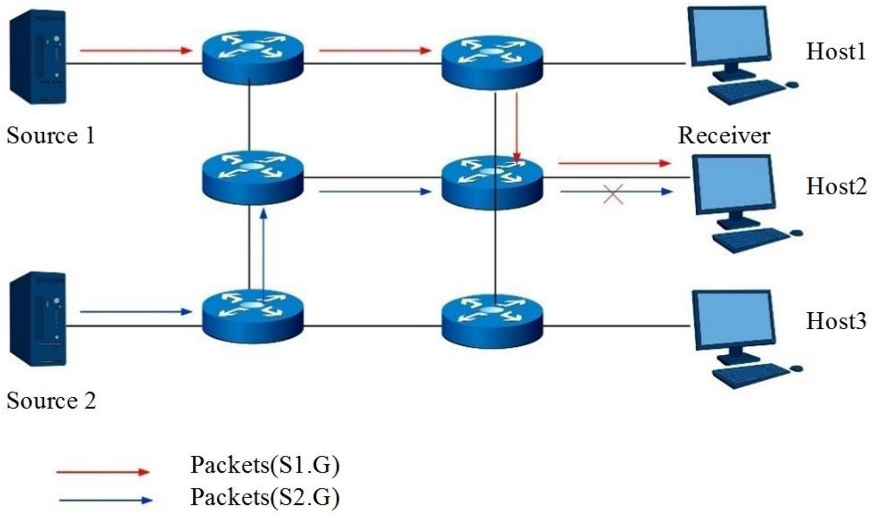


Figure 9-5 IPv4 multicast stream path of specific source group

IGMPv1 runs between hosts and routers

When Host 2 joins IPv4 multicast group G, it cannot select an IPv4 multicast source, so whether Host 2 needs the information or not, IPv4 multicast information from Source 1 and Source 2 will be delivered to Host B.

IGMPv2 runs between hosts and routers

In this mode, Host 2 can only request to receive IPv4 multicast information (S1, G) from Source 1 and destined for G, or request to reject IPv4 multicast information (S2, G) from Source 2 and destined for G, so that only IPv4 multicast information from Source 1 can be delivered to Host 2.

IGMPv3 runs between hosts and routers

IGMPv3 adds a filtering mode (INCLUDE/EXCLUDE) for IPv4 multicast sources, so that hosts can explicitly request to receive or reject IPv4 multicast information from the specific IPv4 multicast source S while joining the IPv4 multicast group G. When a host joins an IPv4 multicast group:

(1) If the host wants to only receive IPv4 multicast information from specified IPv4 multicast sources such as S1 and S2, its report packet can be marked as INCLUDE Sources(S1, S2, ...). If the host wants to reject IPv4 multicast information from specified IPv4 multicast sources, such as S1 and S2, its report packet can be marked as EXCLUDE Sources (S1, S2, ...).

(2) As shown in Figure 9-5, there are two IPv4 multicast sources in the network: Source 1 (S1) and Source 2 (S2), both of which send IPv4 multicast packets to IPv4 multicast group G. Host 2 is only interested in the information sent from Source 1 to G, but not the information from Source 2.

9.2.2.5 Multicast Group State

Multicast routers running IGMP maintain the state of IPv4 multicast groups according to Per Multicast Address Per Attached Link on each directly connected link. An IPv4 multicast group can have the following states:

(1) Filter mode: Keep tracing the status of INCLUDE or EXCLUDE.

(2) Source list: keep track of adding or deleting IPv4 multicast sources.

(3) Timer: the filter timer that switches to the INCLUDE mode after the IPv4 multicast address times out, and the source timer about the source record.

9.2.3 Configuring Basic IGMP Functions

Background

IGMP is applied to the network segment where Switch is connected to the user host, and both Switch and the user host need to run IGMP.

Prerequisite

The link layer protocol parameters and IP address of the interfaces are matched, and the interface state is UP.

Purpose

Configuring basic IGMP functions can realize forwarding of multicast data and maintain membership among multicast group members.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable IGMP globally	1. Access the global configuration view. 2. Run the **igmp start** command to enable IGMP globally. 3. Run the **igmp** or **igmp vpn-instance** *vpn-instance-name* command to enable IGMP for an instance.
Enable IGMP on an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **igmp enable** command.
(Optional) Configure the IGMP version	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **igmp version** { **v1** | **v2** | **v3** | **default** } command.
(Optional) Configure a static IGMP group	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● Run the **igmp static-group** *group-address* command to create a static IGMP multicast group for an interface. ● Run the command **igmp static-group** *group-address* egress-port { **ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* to create a static IGMP multicast group for an interface and specify the outbound interface. ● Run the **igmp static-group** *group-address* **source** *source-address* command to create a static IGMP group and specify a multicast source address on an interface. ● Run the command **igmp static-group** *group-address* **source** *source-address* egress-port { **ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* to create a static IGMP group and specify the outbound interface and multicast source address.
Delete the created static IGMP multicast group and specified outbound interface from an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the command **no igmp static-group** *group-address* **egress-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }.**
Delete the created static IGMP multicast group and specified	1. Access the global configuration view. 2. Access the VLANIF configuration view.

Purpose	Procedure
multicast source address from an interface	3. Run the **no igmp static-group** *group-address* **source** *source-address* command.
Delete the created static IGMP multicast group and specified outbound interface and multicast source address from an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the command **no igmp static-group** *group-address* **source** *source-address* **egress-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.

9.2.4 Configuring IGMP Performance Parameters

Background

Generally, IGMP can work normally with default performance parameters. Switch allows users to adjust parameters as needed.

The following IGMP performance parameters can be configured globally or on a specific interface. The global configuration is valid on all interfaces. Interface-based configuration is valid on the designated interface only. An interface value is superior to the global value, and the global value is inherited when no interface value is not configured.

When IGMPv1 is used, you can configure a sending interval and robust count of the IGMP General Query packets for an IGMP querier.

When IGMPv2 or IGMPv3 is used, you can configure the following parameters for an IGMP querier: sending interval of IGMP General Query packets, sending interval of IGMP Multicast-Address-Specific Query packets, Maximum Response Delay of IGMP query packets, Other IGMP Querier Present Timer, and IGMP robust count.

Prerequisite

Before configuring IGMP performance parameters, you must configure reachable IP routes between nodes on the network and configure basic IGMP functions referring to the section 9.2.3.

Purpose

Optimize IGMP performance parameters based on application environments.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

<table>
<tr><th>Purpose</th><th>Procedure</th></tr>
<tr><td rowspan="2">Configure an IGMP packet option</td><td>[Configure an IGMP packet option globally]
1. Access the global configuration view.
2. Access the IGMP configuration view.
3. Run the require-router-alert command to specify that IGMP packets received must contain the Router-Alert option in packet headers.
Or run the send-router-alert command to specify that IGMP packets sent by devices carry the Router-Alert option in packet headers globally.</td></tr>
<tr><td>[Configure an IGMP packet option for an interface]
1. Access the global configuration view.
2. Access the VLANIF configuration view.
3. Run the igmp require-router-alert command to specify that IGMP packets received must contain the Router-Alert option in packet headers.
Or run the igmp send-router-alert command to specify that IGMP packets sent on an interface must carry the Router-Alert option.</td></tr>
<tr><td rowspan="2">Configure an IGMPv1 querier</td><td>[Configure a global IGMPv1 querier]
1. Access the global configuration view.
2. Access the IGMP configuration view or MLD configuration view.
3. Run the timer query { interval | default } command to configure the sending interval of IGMP General Query packets globally.
4. Run the robust-count { robust | default } command to configure the global IGMP querier robust count (this command is applicable only in the IGMP configuration view).</td></tr>
<tr><td>[Configure an IGMPv1 querier for an interface]
1. Access the global configuration view.
2. Access the VLANIF configuration view.
3. Run the igmp timer query { interval | default } command to configure the sending interval of IGMP General Query packets on an interface.
4. Run the igmp robust-count { robust | default } command to configure the sending interval of an IGMP querier on an interface.</td></tr>
<tr><td>Configure an IGMPv2/v3 querier</td><td>[Configure an IGMPv2/v3 querier globally]
1. Access the global configuration view.
2. Access the IGMP configuration view or MLD configuration view.
3. Run the timer query { interval | default } command to configure the sending interval of IGMP General Query packets globally.
4. Run the robust-count { robust | default } command to configure the global IGMP querier robust count (this command is applicable only in the IGMP configuration view).</td></tr>
</table>

	5. Run the **max-response-time** { *interval* | **default** } command to configure the Maximum Response Delay for an IGMP query packet (this command is applicable only in the IGMP configuration view). 6. Run the **timer other-querier-present** { *interval* | **default** } command to configure the IGMP other querier present timer globally. 7. Run the **lastmember-queryinterval** { *interval* | default } command.
	[Configure an IGMPv2/v3 querier on an interface] 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **igmp timer query** { *interval* | **default** } command to configure the sending interval of IGMP General Query packets on an interface. 4. Run the **igmp robust-count** { *robust* | **default** } command to configure the sending interval of an IGMP querier on an interface. 5. Run the **igmp max-response-time** { *interval* | **default** } command to configure the Maximum Response Delay for IGMP query packets on an interface. 6. Run the **igmp timer other-querier-present** *interval* command to configure the IGMP other querier present timer on an interface. 7. Run the **igmp lastmember-queryinterval** { *interval* | **default** } command to configure the interval at which the IGMP querier sends Group-Specific Query packets after receiving an IGMP Leave packet from a host. 8. Run the **igmp general-query** command to configure VLAN interfaces to send General Query messages globally.
Enable or disable IGMP fast leave	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **igmp fast-leave** { **enable** | **disable** } command.
Configure an IGMP multicast group filter on an interface to limit the range of multicast groups that the host can join	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **igmp group-policy filter-list** *acl-number* ● **igmp group-policy filter-list** *acl-number* **version** *version-list*
Configure an IGMP multicast group filter on an interface to limit the range of multicast groups that the host can join	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **no igmp group-policy** command to delete the IGMP multicast group filter on an interface.

9.2.5 Configuring the IGMP Limit Function

Background

The IGMP Limit function is generally configured on the last hop switch that connects users.

Prerequisite

Before configuring IGMP Limit Function, you must configure reachable IP routes between nodes on the network and configure basic IGMP functions referring to the section 9.2.3.

Purpose

Configure IGMP Limit to limit the number of multicast groups that an interface can join.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the IGMP global entry limit for a single instance	1. Access the global configuration view. 2. Access the IGMP configuration view. 3. Run the **limit** { *number* | **default** } command to configure the maximum number of IGMP entries that can be created in the system.
Configure the number of IGMP group members on an interface	1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the **igmp limit** { *number* | **default** } command.

9.2.6 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the IGMP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the information of an IGMP VPN instance	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the following commands: ● **show igmp vpn-instance** ● **show igmp vpn-instance** *name*
View the IGMP configuration	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the **show igmp config** command.
View information about a multicast outbound interface	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the following commands: ● **show igmp egress-port { static | dynamic | all } [vlan** *vlan-id* **]** ● **show igmp egress-port { static | dynamic | all } vlan** *vlan-id* **group** *group-address* ● **show igmp egress-port { static | dynamic | all } vlan** *vlan-id* **group** *group-address* **source** *source-address*
View information about an IGMP group	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the **show igmp group { static | dynamic | all } [vlan** *vlan-id* **]** command.
View the IGMP information on an interface	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the following commands: ● **show igmp interface**

Purpose	Procedure
	● **show igmp interface vlan** *vlan-id* ● **show igmp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show igmp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface*
View all information about a designated IGMP interface	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the **show igmp interface vlan** *vlan-id* command.
View the multicast source information	1. Access the common user view, privileged user view, global configuration view, VLANIF configuration view, IGMP configuration view, or IGMP VPN configuration view. 2. Run the following commands: ● **show igmp source { static | dynamic | all } [vlan** *vlan-id* **]** ● **show igmp source { static | dynamic | all } vlan** *vlan-id* **group** *group-address*

9.2.7 Configuration Example

Network Requirements

Switch interfaces 10GE1/0/2 and 10GE1/0/3 join VLAN 3 with IP address 1.1.1.2/24. Interfaces 10GE1/0/2 and 10GE1/0/3 connect with Host 1 and Host 2 respectively. Interface 10GE1/0/1 connects other devices and the multicast source. Host 1 sends an IGMP join packet, requesting to receive the data sent to 225.0.0.1. Host 2 does not support IGMP but wants to receive data from 226.1.1.1. Enable IGMP on VLAN 3 to which the hosts connect and enable a static multicast group for Host 2 to realize the above purposes.

Network Diagram

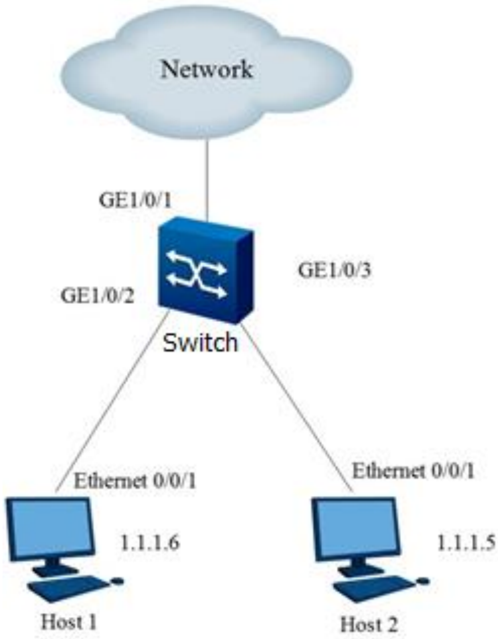


Figure 9-6 IGMP configuration network diagram

Configuration

1. Create VLAN 3 and configure its IP address. Enable GE1/0/2 and GE1/0/3 to join VLAN 3.

```
Switch#configure
Switch(config)#interface vlan 3
Switch(config-vlan-3)#ip address 1.1.1.2/24
Switch(config-vlan-3)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#port hybrid vlan 3 untagged
Switch(config-10ge1/0/2)#port hybrid pvid 3
Switch(config-10ge1/0/2)#no shutdown
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)#port hybrid vlan 3 untagged
Switch(config-10ge1/0/3)#port hybrid pvid 3
Switch(config-10ge1/0/3)#no shutdown
Switch(config-10ge1/0/3)#quit
```

2. Enable IGMP and configure a static multicast group.

```
Switch(config)#igmp start
Switch(config)#igmp
Switch(config-igmp)#quit
Switch(config)#interface vlan 3
```

Switch(config-vlan-3)#igmp enable
Switch(config-vlan-3)#igmp version v3
Switch(config-vlan-3)#igmp static-group 226.1.1.1 egress-port gigaethernet 1/0/3
Switch(config-vlan-3)#quit
Switch(config)#

3. Check the configuration result.

After Host 1 sends an IGMP join packet, run the following commands to view the information.

```
Switch#show igmp config
 igmp start
 igmp
 VID:3
 igmp enable
 igmp version v3
 igmp static-group 226.1.1.1
 igmp static-group 226.1.1.1 egress-port ge1/0/3

Switch#show igmp interface
 VID      Querier-address      Version Fast-leave       Querier-remain
 3        1.1.1.2              v3      disable          36
Switch#show igmp group a
VLAN ID is:3
   Group Address:225.0.0.1
   Last reporter address:1.1.1.6
   Uptime:6490 s
   Expiry Time:242 s
   Exclude mode expiry time:242 s
   V1 Host Timer:0 s
   V2 Host Timer:242 s
   Filter mode:exclude
   Group status:dynamic
VLAN ID is:3
   Group Address:226.1.1.1
   Last reporter address:0.0.0.0
   Uptime:6228 s
   Expiry Time:0 s
   Exclude mode expiry time:0 s
   V1 Host Timer:0 s
   V2 Host Timer:0 s
   Filter mode:include
   Group status:static
```

Switch#show igmp source all

VID	Group-Address	Source-Address	Expiry-Time	Mode	Ingress-Port	Status
3	225.0.0.1	0.0.0.0	0	include	unknown	dynamic
3	226.1.1.1	0.0.0.0	0	include	unknown	static

Switch#show igmp egress-port all

VID	Group-Address	Source-Address	Egress-Port	Status
3	225.0.0.1	0.0.0.0	ge-1/0/2	dynamic
3	226.1.1.1	0.0.0.0	ge-1/0/3	static

9.3 Configuring MLD Snooping

9.3.1 Overview of MLD Snooping

The MLD Snooping protocol has the following features:

1. Static L2 multicast: Adding an interface to a multicast group statically can avoid protocol packet attach. Use the mechanism of directly searching the multicast message forwarding table to reduce network delay.
2. Multicast VLAN copy: Multicast VLAN copy can implement multicast data transmission among different VLANs and thereby provide conveniences in multicast source and group member management and control, which reduces bandwidth consumption.
3. Support for VLAN-based MLD snooping:
   (1) Support MLD V1 and MLD V2
   (2) Support configuring the multicast forwarding mode
   (3) Support static router interfaces
   (4) Support MLD query
   (5) Support MLD packet suppression
   (6) Support the interface fast leave function
   (7) Support configuring an aging time for router interfaces
   (8) Support configuring the maximum response time of group members
   (9) Support configuring multicast policies
   (10) Support configuring the Router Alert option
   (11) Support configuring the source IP address for sending IGMP packets
   (12) Support IGMP proxy

9.3.2 Configuring MLD Snooping

Purpose

By listening to the multicast protocol packets transmitted between routers and hosts, the MLD snooping can maintain the interface information of multicast packets, so as to manage and control the forwarding of multicast data packets and to realize L2 multicasting.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the multicast function globally. If you disable the multicast function globally, all multicast configurations are cleared.	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping** { **start** | **stop** } command.
Configure a specific query interval in the unit of s	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping lastmember-queryinterval** **{** *queryinterval-value* | **default }** command.
Configure a general query interval in the unit of s	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping query-interval** { *queryinterval-value* | **default** } command.
Configure a robust count for outbound interface entries	1. Run the **configure** command to access the global configuration view. 3. Run the **mld-snooping robust-count** { *robust-count-num* | **default** } command.
Configure a router port aging time in the unit of s	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping router-aging-time {** *router-aging-time* | **default }** command.
Create a multicast VLAN and access the multicast VLAN configuration view	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command.

Purpose	Procedure
Configure a forwarding mode for the multicast VLAN To set to the IP mode, the VLAN of the multicast VLAN must be already created.	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping forwarding-mode { ip | mac }** command.
Configure a multicast policy for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping group-policy filter-list** *acl-number* command.
Configure the maximum response time of general queries within the multicast VLAN, in the unit of s	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping max-response-time** { *responsetime-value* | **default** } command.
Enable or disable the multicast copy function within a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping multicast-vlan { enable | disable }** command.
Configure user VLANs for multicast copy	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping multicast user-vlan** *vlan-list* command.
Delete the user VLANs configured for multicast copy	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **no mld-snooping multicast user-vlan** command.
Configure the packet suppression function for a multicast VLAN	1. Run the **configure** command to access the global configuration view.

Purpose	Procedure
	2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping report-suppress { enable | disable }** command.
Enable or disable a querier for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping querier { enable | disable }** command.
Configure the Router Alert option for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping require-router-alert { enable | disable }** command.
Configure an uplink interface (router interface) for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **command mld-snooping uplink-port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
Configure the protocol version for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping version { v1 | v2 }** command.
Configure the protocol working mode for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping workmode { mld-snooping | mld-proxy }** command.
Configure an IP proxy for a multicast VLAN	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping proxy-ip** *ipv6-address* command.

Purpose	Procedure
Enable or disable the fast switchover function when the STP topology changes	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping fast-switch { enable | disable }** command.
Enable or disable sending the query function when fast switchover is triggered due to changes of the STP topology	1. Run the **configure** command to access the global configuration view. 2. Run the **mld-snooping mvlan** *vlan-id* command to access the multicast VLAN configuration view. 3. Run the **mld-snooping fast-switch query { enable | disable }** command.
Enable the multicast protocol on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the command **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* to access the configuration view of a designated interface. 3. Run the **mld-snooping { enable | disable }** command.
Enable quick leave on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the command **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* to access the configuration view of a designated interface. 3. Run the **mld-snooping fast-leave { enable | disable }** command.
Configure a static multicast group on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the command **interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* to access the configuration view of a designated interface. 3. Run the **mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id* **user-vlan** *vlan-list* command.

9.3.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the MLD snooping function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable MLD snooping debugging.	1. Access the privileged user view. 2. Run the **debug mldsnoop** command.
Disable MLD snooping debugging	1. Run the **disable** command to return to the common user view, or remain in the current privileged user view. 2. Run the **no debug mldsnoop** command.
Display the multicast configuration information	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping config** command.
Display the information about a multicast outbound port table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping egress-port** command.
Display the information about a multicast group table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping group** command.
Display the information about a multicast interface table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping interface** command.
Display the information about a	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the

Purpose	Procedure
multicast VLAN table	**interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping mvlan** command.
Display the information about a multicast source table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping source-address** command.
Display the information about a multicast uplink interface table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, run the **interface vlan** *vlan-id* command to access the VLANIF configuration view, or remain in the current privileged user view. 2. Run the **show mld-snooping uplinkport** command.
Display the current basic parameter configurations of MLD snooping	1. Run the **disable** command to return to the common user view. 2. Run the **show mld-snooping** command.
Clear the MLD snooping multicast group information	1. Run the **configure** command to access the global configuration view. 2. Run the **reset mld-snooping group** command.

9.3.4 Configuration Example

9.3.4.1 Configuring MLD Snooping

Network Requirements

As shown in Figure 9-7, the switch interface 10GE1/0/1 is connected to the router on the multicast source side. The interface 10GE1/0/2 is connected to the user host. All hosts in the VLAN 100 can receive multicast data from the group addresses FF1E::1 to FF1E::2 through MLD snooping function.

Network Diagram

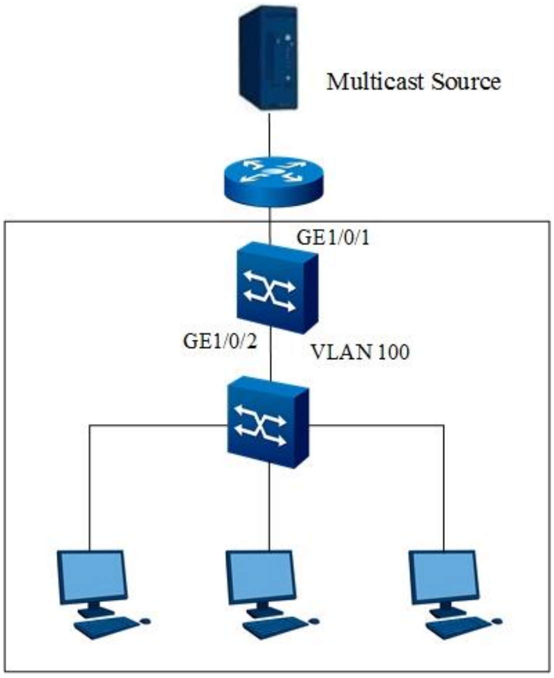


Figure 9-7 Network diagram of MLD snooping configuration

Configuration

1. Enable the MLD snooping protocol globally.

Switch#configure

Switch(config)# mld-snooping start;

Switch(config)#

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.

Switch(config)#vlan 100

Switch(vlan-100)#quit

Switch(config)#interface xge1/0/1

Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/2)#quit

Switch(config)# mld-snooping mvlan 100

Switch(config-mldsnoop-mvlan100)#quit

Switch(config)#

3. Enable the MLD snooping protocol on the interface.

Switch(config)#interface xge1/0/1
Switch(config-10ge1/0/1)#mld-snooping enable

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2
Switch(config-10ge1/0/2)#mld-snooping enable

Switch(config-10ge1/0/2)#quit

Switch(config)#

4. Configure GE1/0/1 as a static router interface.

Switch(config)#mld-snooping mvlan 100

Switch(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1

Switch(config-mldsnoop-mvlan100)#quit

Switch(config)#

5. Configure the static multicast group

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100

Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::2 mvlan 100

Switch(config-10ge1/0/2)#quit

Switch(config)#

6. Check the multicast group table and egress port table after the configuration is complete.

```
Total Entry(s) : 1
  Group Address          MVlan      Pre-join MemNum V2FilterMode
    ff1e::1              100        disable    1       invalid
    ff1e::2              100        disable    1       invalid
Switch#show mld-snooping egress-port
Total Entry(s) : 2
```

Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :   100
    V2 Mode : invalid

Group Address : ff1e::2
MVlan : 100
Source Address : *
Interface : xge-1/0/2
    Type : static
    Expires : ---
    OutVlan :   100
    V2 Mode : invalid

9.3.4.2 Configuring Static L2 Multicast

Network Requirements

As shown in Figure 9-8, the switch interface 10GE1/0/1 is connected to the router on the multicast source side. The interface 10GE1/0/2 is connected to the user host. It is required that all hosts in VLAN 100 can receive the multicast data from the group FF1E::1 for a long time by configuring static L2 multicast.

Network Diagram

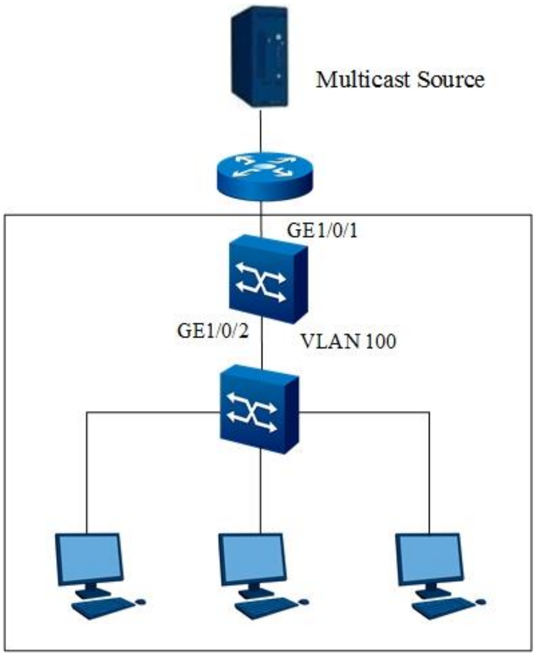


Figure 9-8 Network diagram of static L2 multicast

Configuration

1. Enable the MLD snooping protocol globally.

Switch#configure

Switch(config)# mld-snooping start;

Switch(config)#

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.

Switch(config)#vlan 100

Switch(vlan-100)#quit

Switch(config)#interface xge1/0/1

Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/2)#quit

Switch(config)# mld-snooping mvlan 100

Switch(config-mldsnoop-mvlan100)#quit

Switch(config)#

3. Enable the MLD snooping protocol on the interface.

Switch(config)#interface xge1/0/1

Switch(config-10ge1/0/1)#mld-snooping enable

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#mld-snooping enable

Switch(config-10ge1/0/2)#quit

Switch(config)#

4. Configure GE1/0/1 as a static router interface.

Switch(config)#mld-snooping mvlan 100

Switch(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1

Switch(config-mldsnoop-mvlan100)#quit

Switch(config)#

5. Configure the static multicast group

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100

Switch(config-10ge1/0/2)#quit

Switch(config)#

6. Check the multicast group table and egress port table after the configuration is complete.

```
Switch#show mld-snooping group
 Total Entry(s) : 1
 Group Address          MVlan     Pre-join MemNum V2FilterMode
 ff1e::1                100       disable   1      invalid
Switch#show mld-snooping egress-port
Total Entry(s) : 1
Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V2 Mode : invalid
```

9.3.4.3 Configuring Multicast VLAN Copy

Network Requirements

As shown in Figure 9-9, the switch interface GE1/0/1 is connected to the router on the multicast source side and belongs to VLAN 100. The interfaces GE1/0/2 and GE1/0/3 are connected to the user host, and belong to VLAN 2 and VLAN 3 respectively. The four hosts connected to the switch can receive multicast data from the group addresses FF1E::1 to FF1E::3. VLAN 100 is a multicast VLAN and VLAN 3 and VLAN 4 are user VLANs.

Network Diagram

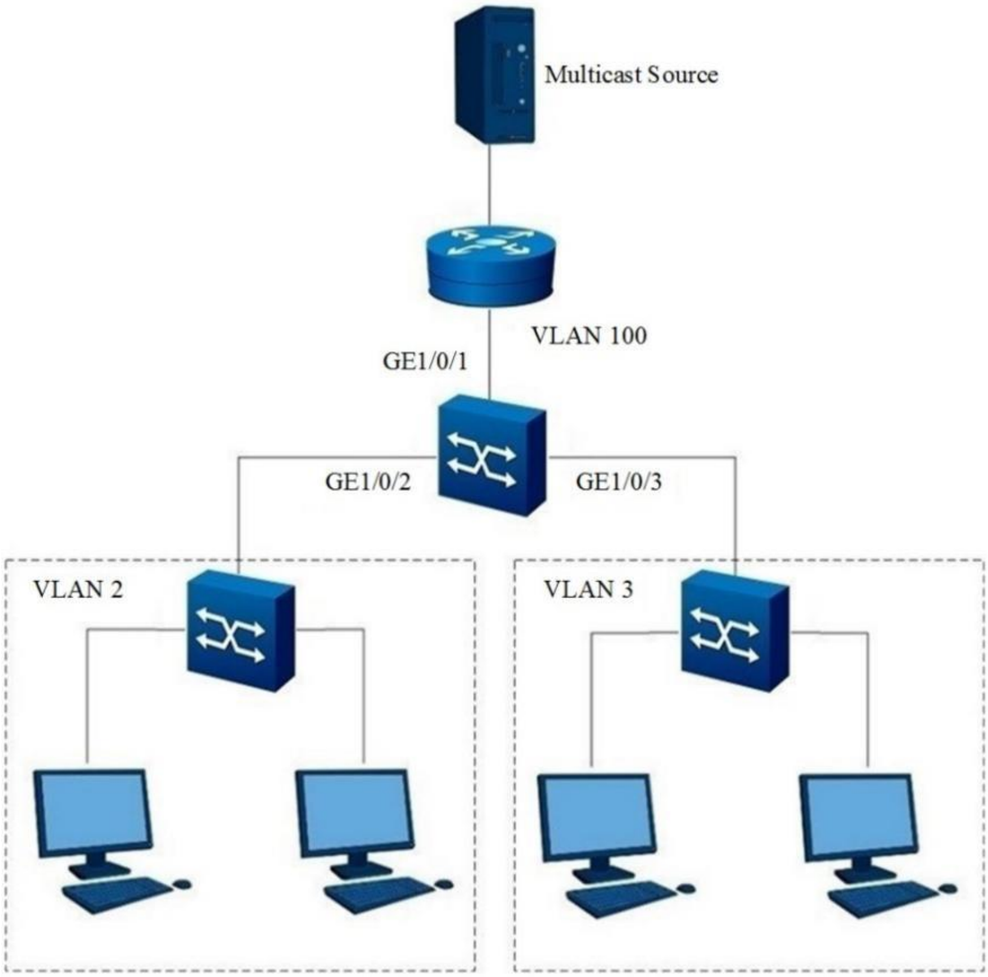


Figure 9-9 Multicast copy topology

Configuration

1. Enable the MLD snooping protocol globally.

Switch#configure

Switch(config)# mld-snooping start;

Switch(config)#

2. Create a VLAN and the corresponding multicast VLAN. Add the interface to the VLAN.

Switch(config)#vlan 2,3,100

Switch(config)#interface xge1/0/1

Switch(config-10ge1/0/1)#port hybrid vlan 100 tagged

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#port hybrid vlan 2 tagged

Switch(config-10ge1/0/2)#quit

Switch(config)#interface xgigaethernet 1/0/3

Switch(config-10ge1/0/3)#port hybrid vlan 3 tagged

Switch(config-10ge1/0/3)#quit

Switch(config)# mld-snooping mvlan 100

Switch(config-mldsnoop-mvlan100)#quit

Switch(config)#

3. Enable the MLD snooping protocol on the interface.

Switch(config)#interface xge1/0/1

Switch(config-10ge1/0/1)#mld-snooping enable

Switch(config-10ge1/0/1)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#mld-snooping enable

Switch(config-10ge1/0/2)#quit

Switch(config)#interface xgigaethernet 1/0/3

Switch(config-10ge1/0/3)#mld-snooping enable

Switch(config-10ge1/0/3)#quit

Switch(config)#

4.Enable the multicast copy function for the multicast VLAN and configure user VLANs.

```
Switch(config)#mld-snooping mvlan 100
Switch(config-mldsnoop-mvlan100)#mld-snooping forwarding-mode ip
Switch(config-mldsnoop-mvlan100)#mld-snooping multicast-vlan enable
Switch(config-mldsnoop-mvlan100)#mld-snooping multicast user-vlan 2,3
Switch(config-mldsnoop-mvlan100)#quit
Switch(config)#
```

5. Configure GE1/0/1 as a static router interface.

```
Switch(config)#mld-snooping mvlan 100
Switch(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1
Switch(config-mldsnoop-mvlan100)#quit
Switch(config)#
```

6. Configure the static multicast group

```
Switch(config)#interface xge1/0/2
Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::2 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::3 mvlan 100 user-vlan 2
Switch(config-10ge1/0/2)#quit
Switch(config)#interface xgigaethernet 1/0/3
Switch(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::1 mvlan 100 user-vlan 3
Switch(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::2 mvlan 100 user-vlan 3
Switch(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::3 mvlan 100 user-vlan 3
Switch(config-10ge1/0/2)#quit
```

7. Check the multicast group table and egress port table after the configuration is complete.

```
Switch#show mld-snooping group
 Total Entry(s) : 3
 Group Address         MVlan     Pre-join MemNum V2FilterMode
 ff1e::1            100      disable   2      invalid
 ff1e::2            100      disable   2      invalid
 ff1e::3            100      disable   2      invalid
```

```
Switch#show mld-snooping egress-port
Total Entry(s) : 6

Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : ge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V2 Mode : invalid
Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : ge-1/0/3
   Type : static
   Expires : ---
   OutVlan :    100
   V2 Mode : invalid
Group Address : ff1e::2
MVlan : 100
Source Address : *
Interface : ge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V2 Mode : invalid
Group Address : ff1e::2
MVlan : 100
Source Address : *
Interface : ge-1/0/3
   Type : static
   Expires : ---
   OutVlan :    100
   V2 Mode : invalid
```

Group Address : ff1e::3
MVlan : 100
Source Address : *
Interface : ge-1/0/2
    Type : static
    Expires : ---
    OutVlan :   100
    V2 Mode : invalid
Group Address : ff1e::3
MVlan : 100
Source Address : *
Interface : ge-1/0/3
    Type : static
    Expires : ---
    OutVlan :   100
    V2 Mode : invalid

Chapter 10 Configuring Security Function

This chapter describes the basic content, configuration procedure, and configuration examples of the security function of the Switch.

10.1 Configuring Time-range

10.1.1 Overview of Time-range

Background

Time-range is a timing module used to limit the effective time range of commands. It can be used with ACL and other functions.

10.1.2 Accessing the Time-range Module and Configuring Its Name

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Access a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module.
Define the descriptive name for a specific time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **name** *name* command;
Delete the range configuration from a specific time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **no time-range** *range-number* command.

10.1.3 Configuring the Start Time Range of a Time-range Module

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the absolute start time and end time of a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the command **time-range** *range-number* absolute **from** hh:mm:ss MM/DD **to** hh:mm:ss MM/DD.
Configure the daily time range for a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everyday** *hh:mm:ss* **to** *hh:mm:ss* command to configure the daily time range for a time-range module..
Configure the hourly time range for a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everyhour** *mm:ss* **to** *mm:ss* command to configure the hourly time range for a time-range module.
Configure the monthly time range for a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everymonth** *hh:mm:ss mm* **to** *hh:mm:ss mm* command to configure the monthly time range for a time-range module.
Configure the weekly time range for a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the command **time-range** *range-number* **everyweek** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } to configure the weekly time range for a time-range module.
Configure the time range on every weekday of a time-range module (except weekends)	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everyweekday** *hh:mm:ss* **to** *hh:mm:ss* command to configure the workday time range (weekdays except the weekends) of the time-range module.

Purpose	Procedure
Configure the time range for a time-range module every weekend	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everyweekend** *hh:mm:ss* **to** *hh:mm:ss* command to configure the weekend time range of the time-range module.
Configure the yearly time range for a time-range module	1. Access the global configuration view. 2. Run the **time-range list** *list-number* command to access a time-range module 3. Run the **time-range** *range-number* **everyyear** *hh:mm:ss mm/dd* **to** *hh:mm:ss mm/dd* command to configure the yearly time range for a time-range module.

10.1.4 Maintenance and Debugging

Purpose

This section describes how to check and locate the fault when the time-range function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable time-range debugging	1. Access the privileged user view. 2. Run the **debug time-range or no debug time-range** command.
View the configuration of all the current time-range modules	1. Access the privileged user view or global configuration view, or run the **time-range list** *list-number* command to access a time-range module. 2. Run the **show time-range config** command.
View the list information of all the current time-range modules or a specific time-range module	1. Access the privileged user view or global configuration view, or run the **time-range list** *list-number* command to access a time-range module. 2. Run the **show time-range list or show time-range list** *list-number* command.

10.2 Configuring IP Address Prefix Filter

10.2.1 Overview of Address Prefix Filter Table

An address prefix filter table provides a set of ordered filter rules based on routing address domains (IP address, address prefix length range, and application rule) to enable selective use of different paths to obtain IP routing entries. Different protocols are matched with the address domains of routing entries to filter routes.

Within the IPv4 range, an address prefix list is identified by the list name under the same address type. Each prefix list may contain multiple entries. Each entry specifies the range for matching a network prefix form, and the match range is identified by an index. The index specifies the order of match checking and can be allocated automatically or manually.

In the matching process, the system checks all indexed entries in ascending order. The matching process ends once a matching entry is found.

Caution

A matching error occurs if the entries of the address prefix list are not configured in logical order. Operators must ensure correct configuration.

10.2.2 Configuring an Address Prefix Filter Table

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create a filter rule to fully match network segment addresses with length of MASKLEN	1. Run the **configure** command to access the global configuration view. 2. Run the **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* command.
Create a filter rule (with the route address mask length greater than or equal to the specified minimum value) to fully match the network	1. Run the **configure** command to access the global configuration view.

Purpose	Procedure
segment address of prefix mask length	2. Run the command **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range*.
Create a filter rule (with the route address mask length smaller than or equal to the specified maximum value) to fully match the network segment address of prefix mask length	1. Run the **configure** command to access the global configuration view. 2. Run the **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **less-equal** *max-range* command.
Create a filter rule (with the route address mask length smaller than or equal to the specified maximum and minimum value range) to fully match the network segment address of prefix mask length	1. Run the **configure** command to access the global configuration view. 2. Run the command **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range* **less-equal** *max-rang*.

10.2.3 Maintenance and Debugging

Purpose

This section describes how to check, debug and locate the fault when the address prefix filter table function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable IP address prefix filter table debugging	1. Remain in the current privileged user view. 2. Run the **debug prefix-list { config | match | error | all }** command.
Disable IP address prefix filter table debugging	1. Remain in the current privileged user view. 2. Run the **no debug prefix-list { config | match | error | all }** command.
Delete an existing filter rule	1. Run the **configure** command to access the global configuration view. 2. Run the **no ip prefix-list** *list-name* [**index** *index-number*] command.

Purpose	Procedure
View rules in a rule table	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, or remain in the current privileged user view. 2. Run the **show ip prefix-list** [*list-name*] command.
View information of IP address prefix rules	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, or remain in the current privileged user view. 2. Run the **show ip prefix-list information** command.

10.3 Configuring ACL

Note:

In this section, ACL means the access control list for filtering IPv4 packets.

10.3.1 Overview of ACL

ACL Function

The Switch determines whether to forward or deny data packets based on the rules and actions configured for an access control list (ACL). ACL configuration implements data transmission control, improves network performance, and guarantees service security.

ACL is a series of sequential rules and actions composed of L2 MAC and L3 IP addresses. These rules are used to filter data packets according to the source and destination addresses and port numbers of data packets. Data packets are classified based on ACL rules. After ACL rules are applied to the Switch, the switch determines whether to accept, deny, or take other actions on received packets based on the rules.

ACLs Supported by Switch

Switch supports the following types of ACLs:

- L2 ACL: Classifies data packets mainly based on the source MAC address, destination MAC address, VLAN, priority, protocol type, rate limiting template, and time range template.
- L3 ACL: Performs more refined classification of data packets based on the source IP address, destination IP address, source port number, destination port number, protocol type, priority, fragmentation, TTL, rate limiting template, and time range template.
- Mixed ACL: Classifies data packets mainly based on the source MAC address, destination MAC address, source IP address, destination IP address, source port number, destination port number, protocol type, priority, VLAN, rate limiting template, and time range template.

10.3.2 Configuring an L2 ACL

Background

An ACL is a series of lists composed of rules and actions.

Before configuring an L2 ACL rule, you need to create an L2 ACL and specify the ACL type number in the range 1 to 1000.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an L2 ACL	1. Access the global configuration view. 2. Run the **filter-list** *acl-number* [**name** *filter-name*] command to create an L2 ACL and access the L2 ACL configuration view.
Configure an L2 ACL rule	1. Access the global configuration view. 2. Access the L2 ACL configuration view. 3. Run the following commands to configure ACL rules matching the MAC entry (users can choose from the following commands on demand):

Purpose	Procedure
	• **filter** *rule-number* **mac {** src-mac-address/M **| any } {** dst-mac-address/M **| any }** • **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } { **customer | provider } (any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* } • **filter** *rule-number* **src-mac** *src-mac-address* **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **{ customer | provider } { any |** *vlan-id* **|** *vlan-id1/vlan-id2* **} { any |** *priority* **}** • **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | *digitial-protocol-value* } • **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* } • **filter** *rule-number* **mac {** *src-mac-address/M* **| any }** { *dst-mac-address/M* **| any } provider {** *vlan-id1/vlan-id2* **} { any |** *priority* **} customer { any |** *vlan-id* **} { any |** *priority* **}** • **filter** *rule-number* **mac** { *src-mac-address/M* | **any**) { *dst-mac-address/M* | **any**) **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { *vlan-id1/vlan-id2* } { **any** | *priority* } • **filter** *rule-number* **src-mac** { *src-mac-address/M* | **any** } **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id*) { **any** | *priority* } • **filter** *rule-number* **src-mac** { *src-mac-address/M* | **any** } **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider** { *vlan-id1/vlan-id2* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* } • **filter** *rule-number* **src-mac** { *src-mac-address/M* **| any } src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider { any** | *vlan-id* } **{ any** | *priority* **} customer {** *vlan-id1/vlan-id2*) **{ any** | *priority* **}**
Configure an L2 ACL action	1. Access the global configuration view. 2. Access the L2 ACL configuration view. 3. Run the following commands: • **filter** *rule-number* **action { permit | deny }** • **filter** *rule-number* **action redirect cpu** • **filter** *rule-number* **action mirror group** *group-number*

Purpose	Procedure
	• **filter** *rule-number* **action redirect { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* • **filter** *rule-number* **action redirect eth-trunk** *trunk-number* • **filter** *rule-number* **action { insert-inner-vid | insert-outer-vid }** *vlan-id* • **filter** *rule-number* **action replace-inner-vid** *vlan-id* • **filter** *rule-number* **action replace-outer-vid** *vlan-id* • **filter** *rule-number* **action { remove-inner-vid | remove-outer-vid }** *vlan-id* • **filter** *rule-number* **action { cos | precedence }** *priority-value* • **filter** *rule-number* **action { outer-tag-priority | inner-tag-priority }** *priority-value* • **filter** *rule-number* **action dscp** *dscp*
Delete an ACL action	1. Access the global configuration view. 2. Access the ACL configuration view. 3. Run the **no filter** *rule-number* **action** command.
Delete an ACL rule	1. Access the global configuration view. 2. Access the ACL configuration view. 3. Run the **no filter** *rule-number* command.
Delete an ACL	1. Access the global configuration view. 2. Access the ACL configuration view. 3. Run the **no filter-list** *acl-number* command.
Bind an L2 ACL	1. Access the global configuration view. 2. Access the Ethernet interface configuration view or L2 ACL configuration view, and run the following commands to bind an ACL to a physical port, Trunk interface, or a VLAN interface: • **filter-list-l2 { in | out }** *acl-number* • **filter-list-l2 { in | out } name** *acl-name* or 1. Access the global configuration view. 2. Run the **filter-list-l2 global** { **in** | **out** } *acl-number* command.

10.3.3 Configuring an L3 ACL

Background

An ACL is a series of lists composed of rules and actions.

Before configuring an L3 ACL rule, you need to create an L3 ACL and specify the ACL type number in the range 1001 to 2000.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an L3 ACL	1. Access the global configuration view. 2. Run the **filter-list** *acl-number* [**name** *filter-name*] command to create an L3 ACL and access the L3 ACL configuration view.
Configure an L3 ACL rule	1. Access the global configuration view. 2. Access the L3 ACL configuration view. (You can perform configuration as needed in Steps 3 through 8.) 3. (Optional) Run the following commands to configure an ACL rule for IP address matching (you can choose from the following commands as needed): ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** } **precedence** tos-priority ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** **{** *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask {***dst-ip-mask* | **any** } **precedence** *tos-priority* ● **filter** *rule-number* ip **{** *src-ip-address/M* **| any } {** *dst-ip-address/M* **| any } dscp {dscp field | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }** ● **filter** *rule-number* **src-ip {** *src-ip-address* **| any } src-mask {***src-ip-mask* **| any} dst-ip {***dst-ip-address* **| any } dst-mask {** *dst-ip-mask* **| any } dscp { dscp field | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }**

Purpose	Procedure
	● **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** } **fragment** ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** **{** *src-ip-mask* | any} **dst-ip {** *dst-ip-address* | **any** } **dst-mask {** *dst-ip-mask* | **any** } **fragment** ● **filter** *rule-number* **ip** {*src-ip-address/M* | **any** } {*dst-ip-address/M* | **any** } **precedence** *tos field* **fragment** ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **precedence** *tos field* **fragment** ● **filter** *rule-number* **ip** { *src-ip-address/M* **| any** } { *dst-ip-address/M* **| any** } **tos** *tos-value* ● **filter** *rule-number* **ip {** *src-ip-address/M* **| any } {** *dst-ip-address/M* **| any } dscp {*dscp field* | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef } fragment** ● **filter** *rule-number* **src-ip {** *src-ip-address* **| any } src-mask { *src-ip-mask* | any } dst-ip {** *dst-ip-address* **| any } dst-mask {** *dst-ip-mask* **| any } dscp { *dscp field* | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef } fragment** ● **filter** *rule-number* **ip** { *src-ip-address/M* **| any** } { *src-ip-address/M* **| any** } **proto-type** *proto-type field* ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **proto-type** *proto-type field* ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **ttl** *ttl-value* ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** **{** *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **ttl** *ttl-value* 4. (Optional) Run the following commands to configure an ACL rule for TCP matching (you can choose from the following commands as needed): ● **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } ● **filter** *rule-number* **tcp** *{ src-ip-address/M* | **any** *} { src-port-number* | **any** | *source-port-number-range } { dst-ip-address/M* | **any** *}*

Purpose	Procedure
	{ dst-port-number | **any** | *destination-port-number-range } {* **syn** | **synack** | **ack** | **fin** *}* ● **filte*r*** *rule-number* **tcp** *{ src-ip-address/M* | **any** *} { src-port-number* | **any** | *source-port-number-range } { dst-ip-address/M* | **any** *} { dst-port-number* | **any** | *destination-port-number-range } {* **syn** | **synack** | **ack** | **fin** } **fragment** ● **filter** *rule-number* **tcp** *{ src-ip-address/M* | **any** *} { src-port-number* | **any** | *source-port-number-range } { dst-ip-address/M* | **any** *} { dst-port-number* | **any** | *destination-port-number-range }* **fragment** ● **filter** *rule-number* **tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** *{ src-ip-mask* | **any** } **dst-mask** *{ dst-ip-mask* | **any** } *{ dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } [**fragment**] ● **filter** *rule-number* **tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } [**fragment**] 5. (Optional) Run the following commands to configure an ACL rule for ICMP matching (you can choose from the following commands as needed): ● **filter** *rule-number* **icmp** { *src-ip-address/M* **| any }** { *dst-ip-address/M* **| any** } ● **filter** *rule-number* **icmp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } ● **filter** *rule-number* **icmp** { *src-ip-address/M* **| any }** { *dst-ip-address/M* **| any** } { *icmp type* **| any** } { *icmp code* | **any** } ● **filter** *rule-number* **icmp src-ip** *src-ip-address* **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *icmp type* **| any** } { *icmp code* **| any** } ● **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } **fragment** ● **filter** *rule-number* **icmp src-ip** *src-ip-address* **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } **fragment** 6. (Optional) Run the following commands to configure an ACL rule for IGMP matching (you can choose from the following commands as needed):

Purpose	Procedure
	● **filter** *rule-number* **igmp** { *src-ip-address/M* **| any }** { *dst-ip-address/M* **| any** } ● **filter** *rule-number* **igmp src-ip** { *src-ip-address/M* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } ● **filter** *rule-number* **igmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **fragment** ● filter *rule-number* igmp src-ip { *src-ip-address/M* | any } src-mask { *src-ip-mask* | any } dst-ip { *src-ip-mask* | any } dst-mask { dst-ip-mask | any } fragment 7. (Optional) Run the following commands to configure an ACL rule for UDP matching (you can choose from the following commands as needed): ● **filter** *rule-number* **udp** { *src-ip-address/M* | **any** } { *src-port-numbe*r | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } **{** *dst-port-number* **| any } | fragment** ● **filter** *rule-numbe*r **udp {***src-ip-address/M* **| any} {** *src-port-number* **|** *source-port-number-range/destination-port-number-range* **| any} {** *dst-ip-address/M* **| any} {** *dst-port-number* **|** *source-port-number-range/destination-port-number-range* **| any } | precedence** *tos-priority* ● **filter** *rule-number* **udp src-ip** { *src-ip-address* | **any**} **src-mask** *src-ip-mask* **{** *src-port-number* **| any } dst-ip** { *src-ip-mask* | **any** } **dst-mask {** *dst-ip-mask* | **any** } **{** *dst-port-number* **| any }** ● **filter** *rule-number* **udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range }* **{** *dst-port-number* **| any } | precedence** *tos-priority*
Configure an L3 ACL action	1. Access the global configuration view. 2. Access the L3 ACL configuration view. 3. Run the following commands: ● **filter** *rule-number* **action { permit | deny }** ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **filter** *rule-number* **action redirect eth-trunk** *trunk-number* ● **filter** *rule-number* **action { insert-inner-vid | insert-outer-vid }** *vlan-id*

Purpose	Procedure
	• **filter** *rule-number* **action replace-inner-vid** *vlan-id* • **filter** *rule-number* **action replace-outer-vid** *vlan-id* • **filter** *rule-number* **action remove-inner-vid** *vlan-id* • **filter** *rule-number* **action remove-outer-vi**d *vlan-id* • **filter** *rule-number* **action { outer-tag-priority | inner-tag-priority }** *Priority-value* • **filter** *rule-number* **action** { **cos** | **precedence** } *priority-value* • **filter** *rule-number* **action dscp** *dscp* • **filter** *rule-number* **action { precedence-priority | priority-precedence }** • **filter** rule-number **action counter** *counter number* • **filter** rule-number **action tos** *tos number*
Bind an L3 ACL	1. Access the global configuration view. 2. Access the Ethernet interface configuration view or L2 ACL configuration view, and run the following commands to bind an ACL to a physical port, Trunk interface, or a VLAN interface: • **filter-list-ipv4 { in | out }** *acl-number* • **filter-list-ipv4 { in | out } name** *acl-name* or 1. Access the global configuration view. 2. Run the **filter-list-ipv4 global** { **in** | **out** } *acl-number* command.

10.3.4 Configuring a Mixed ACL

Background

An ACL is a series of lists composed of rules and actions.
Before configuring a mixed ACL rule, you need to create a mixed ACL and specify the ACL type number in the range 2001 to 3000.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a mixed ACL	1. Access the global configuration view. 2. Run the **filter-list** *acl-number* [**name** *filter-name*] command to create a mixed ACL and access mixed ACL configuration view.
Configure a mixed ACL rule	1. Access the global configuration view. 2. Access the mixed ACL configuration view. 3. In mixed mode, you can configure L2 and L3 ACL rules. See 10.3.2 and 0.
Configure a mixed ACL action	1. Access the global configuration view. 2. Access the mixed ACL configuration view. 3. Run the following commands: ● **filter** *rule-number* **action { permit | deny }** ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **filter** *rule-number* **action { insert-inner-vid |insert-outer-vid }** *vlan-id* ● **filter** *rule-number* **action replace-inner-vid** *vlan-id* ● **filter** *rule-number* **action replace-outer-vid** *vlan-id* ● **filter** *rule-number* **action remove-inner-vid** ● **filter** *rule-number* **action** { **cos** | **precedence** } *priority-value* ● **filter** *rule-number* **action { outer-tag-priority | inner-tag-priority }** *priority-value* ● **filter** *rule-number* **action dscp** *dscp* ● **filter** *rule-number* **action { precedence-priority | priority-precedence }** ● **filter** rule-number **action counter** *counter number* ● **filter** rule-number **action tos** *tos number*
Bind a mixed ACL	1. Access the global configuration view. 2. Access the Ethernet interface configuration view or L2 ACL configuration view, and run the following commands to bind an ACL to a physical port, Trunk interface, or a VLAN interface: ● **filter-list-hybrid { in | out }** *acl-number* ● **filter-list-hybrid { in | out } name** *acl-name* or 1. Access the global configuration view. 2. Run the **filter-list-hybrid global** { **in** | **out** } *acl-number* command to bind an ACL to all interfaces.

10.3.5 Configuring an L3 ACL6

Background

An ACL is a series of lists composed of rules and actions.

Before configuring ACL6 rules, create an L3 ACL6 and assign a number in the range of 3001-4000 to the ACL6.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create an L3 ACL6	1. Run the **configure** command to access the global configuration view. 2. Run the **filter-list** *acl-number* command to create an L3 ACL6 and access its configuration view.
Configure an L3 ACL6 rule	1. Run the **configure** command to access the global configuration view. 2. Run the **filter-list** *acl-number* command to access the L3 ACL6 configuration view. (You can perform configuration as needed in Steps 3 through 8.) 3. (Optional) Run the following commands to configure an ACL rule matching IPv6 addresses (you can choose from the following commands as needed): ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **next-header** *next-header-value* ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **hop-limit** *hop-limit-value* 4. (Optional) Run the following commands to configure ACL rules matching TCP6 fields (you can choose from the following commands as needed): ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**

Purpose	Procedure
	● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** } ● **filter** *rule-numbe*r **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** } **fragment** 5. (Optional) Run the following commands to configure ACL rules matching ICMP6 fields (you can choose from the following commands as needed): ● **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } [**fragment**] ● **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** } [**fragment**] 6. (Optional) Run the following command to configure ACL rules matching IGMP6 fields (you can choose from the following commands as needed):: ● **filter** *rule-number* **igmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } 7. (Optional) Run the following commands to configure ACL rules matching UDP6 fields (you can choose from the following commands as needed): ● **filter** *rule-number* **udp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } ● **filter** *rule-number* **udp6** *{ src-ip6-address/M* | **any** *}* *{ src-port-number* | **any** | *src-port-range } { dst-ip6-address/M* | **any** *} { dst-port-number* | **any** | *dst-port-range }* **fragment**
Configure an L3 ACL6 action	1. Run the **configure** command to access the global configuration view. 2. Run the **filter-list** *acl-number* command to access the L3 ACL6 configuration view. 3. Run the following commands to configure an ACL action: ● **filter** *rule-number* **udp6** *{ src-ip6-address/M* | **any** *}* *{ src-port-number* | **any** | *src-port-range } { dst-ip6-address/M* | ***any*** *} { dst-port-number* | **any** | *dst-port-range }* **fragment** ● **filter** *rule-number* **action redirect cpu**

Purpose	Procedure
	● **filter** *filter-rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **filter** *rule-number* **action redirect eth-trunk** *trunk-number* ● **filter** *rule-number* **action { insert-inner-vid | insert-outer-vid }** *vlan-id* ● **filter** *rule-number* **action replace-inner-vid** *vlan-id* ● **filter** *rule-number* **action replace-outer-vid** *vlan-id* ● **filter** *rule-number* **action remove-inner-vid** ● **filter** *rule-number* **action remove-outer-vid** ● **filter** *rule-number* **action { outer-tag-priority | inner-tag-priority }** *priority-value* ● **filter** *rule-number* **action dscp** *dscp-value* ● **filter** *filter-rule-number* **action counter** *counter-number* ● **filter** *rule-number* **action tos** *tos number*
Bind an L3 ACL6	1. Access the global configuration view. 2. Access the Ethernet interface configuration view or L2 ACL configuration view, and run the following commands to bind an ACL to a physical port, Trunk interface, or a VLAN interface: ● **filter-list-ipv6 { in | out }** *acl-number* ● **filter-list-ipv6 { in | out } name** *acl-name* or 1. Access the global configuration view. 2. Run the **filter-list-ipv6 global** { **in** | **out** } *acl-number* command.

10.3.6 Configuring ACL Optional Functions

Background

ACL optional functions include:

- Creating an ACL effective time period

  After the ACL effective time period is created and applied when an ACL rule is configured, this ACL rule is effective during this period. If the time period is not specified when the ACL rule is configured, this rule is not limited by time range unless the ACL is deleted.

- Creating an ACL rate limiting template

  After an ACL rate limiting template is created and bound to an ACL rule, data packets are filtered according to different rate limiting rules.

- Creating an ACL counter template

  After an ACL counter template is created and bound to an ACL rule, statistics are collected on data packets according to different types of counting.

Purpose

This section describes how to configure ACL optional functions according to practical applications to provide multiple methods of packet filtering.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an ACL effective time period	1. Access the global configuration view. 2. Run the **time-range list** *LIST-NUMBER* command to access the time range configuration view. 3. Run the following commands to configure the absolute start time and end time for a time-range module: ● **time-range** *range-number* **absolute from** *hh:mm:ss YY/MM/DD* ● **time-range** *range-number* **absolute from** *hh:mm:ss YY/MM/DD* **to** *hh:mm:ss YY/MM/DD* 4. Run the **time-range** *range-number* **everyday** *hh:mm:ss* **to** *hh:mm:ss* command to configure the daily time range for a time-range module. 5. Run the **time-range** *range-number* **everyhour** *mm:ss* **to** *mm:ss* command to configure the hourly time range for a time-range module. 6. Run the **time-range** *range-number* **everymonth** *hh:mm:ss MM* **to** *hh:mm:ss MM* command to configure the monthly time range for a time-range module. 7. Run the command **time-range** *range-number* **everyweek** *hh:mm:ss* **{ mon | tue | wed | thu | fri | sat | sun } to hh:mm:ss { mon | tue | wed | thu | fri | sat | sun }** to configure the weekly time range for a time-range module.

Purpose	Procedure
	8. Run the **time-range** *range-number* **everyweekday** *hh:mm:ss* **to** *hh:mm:ss* command to configure the workday time range (weekdays except the weekends) of the time-range module. 9. Run the **time-range** *range-number* **everyweekend** *hh:mm:ss* **to** *hh:mm:ss* command to configure the weekend time range of the time-range module. 10. Run the **time-range** *range-number* **everyyear** *hh:mm:ss MM/DD* **to** *hh:mm:ss MM/DD* command to configure the yearly time range for a time-range module. 11. Run the **quit** command to return to the global configuration view. 12. Access the ACL configuration view. 13. Run the **time-range list** *list-number* command to bind a time range template to an ACL.
Create an ACL rate limiting template	1. Access the global configuration view. 2. Run the following commands to configure a meter template: ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number {* **aware | blind** *}* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number {* **aware | blind** *}* 3. Access the ACL configuration view. 4. Run the **filter** *filter rule number* **meter** *meter number* command to bind an ACL rule to a meter template. 5. Run the following commands to configure coloring packet processing according to the rate limiting template: ● **filter** *rule-number* **outaction { red | yellow } drop** ● **filter** *rule-number* **outaction { red | yellow } remark-dscp** *dscp* ● **filter** *rule-number* **outaction { red | yellow } remark-dot1p** *priority* ● **filter** *rule-number* **car** *car-value* **outaction drop** ● **filter** *rule-number* **outaction { red | yellow } remark-cfi** *cfi-value*
Create an ACL counter template	1. Access the global configuration view.

Purpose	Procedure
	2. Run the command **counter** *counter-number* **{ packet | byte | all } sort { green | red | greenred | greenyellow | redyellow | total }** to configure a counter template. 3. Access the ACL configuration view. 4. Run the **filter** *rule-number* **action counter** *counter-number* command to bind the counter template to an ACL.

10.3.7 View and Debugging

Purpose

To implement ACL function viewing, statistics, or modification. ACL statistics enable the device to monitor the interfaces and debug device traffic or template problems.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Clear ACL statistics	1. Access the global configuration view. 2. Run the following commands to reset ACL filter entry count: ● **reset counter filte-list** *acl-number* **filter** *rule-number* **{ in | out }** ● **reset counter filte-list** *acl-number* **filter** *rule-number* **port { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **{ in | out }** ● **reset counter filte-list** *acl-number* **filter** *rule-number* **port eth-trunk** *trunk-number* **{ in | out }** ● **reset** counter **filte-list** *acl-number* **filter** *rule-number* **vlan** *vlan-id* { **in** | **out** }
View the ACL configuration	1. Access the common user view, privileged user view, global configuration view, filter configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, interface group configuration view, or batch interface configuration view. 2. Run the following commands: ● **show filter-list** ● **show filter-list** *acl-number*

Purpose	Procedure
View the ACL configuration file information	1. Access the common user view, privileged user view, global configuration view, filter configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show filter-list config** command.
View ACL statistics	1. Access the common user view, privileged user view, global configuration view, filter configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show filter-list statistic** command.
View the information of all ACL-enabled interfaces	1. Access the common user view, privileged user view, global configuration view, filter configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, interface group configuration view, or batch interface configuration view. 2. Run the s**how filter-list interface** command.
View the global ACL configuration	1. Access the common user view, privileged user view, global configuration view, filter configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, interface group configuration view, or batch interface configuration view. 2. Run the **show filter-list global** command.
View statistical table information and configuration	1. Access the privileged user view, global configuration view, common user view, interface group configuration view, and interface configuration view. 2. Run the following commands: ● **show counter config** ● **show counter** *counter-id* ● **show counter**

10.3.8 Configuration Example

10.3.8.1 Example of Configuring an L2 ACL

Network Requirements

The switch Switch works as a gateway and connects to user PCs. It is required to configure an ACL to reject packets with source MAC address 0001-0203-0405 and destination MAC address 0102-0304-0506, as shown in Figure 10-1.

Network Diagram

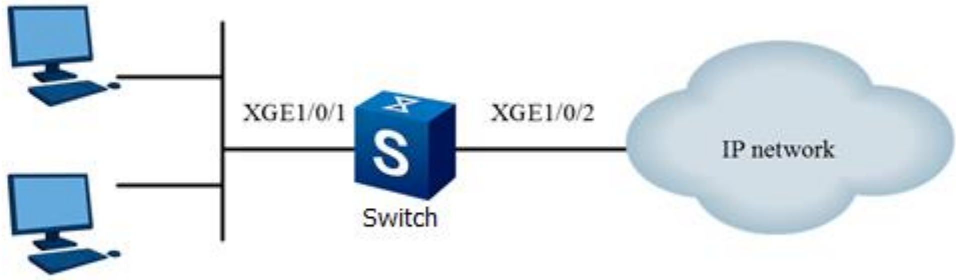


Figure 10-1L2 ACL network diagram

Configuration

1. Create an L2 ACL.
Switch#configure
Switch(config)#filter-list 1
Switch(configure-filter-l2-1)#

2. Configure an L2 ACL rule.
Switch(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 01:02:03:04:05:06/48
3. Configure an L2 ACL action.
Switch(configure-filter-l2-1)#filter 1 action deny
4. Bind the ACL with an interface.
Switch(configure-filter-l2-1)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#filter-list-l2 in 1

10.3.8.2 Example of Configuring an L3 ACL

Network Requirements

Different departments of the corporate network are interconnected via the switch. It is required to configure an IPv4 ACL to prevent the R&D department from accessing the salary query server (IP address: 10.164.9.9) during work time (08:30 to 17:30) and to allow the CEO office to access the salary query server at any time without restriction, as shown in Figure 10-2.

Network Diagram

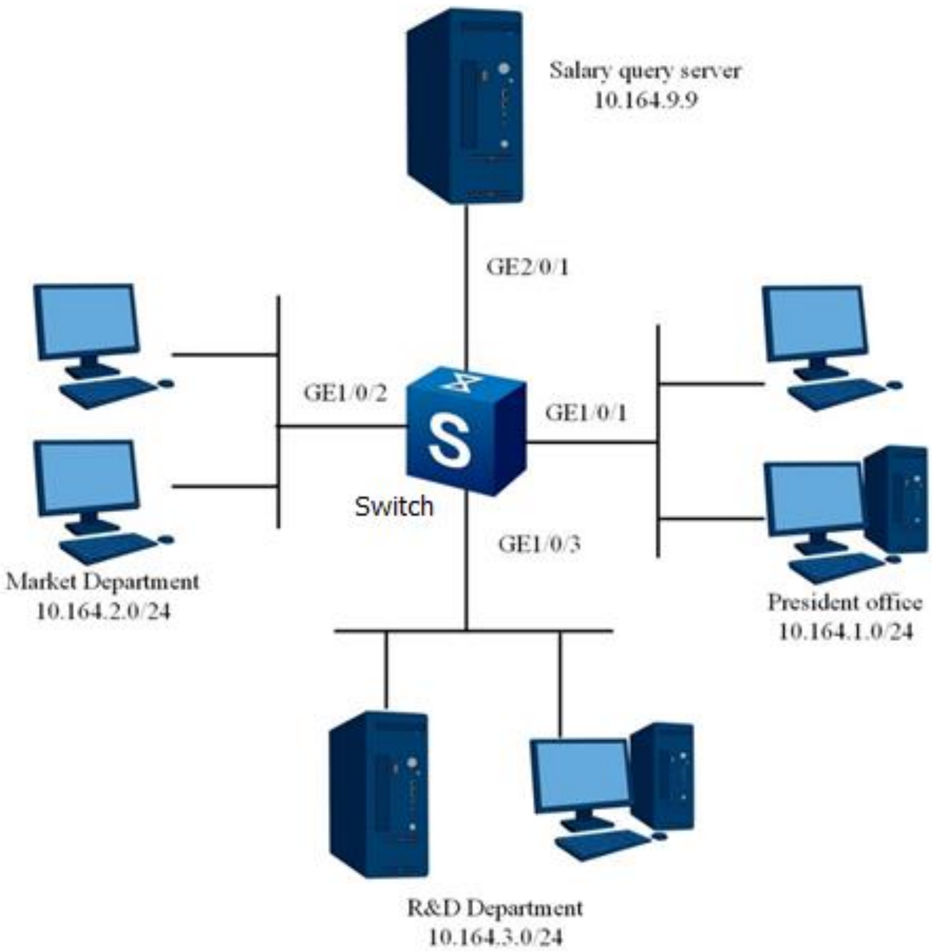


Figure 10-2L3 ACL network diagram

Configuration

1. Configure the time-range.

```
Switch#configure
Switch(config)#time-range list 1
Switch(config-timerange1)#time-range 1 everyweekday 8:30:00 AM to 5:30:00 PM
Switch(config-timerange1)#quit
```

2. Configure an ACL to allow the CEO office to access the salary query server.

```
Switch(config)# filter-list 1001
Switch(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32
Switch(configure-filter-ipv4-1001)#filter 1 action permit
Switch(configure-filter-ipv4-1001)#quit
```

3. Configure an ACL to prevent the marketing department from accessing the salary query server during the designated period of time.

```
Switch(config)#filter-list 1002
Switch(configure-filter-ipv4-1002)#filter 1 ip 10.164.2.0/24 10.164.9.9/32
Switch(configure-filter-ipv4-1002)#filter 1 time-range 1
Switch(configure-filter-ipv4-1002)#filter 1 action deny
Switch(configure-filter-ipv4-1002)#quit
```

4. Configure an ACL to prevent the R&D department from accessing the salary query server during the designated period of time.

```
Switch(configure)# filter-list 1003
Switch(configure-filter-ipv4-1003)#filter 1 ip 10.164.3.0/24 10.164.9.9/32
Switch(configure-filter-ipv4-1003)#filter 1 time-range 1
Switch(configure-filter-ipv4-1003)#filter 1 action deny
Switch(configure-filter-ipv4-1003)#quit
```

5. Apply the ACLs to the interface.

```
Switch(config)#interface xgigaethernet 1/0/1
Switch(config-10ge1/0/1)#filter-list-ipv4 in 1001
Switch(config-10ge1/0/1)#quit
Switch(config)#interface xgigaethernet 1/0/2
Switch(config-10ge1/0/2)#filter-list-ipv4 in 1002
Switch(config-10ge1/0/2)#quit
Switch(config)#interface xgigaethernet 1/0/3
Switch(config-10ge1/0/3)#filter-list-ipv4 in 1003
```

10.3.8.3 Example of Configuring a Mixed ACL

Network Requirements

The switch Switch works as a gateway and connects to user PCs. It is required to configure an ACL to send packets with source MAC addresses in the 00:01:02:00:00:00/24 network segment and source IP addresses in the 1:2:3:1/24 network segment to the CPU, as shown in Figure 10-3.

Network Diagram

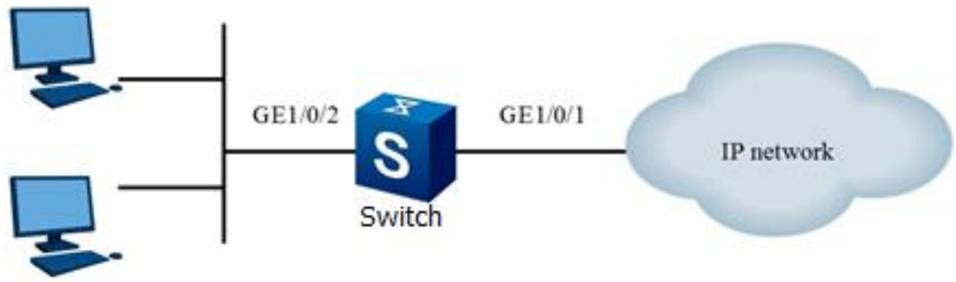


Figure 10-3 Mixed ACL network diagram

Configuration

1. Create a mixed ACL.

Switch#configure

Switch(config)#filter-list 2001

Switch(configure-filter-hybrid-2001)#

2. Configure an L2 ACL rule.

Switch(configure-filter-hybrid-2001)#filter 1 mac 00:01:02:00:00:00/24 any eth-type any provider any any customer any any ip 1.2.3.1/24 any proto-type any

3. Configure an L2 ACL action.

Switch(configure-filter-hybrid-2001)#filter 1 action cpu

4. Bind the ACL with an interface.

Switch(configure-filter-hybrid-2001)#quit

Switch(config)#interface xgigaethernet 1/0/2

Switch(config-10ge1/0/2)#filter-list-hybrid in 2001

10.3.8.4 Example of Configuring a Rate Limiting Template

Network Requirements

The switch Switch works as a gateway and connects to user PCs. It is required to configure an ACL to limit the rate of packets with source MAC address 0001-0203-0405 received by interface GE1/0/2 of the switch Switch, and change the DSCP value of yellow packets to AF11, as shown in Figure 10-4.

Network Diagram

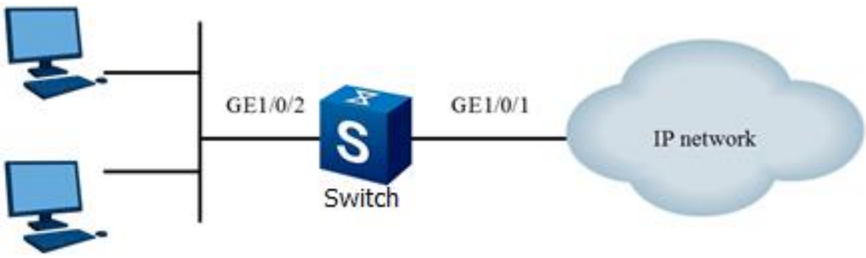


Figure 10-4 Network diagram of rate limiting template

Configuration

1. Configure a rate limiting template.
Switch#configure
Switch(config)#meter 1 cir 64 cbs 10000 pbs 10000 pir 64

2. Create an ACL.
Switch(config)#filter-list 1
Switch(configure-filter-l2-1)#

3. Configure an ACL rule.
Switch(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 any

4. Bind the rate limiting template with the ACL.
Switch(configure-filter-l2-1)#filter 1 meter 1

5. Configure an ACL action.
Switch(configure-filter-l2-1)#filter 1 outaction yellow remark-dscp af11

6. Bind the ACL with the interface.
Switch(configure-filter-l2-1)#quit
Switch(config)#interface xgigaethernet 1/0/2
Switch(config-10ge1/0/2)#filter-list-l2 in 1

10.3.8.5 Example of Configuring a Counter Template

Network Requirements

The switch Switch works as a gateway and connects to user PCs. It is required to configure an ACL to count the number of packets with source IP addresses in the 10.1.1.1/24 network segment that are received by interface GE1/0/2 of the switch Switch, as shown in Figure 10-5.

Network Diagram

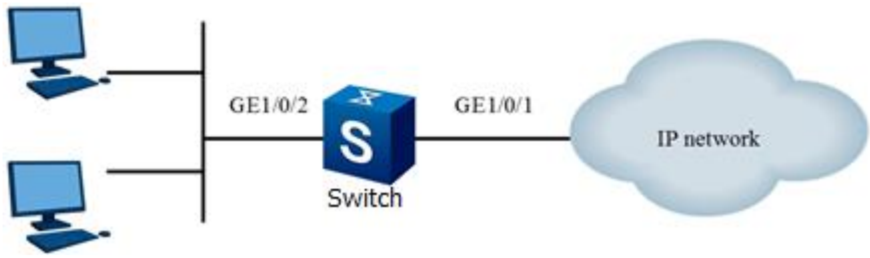


Figure 10-5 Network diagram of counter template

Configuration

1. Configure a counter template.
Switch#configure
Switch(config)# counter 1 packet sort total

2. Create an ACL.
Switch(config)#filter-list 1001
Switch(configure-filter-ipv4-1001)#

3. Configure an ACL rule.
Switch(configure-filter-ipv4-1001)#filter 1 ip 10.1.1.1/24 any

4. Bind the counter template with the ACL.
Switch(configure-filter-ipv4-1001)#filter 1 action counter 1

5. Bind the ACL with an interface.
Switch(configure-filter-ipv4-1001)#quit
Switch(config)#interface xgigaethernet 1/0/2
Switch(config-10ge1/0/2)#filter-list-ipv4 in 1001

10.4 Configuring CPU Defense

10.4.1 CPU Defense Overview

This module implements CPU defense in following ways:

1. Whitelist

A whitelist is a collection of legitimate users or high-priority users. You can define an ACL to configure a whitelist and packets matching the characteristics of the whitelist will be processed first. This can actively protect existing services and protect high-priority user services. You can add authorized users or high-priority users using the device normally to a whitelist.

2. Blacklist

A blacklist is a collection of unauthorized users. You can define an ACL to configure a blacklist and packets matching the characteristics of the blacklist will be discarded. You can add unauthorized users who are determined as attackers to a blacklist.

3. User-defined stream

User-defined steam refers to user-defined anti-attack ACL rules. When a network suffers from unknown attacks, you can use the user-defined stream to indicate the characteristics of attack stream data and restrict uploading of data streams meeting the characteristics.

After a user-defined stream is bound to an ACL rule, when the network suffers from unknown attacks, you can run the **car** and **deny** commands to limit the uploading rate of or discard data streams meeting these characteristics. The **car** command is equivalent to a whitelist. The **deny** command is equivalent to a blacklist.

4. CAR

CAR is used to limit the uploading rate of packets sent to CPU. You can set Committed Information Rate (CIR) and Committed Burst Size (CBS) for each type of packet. You can set different CAR rules for different packets to reduce mutual influence between packets and protect the CPU. CAR can also limit the overall uploading rate of packets sent to the CPU. When the overall uploading rate exceeds the threshold, packets are discarded to avoid CPU overload.

10.4.2 Configuring CPU Defense

Purpose

The application scenario of anti-attack policies varies with the product. For integrated devices, the anti-attack policies can only be applied globally. For distributed devices, the anti-attack policies and applied globally or applied on slots.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Bind a CPU defense policy	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **cpu-defend-policy** *policy-name* command. 3. Run the **cpu-defend bind-policy** *policy-name* command.
Delete a bound CPU defense policy	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **cpu-defend-policy** *policy-name* **or no cpu-defend-policy** command.
Configure an overall uploading rate for packets sent to the CPU	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **cpu-defend policy** *policy-name* command. 3. Run the **car packet-type total cir** { *cir-value* | **default** } **cbs** { *cir-value* | **default** } command.
Configure the CIR and CBS for protocol packets	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the following commands: ● **car packet-type { telnet | ftp | snmp } cir {** *cir* | **default }** ● **car packet-type { telnet | snmp | bpdutunnel | fib6hit | fibhit | icmp | ssh | tcp | total } cir {** *cir* | **default } cbs {** *cbs* | **default }**
Delete the CIR and CBS settings of protocol packets	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view.

Purpose	Procedure
	2. Run the **no car packet-type { telnet | ftp | snmp | bpdutunnel | fib6hit | fibhit | icmp | ssh | tcp | total }** command.
Configure the description of a CPU defense policy	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **description** *descr* command.
Cancel the description settings of a CPU defense policy	1. Run the corresponding command to access the global configuration view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **no description** command.

10.4.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the CPU defense function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable CPU defense debugging	1. Remain in the current privileged user view. 2. Run the **debug cpu-defend { autodefend | carpkt | device | error | event | sync | timer | trap }** command.
Disable CPU defense debugging	1. Remain in the current privileged user view. 2. Run the **no debug cpu-defend** command.
Display the CPU defense configuration	1. Run the corresponding command to access the global configuration view, privileged user view, common user view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the **show cpu-defend config** command.
Display information about all CPU defense policies or a specified CPU defense policy	1. Run the corresponding command to access the global configuration view, privileged user view, common user view, VLANIF configuration view, interface configuration view, interface group configuration view, or VLAN configuration view. 2. Run the following commands: ● **show cpu-defend policy** ● **show cpu-defend policy** *policy-name*

10.5 Configuring Anti-Attack

10.5.1 Configuring a Rate Threshold

Purpose

This section describes how to configure the rate threshold for various protocol types. **iptoself** refers to protocol packets of the switch and **ipforward** refers to forwarded packets.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a rate threshold	1. Run the **configure** command. 2. Run the command **antiattack pkt-limit { arp-request | arp-reply | stp | icmp | igmp | dhcp | udp | tcp | sgm | other | ip-to-self | ip-forward | ospf | bgp | rip }** *limit-value*.

10.5.2 Enabling the ARP Anti-attack Sub-switch

Purpose

This section describes how to enable the ARP anti-attack sub-switch.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the function of checking whether packets match the ARP table	1. Run the **configure** command. 2. Run the command **arp-antiattack { src-ip | src-mac | arp-cheat | gateway-cheat | gratuitous-arp } { enable | disable }.**
Enable or disable the function of checking whether ARP packets match the binding table on the interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-antiattack check user-bind { enable | disable }** command.

Purpose	Procedure
Configure the item of checking whether ARP packets match the binding table	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the following commands: ● **arp-antiattack check user-bind check-item { ip-address | mac-address | vlan }** ● **arp-antiattack check user-bind check-item ip-address vlan** ● **arp-antiattack check user-bind check-item mac-address vlan** ● **arp-antiattack check user-bind check-item ip-address mac-address**
Restore the ARP packet check item to the default value	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-antiattack check user-bind check-item ip-address mac-address** command.
Enable or disable ARP aging unicast detection	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp detect-mode unicast { enable | disable }** command.
Configure the maximum number of ARP mapping entries that an interface can learn	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-limit vlan** *vlan-id* **maxnum** *maxnum command.*
Cancel the upper limit of ARP mapping entries configured for an interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **no arp-limit vlan** *vlan-id* command.
Enable or disable packet limiting	1. Run the corresponding command to access the global configuration view. 2. Run the **antiattack pkt-limit { enable | disable }** command.
Enable or disable the DoS anti-attack limit function	1. Run the corresponding command to access the global configuration view. 2. Run the **antiattack dos-limit { abnormal | fragment | tcp-syn | udp-flood | icmp-flood } { enable | disable }** command.
Configure the committed access	1. Run the corresponding command to access the global configuration view.

Purpose	Procedure
rate and committed information rate of DoS anti-attack limit to the specified packet	2. Run the **antiattack dos-limit { fragment | tcp-syn | icmp-flood } car cir { value | default }** command.

10.5.3 Configuring ARP Interface Anti-attack Parameters

Purpose

This section describes how to configure ARP interface anti-attack parameters.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the function of checking whether ARP packets match the binding table on an interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-antiattack check user-bind { enable | disable }** command.
Enable or disable the function of checking whether ARP packets match the binding table on an interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-antiattack check user-bind { enable | disable }** command.
Restore the ARP packet check item to the default value	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **no arp-antiattack check user-bind check-item** command.
Enable or disable ARP aging unicast detection	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp detect-mode unicast { enable | disable }** command.

Purpose	Procedure
Configure the maximum number of ARP mapping entries that an interface can learn	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **arp-limit vlan** *vlan-id* **maxnum** *maxnum* command.
Cancel the upper limit of ARP mapping entries configured for an interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **no arp-limit vlan** *vlan-id* command.
Configure the limit on a specified packet	1. Run the corresponding command to access the global configuration view. 2. Run the **antiattack pkt-limit** *packet-type max-num* command.

10.5.4 Anti-attack Module Debugging

Purpose

This section describes how to display or hide the debugging information of the anti-attack module.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display the debugging information of the anti-attack module	1. Access the common user view or privileged user view. 2. Run the **debug arp-antiattack** command.
Hide the debugging information of the anti-attack module	1. Access the common user view or privileged user view. 2. Run the **no debug arp-antiattack** command.
Clear the counter of packets dropped to binding table mismatch on an interface	1. Run the corresponding command to access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **reset arp-antiattack statistic check user-bind** command.
Enable DoS anti-attack debugging	1. Access the privileged user view. 2. Run the **debug dos-antiattack { all | config | dev | info }** command.

Purpose	Procedure
Disable DoS anti-attack debugging	1. Access the privileged user view. 2. Run the **no debug dos-antiattack { all | config | dev | info }** command.
Reset the DoS anti-attack limit statistics	1. Access the common user view. 2. Run the **reset antiattack dos-limit statistics** command.
Display configuration of the DoS anti-attack module	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or VLAN configuration view. 2. Run the following commands: ● **show antiattack dos-limit config** ● **show antiattack dos-limit statistic**
Display the check items for ARP packet check against the binding table	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or VLAN configuration view. 2. Run the **show arp-antiattack check user-bind** command.
Display the ARP anti-attack configuration	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show arp-antiattack config** command.
Display the ARP anti-attack statistics	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show arp-antiattack statistic** command.

10.5.5 Viewing the ARP Anti-attack Configuration

Purpose

This section describes how to check the ARP anti-attack configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View the ARP anti-attack configuration	1. Run the corresponding command to access the common user view, privileged user view, global configuration view, interface configuration view, VLANIF configuration view (Ethernet or Trunk interface), or interface group configuration view.

Purpose	Procedure
	2. Run the **show arp-antiattack config** command.
Display the check items for ARP packet check against the binding table	1. Run the corresponding command to access the common user view, privileged user view, global configuration view, interface configuration view, VLANIF configuration view (Ethernet or Trunk interface), or interface group configuration view. 2. Run the **show arp-antiattack check user-bind** command.
Display the ARP anti-attack statistics	1. Run the corresponding command to access the common user view, privileged user view, global configuration view, interface configuration view, VLANIF configuration view (Ethernet or Trunk interface), or interface group configuration view. 2. Run the **show arp-antiattack statistic** command.

10.6 Configuring IP Source Guard

10.6.1 Introduction to IP Source Guard

10.6.1.1 Technical Background

Common methods used to steal IP addresses include:

1. Static modification of IP addresses

   IP address configuration is required to implement TCP/IP. IP address theft occurs if the IP address used for configuring or modifying TCP/IP is not authorized. No restriction is imposed on static modification of the host IP address because the IP address is a logical address.

2. Modification of IP address and MAC address in pair. Many organizations use the IP-MAC address binding technique to prevent static modification of IP addresses. However, this technique is useless if IP address thieves modify IP address and MAC address in pair. The MAC addresses of some compatible network adapters can be modified using the configuration program of the network adapter. A host can access the network by changing its IP address and MAC address to those of an authorized host.

   Software can be used to modify the MAC address of a network adapter that otherwise cannot be modified directly. That is, the underlying network software is modified for the purpose of upper-layer network spoofing.

3. Dynamic modification of IP addresses. A type of attack program is developed for IP address spoofing by bypassing upper-layer network software and dynamically modifying its IP address (or IP-MAC address pair) when receiving/sending packets.

IP source guard (IPSG) is an L2 interface feature that provides a checking mechanism to ensure that the packet received by an interface can also be received by all other interfaces. If checking is passed, the packet is authorized; if checking is not passed, policy violation occurs. IPSG avoids IP address hijack for terminal devices in L2 networks and prevents unauthorized devices from accessing the network by self-designation of IP addresses, which may cause network crash.

After IPSG is configured, only DHCP packets are allowed to pass when the link is up. The DHCP binding table is updated after the DHCP server is assigned an IP address. Then IPSG automatically loads a port-based ACL to the interface. The preceding process is intended to limit the traffic of the client to the source IP address configured in the binding table. The traffic of host ports from other source IP addresses than the bound source IP address is filtered to prevent a host from seizing the IP address of a neighboring host for network attack.

IPSG is a port traffic filter technique based on IP/MAC address for preventing IP address spoofing in LAN. The switch has an IP source binding table used as the standard for checking the packet received by each port. The switch forwards data only in two conditions: a. The received IP packet satisfies the port/IP/MAC address mapping defined in the IP source binding table; b. The received packet is a DHCP packet. In other cases, the switch discards received packets. The IP source binding table can be configured manually on the switch in static mode, or can be learned automatically by the switch via DHCP snooping. Static configuration is simple and fixed with low flexibility. Therefore, you are advised to use IPSG in conjunction with DHCP snooping so that the IP source binding table can be generated from the DHCP snooping binding database.

10.6.1.2 Basic Concepts

IPSG

IPSG is equivalent to adding an ACL to a port to filter all IP packets (except DHCP packets) that users send from the port. After a user applies for an IP address via DHCP interaction, a filter entry is added to the port to allow the user to use the IP address for IP packet communication, while communication of other users is still disabled.

DHCP snooping

DHCP snooping is implemented on the DHCP packets exchanged between client and server to monitor users. With proper configuration, DHCP snooping can filter packets to further filter unauthorized servers.

IP Source Binding Table

The IP source binding table can be configured manually on the switch in static mode, or can be learned automatically by the switch via the DHCP snooping binding table. Static configuration is simple and fixed with low flexibility. Therefore, you are advised to use IPSG in conjunction with DHCP snooping so that the IP source binding table can be generated from the DHCP snooping binding table.

ACL

The ACL is an instruction list applied to a router interface to instruct the interface to accept and reject specified packets. Whether a packet is accepted or rejected is determined by a set of conditions such as the source address, destination address, port number, and protocol.

10.6.1.3 Functions

Table 10-1 lists the functions of IPSG.

Table 10-1IPSG functions

SN	Function	Purpose
1	Filter based on the source IP address and port number	IP traffic is filtered based on the source IP address and port number. Only traffic that matches the binding entry is allowed to pass. The IP source address filter changes when an IP source binding entry is created, modified, or deleted on the port. After the IP source binding entry is changed, the ACL is modified and then re-applied to the port to reflect the change. If IPSG is enabled on a port without the IP source binding entry, by default, the ACL instructs the port to reject all IP traffic except DHCP traffic.
2	Filter based on the source IP address, port number, and MAC address	Same as above
3	Filter based on the source IP address, port number, and VLAN	Same as above
4	Filter based on the source IP address, port number, MAC address, and VLAN	Same as above

10.6.1.4 System Features

IPSG has the following system features:

- Filters IP traffic based on a set of conditions including the source IP address, port number, MAC address, and VLAN.
- Works independently or in conjunction with DHCP snooping.
- Takes precedence over DHCP snooping in terms of configuration.
- Shares the upper configuration limit with DHCP snooping.
- Provides powerful debugging.

10.6.2 Viewing the IPSG Configuration

Purpose

This section describes how to view the IPSG configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View all binding entries	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show user-bind** command.
View the configuration of static binding entries	1. Enter the common user view or Privileged User View. 2. Run the **show user-bind config** command.
Display information of the IP packet checking function	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **show ip source check user-bind** command.

10.6.3 Configuring Check Items

Purpose

This section describes how to view the IPSG check items.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable the IP packet checking function on an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **ip source check user-bind enable** command.
Disable the IP packet checking function on an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **ip source check user-bind disable** command.
Configure the IP packet check items	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **ip source check user-bind enable** command to enable the IP packet checking function on an interface 3. Run the following commands: ● **ip source check user-bind check-item { ip-address | mac-address | vlan }** ● **ip source check user-bind check-item ip-address mac-address** ● **ip source check user-bind check-item ip-address vlan** ● **ip source check user-bind check-item mac-address vlan**
Restore the IP packet check items to default values	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **no ip source check user-bind check-item** command.
Clear the IPSG statistics	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **ip source check user-bind enable** command to enable the IP packet checking function on an interface 3. Run the **reset ip source statistic check user-bind** command.

Purpose	Procedure
Enable or disable the IP packet checking alarm function	1. Access the global configuration view. 2. Run the **user-bind alarm untrust-user { enable | disable }** command.
Configure an IP packet checking alarm threshold	1. Access the global configuration view. 2. Run the **user-bind alarm untrust-user threshold {** *threshold* | **default }** command.
Enable or disable the IP packet blacklist feature	1. Access the global configuration view. 2. Run the u**ser-bind black-list { enable | disable }** command.

10.6.4 Configuring a Static Binding Entry

Purpose

This section describes how to configure a static binding entry for IPSG.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a static binding entry	1. Access the global configuration view. 2. Run the following commands: ● **user-bind static ip {** *ipv4-address* **| any } mac {** *src-mac-address* **| any } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **vlan { any |** *vlan-id* } ● **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* }
Delete a static binding entry	1. Access the global configuration view. 2. Run the following commands: ● **no user-bind static ip {** *ipv4-address* **| any } mac {** *src-mac-address* **| any } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **vlan { any |** *vlan-id* **}** ● **no user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **vlan** { **any** | *vlan-id* } ● **no user-bind static all**

Purpose	Procedure
	● **no user-bind static interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet | eth-trunk }** *interface-number* ● **no user-bind static ip** *ipv4-address* ● **no user-bind static mac** *src-mac-address* ● **no user-bind static vlan** *vlan-id*

10.7 Configuring AAA/Radius

10.7.1 AAA Overview

AAA is short for Authentication, Authorization and Accounting. It implements unified management for configuration of three types of security functions. AAA configuration is the management for network security, which mainly means access control. For example, you can check

- What users can access the network server.
- What services are available for the users with access authority.
- How to charge the users who are using network resources.

Generally, AAA uses the client/server structure. The client runs on the network access server (NAS) and the server mainly manages user information. NAS is the server end for users and is the client end for the server. Figure10-6 shows the basic network structure of AAA.

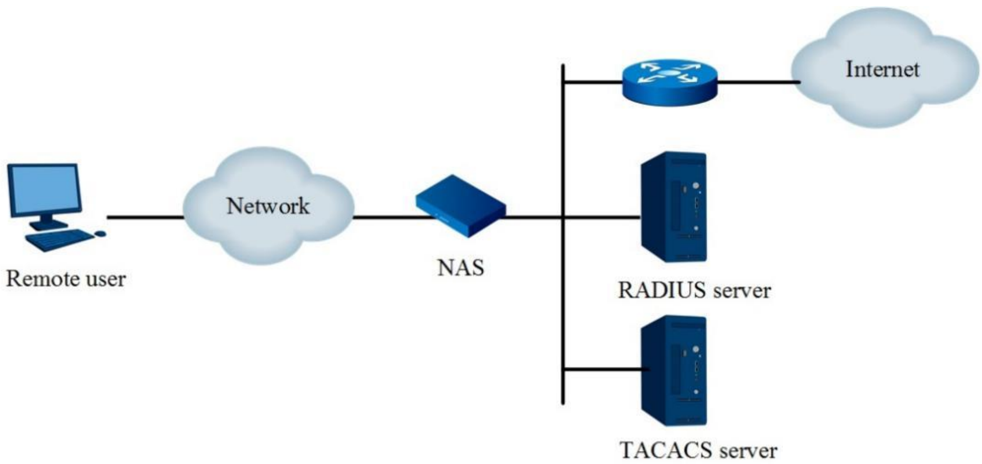


Figure10-6 AAA basic network architecture

Authentication Function

AAA supports the following authentication modes:

- No authentication: Trusts users and skips the validity checking. This mode is generally not used.
- Local authentication: Configures user information (including the username, password, and attributes of local users) on the device. Local authentication is quick and lowers the operation cost, but information storage is limited by the hardware condition.
- Remote authentication: Supports remote authentication through RADIUS or Terminal Access Controller Access Control System (TACACS). The device acts as the client and communicates with the RADIUS or TACACS server. For the RADIUS protocol, the standard or extended RADIUS protocol can be used to perform authentication in conjunction with a system such as iTELLIN or CAMS.

Accounting Function

AAA supports the following accounting modes:

- **None**: Users are not charged.
- **Local** accounting: Supports limiting and management of local user connections. This mode collects statistics on the number of accessing users without the actual fee statistics function. The local access quantity management is only available for local accounting, but not available for local authentication and authorization.
- Remote accounting: Supports remote accounting using the RADIUS server or TACACS server.

Generally, AAA uses the client/server structure. The client runs at the managed resource side and the server mainly stores user information. Therefore, AAA is highly scalable and can perform centralized management of user information easily. AAA can be implemented via various protocols. Currently AAA is based on the RADIUS or TACACS protocol.

Authorization Function

AAA supports the following authorization modes:

- Direct authorization: Trusts users and authorizes users directly. The user authority is the default authority of the system.
- Local authorization: Authorizes users according to the relevant attributes configured for the local user account on the device.
- TACACS authorization: The TACACS server authorizes users.
- RADIUS authorization: RADIUS authorization is a special process. RADIUS authentication and authorization are completed in one process. RADIUS encapsulates the authorization information in the RADIUS authentication response packet for transmission when RADIUS authentication is completed.

10.7.2 Accessing the AAA Configuration View

Purpose

This section describes how to access the AAA configuration view.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Access the AAA configuration view	1. Access the global configuration view. 2. Run the **aaa** command.

10.7.3 Configuring an AAA Authentication Method

Purpose

This section describes how to create an AAA authentication method.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an AAA authentication method	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname* ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname* **{ local | none }** ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname* **local none** ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname groupname* ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname groupname* **{ local | none }** ● **aaa authentication { dot1x | login | enable } method** ***name*** **server-group** *groupname groupname* **local none**
Configure a local AAA authentication method name	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **aaa authentication { dot1x | login | enable } method** *name* **local** command.
Configure an authentication port for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **radius-server** *name* **auth-port** { *auth-port* | **default** } command.
Delete an existing AAA method server group	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* **server-group** *group-name* command.
Delete an existing AAA method	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* command.

10.7.4 Configuring an AAA Authorization Method

Purpose

This section describes how to create an AAA authorization method.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create an AAA authorization method	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **aaa authorization method *name* server-group** *groupname* ● **aaa authorization method *name* server-group** *groupname* **{ local | none }** ● **aaa authorization method *name* server-group** *groupname groupname* ● **aaa authorization method *name* server-group** *groupname groupname* **{ local | none }**
Delete an existing AAA method server group	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* **server-group** *group-name* command.
Delete an existing AAA method	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* command.
Enable the console to use the AAA authorization method	1. Access the global configuration view. 2. Run the **aaa authorization console** command.
Disable the AAA authorization method on the console	1. Access the global configuration view. 2. Run the **no aaa authorization console** command.

10.7.5 Configuring an AAA Accounting Method

Purpose

This section describes how to create an AAA accounting method.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the remote AAA authentication parameters	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **aaa accouting { dot1x | login } method** *name* **server-group** *group-name* ● **aaa accouting { dot1x | login } method** *name* **server-group** *group-name* **{ local | none }** ● **aaa accouting { dot1x | login } method** *name* **server-group** *group-name group-name* ● **aaa accouting { dot1x | login } method** *name* **server-group** *group-name group-name* **{ local | none }** ● **aaa accouting { dot1x | login } method** *name* **server-group** *group-name* **local none**
Configure an accounting port for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **radius-server** *name* **acc-port** { *acc-port* | **default** } command.
Configure a real-time accounting failure time for an AAA server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **accouting realtime** { *realtime* | **default** } command.
Delete an existing AAA method server group	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* **server-group** *groupname* command.
Delete an existing AAA method	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no aaa method** *name* command.

10.7.6 Creating and Deleting a Server Group

Purpose

This section describes how to create and delete a server group.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a server group, set the group protocol type, and add servers	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **server-group** *name* **radius-server** *servername* ● **server-group** *name* **tacacs-server** *servername*
Remove a server from a server group	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **no server-group** *name* **radius-server** *servername* ● **no server-group** *name* **tacacs-server** *servername*
Delete a server group	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no server-group** *name* command.

10.7.7 Configuring a RADIUS Server

Purpose

This section describes how to configure a RADIUS server.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **radius-server** *name* **ip-address** *ipv4-address* **key** *key* command.

Purpose	Procedure
Create a RADIUS server based on IPv4 addresses	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the command **radius-server** *name* **ip-address** *ipv4-address* **key** *key* **auth-port** { *auth-port* | **default** } **acc-port** { *acc-port* | **default** }.
Configure the dead time for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● r**adius-server deadtime {** *deadtime* **| default }** ● **radius-server** *name* **deadtime {** *deadtime* **| default }**
Configure the number of retransmissions for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **radius-server max-retransmit {** *max-retransmit* **| default }** ● **radius-server** *name* **max-retransmit {** *max-retransmit* **| default }**
Configure the retransmission interval for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **radius-server retransmit-interval {** *retransmit-interval* **| default }** ● **radius-server** *name* **retransmit-interval {** *retransmit-interval* **| default }**
Configure the srcip (IPv4) for an AAA RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **radius-server** *name* **src-ip** *ip-address* command.
Delete the srcip (IPv4) of a designated AAA RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no radius-server** *name* **src-ip** command.
Configure an authentication port for a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **radius-server** *name* **auth-port** { *auth-port* | **default** } command.
Delete a RADIUS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no radius-server** *name* command.

10.7.8 Configuring a TACACS Server

Purpose

This section describes how to configure a TACACS server.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Create a TACACS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **tacacs-server** *name* **ip-address** *ip-address* **key** *key* command.
Create a TACACS server based on IPv4 addresses	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **tacacs-server** *name* **ip-address** *ip-address* **key** *key* **port { *port-num*** | **default } single-connection { enable | disable }** command.
Configure the timeout time for a TACACS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: ● **tacacs-server deadtime {** *deadtime* **| default }** ● **tacacs-server** *name* **deadtime {** *deadtime* **| default }**
Configure a global dead time for a TACACS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the following commands: **tacacs-server deadtime {** *deadtime* **| default }** **tacacs-server** *name* **deadtime {** *deadtime* **| default }**
Configure the TACACS server port	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **tacacs-server** *name* **port** { *port-number* | **default** } command.
Configure the single-connection function for a TACACS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **tacacs-server** *name* **single-connection { enable | disable }** command.
Configure the source IP address of	1. Access the global configuration view. 2. Access the AAA configuration view.

a request packet sent to a TACACS server	3. Run the following commands: ● **tacacs-server** *name* **src-ip** *ip-address* ● **no tacacs-server** *name* **src-ip**
Delete a TACACS server	1. Access the global configuration view. 2. Access the AAA configuration view. 3. Run the **no tacacs-server** *name* command.

10.7.9 Configuring an AAA Terminal

Purpose

This section describes how to configure an AAA terminal.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the AAA authentication type for Telnet or console login on the terminal	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the following commands: ● **login authentication aaa method** *name* **auth-type { pap | chap | ascii }** ● **login authentication local**
Configure a login authorization method on the terminal	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the **login authorization aaa method** *name* command.
Delete the configured login authorization method on the terminal	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the **no login authorization aaa method** command.
Configure secondary authentication for user terminals	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the following commands: ● **enable authentication { local | none }** ● **enable authentication aaa method** *name*
Configure the AAA authentication method used for password	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the **command authorization** *level-value* **aaa method** *name* command.

Purpose	Procedure
check at a specified privilege level	
Configure authorization for commands in the global configuration view	1. Access the global configuration view. 2. Access the line configuration view. 3. Run the command **authorization config-command** command.
Configure a password of the local secondary authentication level	1. Access the line configuration view. 2. Run the following commands: ● **enable password level** *level-value* **{ cipher | plain }** *password* ● **enable password { cipher | plain }** *password*
Delete the password of the local secondary authentication level	1. Access the line configuration view. 2. Run the following commands: ● **no enable password level** *level-value* ● **no enable password**
Increase or decrease the permission of a user	1. Access the privileged user view or common user view. 2. Run the **enable | disable** [*level-value*] command.

10.7.10 Displaying the AAA Configuration

Purpose

This section describes how to display the AAA configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the remote user configuration	1. Access the common user view, privileged user view, global configuration view, AAA configuration view, interface configuration view (Ethernet or Trunk), or interface group configuration view. 2. Run the **show aaa** command.
Display global configuration	1. Access the privileged user view, global configuration view, or AAA configuration view. 2. Run the **show aaa config** command.

Purpose	Procedure
Display the AAA method information	1. Access the privileged user view, global configuration view, or AAA configuration view. 2. Run the following commands: ● **show aaa method** ● **show aaa method** *name*
Display the AAA server name	1. Access the common user view, privileged user view, global configuration view, or AAA configuration view. 2. Run the following commands: ● **show aaa server** ● **show aaa server** *name*
Display the AAA server group information	1. Access the privileged user view, global configuration view, or AAA configuration view. 2. Run the following commands: ● **show aaa server-group** ● **show aaa server-group** *group-name*
Display all client information	1. Access the common user view, privileged user view, global configuration view, or AAA configuration view. 2. Run the **show radius client** command.
Display the TACACS server statistics	1. Access the privileged user view, global configuration view, or AAA configuration view. 2. Run the following commands: ● **show aaa tacacs-server** *name* **statistic** ● **show aaa tacacs-server statistic**

10.7.11 Debugging AAA

Purpose

This section describes how to enable or disable the AAA debugging function.

Procedure

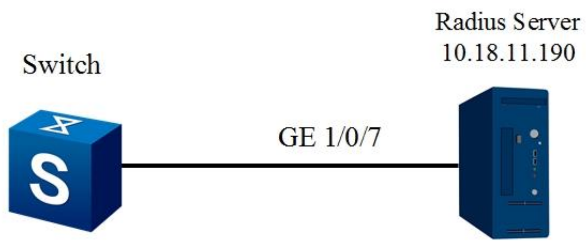
Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable AAA debugging	1. Access the privileged user view. 2. Run the following commands: ● **debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }** ● **no debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }**

10.7.12 Configuration Example

10.7.12.1 LOGIN AAA RADIUS Authentication

Network Diagram



Configuration

LOGIN authentication is used for AAA authentication when users log in to the device through a serial port. The configuration steps are as follows:

Access the AAA configuration node, configure a RADIUS server, and create an AAA server group and AAA method.

Switch(config-aaa)#radius-server server1 ip-address 10.18.11.190 key wri

Switch(config-aaa)#server-group grp1 radius-server server1

Switch(config-aaa)#aaa authentication login method radius server-group grp1

After configuring AAA, configure LOGIN AAA on the terminal.

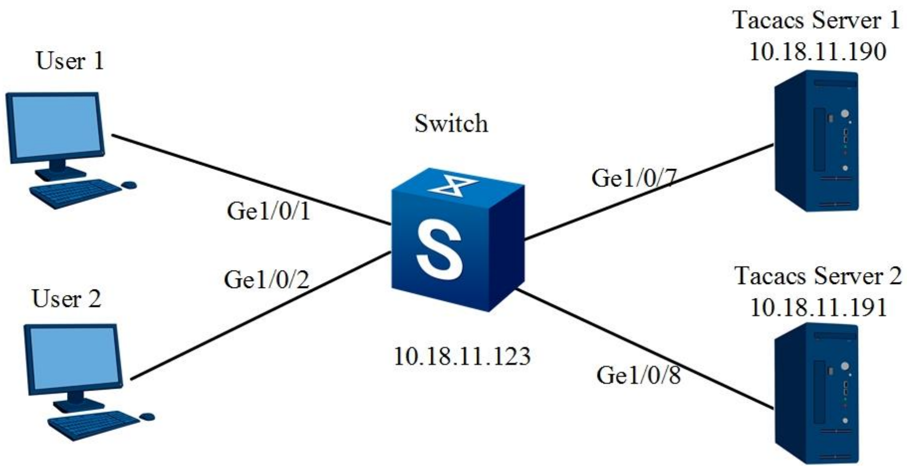
Switch(config)#line console 1

Switch(config-line)#login authentication aaa method me auth-type chap

10.7.12.2 DOT1X AAA TACACS Authentication

Network Diagram

The network diagram of authentication based on DOT1x and AAA is shown below. User 1 and User 2 connect to Dot1x-enabled interfaces GE1/0/1 and GE1/0/2 of the switch. TACACS Server 1 connects to the devices through interface GE1/0/7 and the IP address is 10.18.11.190. TACACS Server 2 connects to devices through interface GE1/0/8 and the IP address is 10.18.11.191. The IP address of the two devices is 10.18.11.123 and the two devices share the key **wri**. Dot1x uses the TACACS servers for authentication.



Configuration

Access the AAA configuration node, configure a RADIUS server, and create an AAA server group and AAA method.

Switch(config-aaa)#tacacs-server server1 ip-address 10.18.11.190 key wri
Switch(config-aaa)#tacacs-server server2 ip-address 10.18.11.191 key wri
Switch(config-aaa)#server-group grp1 tacacs-server server1
Switch(config-aaa)#server-group grp1 tacacs-server server2
Switch(config-aaa)#aaa authentication dot1x method dot1x_auth server-group grp1 local

After configuring AAA, configure Dot1x.

Switch(config)#dot1x start
Switch(config)#dot1x interface aaa enable
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-ge1/0/1)#dot1x enable
Switch(config-ge1/0/1)#dot1x aaa-authentication dot1x_auth
Switch(config-ge1/0/1)#

Configure GE1/0/2 in the same way as GE1/0/1. Then, User 1 and User 2 can be logged in through the 802.1x terminal. The above configuration ensures that authentication can be performed on TACACS Server 2 when TACACS Server 1 fails. If both TACACS servers fail, local authentication is used.

10.8 Configuring 802.1x

10.8.1 802.1x Overview

Based on traditional Ethernet devices, the port-based network access control technology uses the IEEE 802.1x protocol to authenticate and authorize users based on Ethernet interface point-to-point connection. Therefore, Ethernet devices can meet the requirements of Telecom carriers, and play an important role in broadband MAN construction.

The 802.1x protocol is an access control and authentication protocol based on the client/server architecture. It restricts the access of unauthorized users and devices to LAN/MAN via the access port. Users and devices connected to switch ports must pass 802.1x authentication before accessing the services provided by switches or LANs. Before users and devices are authenticated, 802.1x only permits the Extensible Authentication Protocol Over LAN (EAPoL) data to pass through the port of the switch connected to the device; after users and devices are authenticated, normal data can pass through the Ethernet port.

The basic principle of the port-based network access technology is that the network system can control the Ethernet port oriented toward terminal users, only allowing the users permitted and authorized by the system to access various services in the system (such as Ethernet connection, network layer routing, and Internet access).

The core of the network access technology is port access entity (PAE). During the access control process, the PAE includes three aspects:

- Authenticator: the port that authenticates the connected user or device.
- Requester: the authenticated user or device.
- Authentication server: the device that actually authenticates the user or device requesting to access network resources.

Each physical port of the Ethernet is divided into two logical ports (controllable and uncontrollable). Each frame received by the physical port is sent to the controllable and uncontrollable ports. Access to the controllable port is limited by the authorization status of the port. The PAE controls the authorized/unauthorized state of the controllable port according to the authentication result of the authentication server. The unauthorized controllable port denies the access of users and devices.

10.8.2 Configuring 802.1x Authorization

10.8.2.1 Enabling or Disabling 802.1x Globally

Purpose

This section describes how to enable or disable the 802.1x protocol globally.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable 802.1x globally	1. Access the global configuration view. 2. Run the **dot1x start** command. 3. Run the **dot1x interface aaa enable** command to enable Dot1x for AAA authentication.
Disable 802.1x globally	1. Access the global configuration view. 2. Run the **dot1x stop** command.

10.8.2.2 Enabling or Disabling 802.1x on an Interface

Purpose

This section describes how to enable or disable the 802.1x protocol on an interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable 802.1x on an interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **dot1x enable** command.
Disable 802.1x on an interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **dot1x disable** command.

10.8.2.3 Configuring 802.1x Parameters

Purpose

This section describes how to configure 802.1x parameter on an interface or globally.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
(Optional) Set the maximum number of accessing users supported by an interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **dot1x authentication max-user {** *max-use* | **default }** command.
(Optional) Set the quiet period after authentication failure	1. Access the global configuration view. 2. Run the corresponding command to access the interface configuration view or interface group configuration view. 3. Run the **dot1x authentication quiet-period** { *quiet-period* | **default** } command.
(Optional) Set the interval between successful authentication and the next authentication	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **dot1x authentication reauthenticate-period** { *reauthenticate-period* | **default** } command.
(Optional) Enable or disable re-authentication	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **dot1x reauthenticate { enable | disable }** command.
Set the working mode for an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **dot1x link-mode** { **passive** | **active** } command.
Bind an AAA authentication method name to an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet) or interface group configuration view. 3. Run the **dot1x aaa- authentication** *authname* command.
Unbind an AAA authentication method name from an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **no dot1x aaa-authentication** command.

Purpose	Procedure
Set an authentication method for 802.1x users	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication auth-method { eap | chap | pap }** command.
Set the timeout duration for the response from a supplicant (802.1x client) after the authenticator (Switch) sends a Request/MD5-Challenge packet to the supplicant	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication client-timeout** { *client-timeout* | **default** } command.
Set the logical port generation mode	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication logical-port { port-mac | port }** command.
Configure the maximum times for the device to repeatedly send authentication request frames to accessing users	1. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **dot1x authentication max-request** { *max-request* | **default** } command.
Set the maximum number of 802.1x users allowed by an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication max-user {** ***max-use*** **| default }** command.
Set the timeout duration for the authentication server	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication server-timeout {** *server-timeout* | **default }** command.
Set the interval between two Request/Identity packets that the device sends to the client in the case of response timeout	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x authentication tx-period** { *tx-period* | **default** } command.
Configure a guest VLAN on an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **dot1x guest vlan** *vlan-id* command.

Purpose	Procedure
Delete the configured guest VLAN from an interface	1. Access the interface configuration view (Ethernet) or interface group configuration view. 2. Run the **no dot1x guest vlan** command.
Configure the VLAN allocation mode used by the device interfaces during 802.1x authentication	1. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **dot1x vlan-assginment-mode { integer | string }** command.
Bind an AAA authentication method name globally	1. Access the global configuration view. 2. Run the **dot1x default aaa-authentication** *auth-name* command.
Unbind an AAA authentication method name globally	1. Access the global configuration view. 2. Run the **no dot1x default aaa-authentication** command.
Configure a global default client type	1. Access the global configuration view. 2. Run the **dot1x default supplicant-support { normal | sep }** command.
Configure the VLAN allocation mode used by the device during 802.1x authentication globally	1. Access the global configuration view. 2. Run the **dot1x default vlan-assginment-mode { integer | string }** command.
Enable or disable AAA method name binding to interfaces	1. Access the global configuration view. 2. Run the **dot1x interface aaa { enable | disable }** command.
Configure a global default client type	1. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **dot1x supplicant-support { normal | sep }** command.

10.8.2.4 Deleting 802.1x Users

Purpose

This section describes how to delete all the 802.1x users or the local user accounts.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Delete all the 802.1x users or the local user accounts	1. Access the global configuration view. 2. Run the following commands: ● **no dot1x authentication user all** ● **no dot1x interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **user all**
Unbind the default AAA authentication method name	1. Access the global configuration view. 2. Run the **no dot1x default aaa-authentication** command.

10.8.2.5 Viewing the 802.1x Configuration

Purpose

This section describes how to check the 802.1x configuration.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display interface user information	1. Access the common user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **show dot1x authentication user** command.
Display the interface configuration	1. Access the common user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the following commands: ● **show dot1x interface** ● **show dot1x interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
View the Dot1x configuration	1. Access the common user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **show dot1x config** command.
View the user interface statistics of Dot1x	1. Access the common user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **show dot1x statistic** command.
Display statistics on an interface	1. Access the common user view, global configuration view, interface configuration view (Ethernet), or interface group configuration view.

Purpose	Procedure
	2. Run the command **show dot1x statistic { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.

10.9 Configuring Storm Suppression

10.9.1 Configuring Storm Suppression Logging/Trap Function

Purpose

Configure the storm suppression logging and trap function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable storm suppression logging	1. Run the **configure** command to access the global configuration view. 2. Run the **storm-suppression log { enable | disable }** command.
Enable or disable the storm suppression trap function	1. Run the **configure** command to access the global configuration view. 2. Run the **storm-suppression trap { enable | disable }** command.

10.9.2 Configuring a Storm Suppression Threshold and Percentage

Purpose

This section describes how to configure a storm suppression threshold and percentage.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the maximum and minimum rates in percentage of storm suppression.	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the command **storm-suppression { multicast | broadcast | dlf } min-rate percent** *percent* **max-rate percent** *percent*.

10.9.3 Configuring a Storm Suppression Detection Interval and Action

Purpose

This section describes how to configure a storm suppression detection interval and action.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a detection interval for storm suppression	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **storm-suppression interval {** *interval* | **default }** command.
Configure a storm suppression action	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **storm-suppression action { block | error-down | none }** command.

10.9.4 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the storm suppression function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View the storm suppression information on an Ethernet interface	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, or remain in the current privileged user view. 2. Run the command **show storm-suppression interface or show storm-suppression interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
View the storm suppression configuration	1. Run the **disable** command to return to the common user view, run the **configure** command to access the global configuration view, or remain in the current privileged user view. 2. Run the **show storm-suppression config** command.

Chapter 11 Configuring Reliability

This chapter describes the basic content, configuration procedure, and configuration examples of the reliability management of the Switch.

11.1 Configuring MSTP

11.1.1 Overview of STP

Origin of STP

In the L2 switched network, a loop can cause proliferation and infinite loop of packets within the loop network, which results in broadcast storms, occupies all effective bandwidth, and makes the network unavailable.

The Spanning Tree Protocol (STP) is defined in IEEE Std 802.1D published in 1998 by the IEEE to address these issues.

Working Principle of STP

Firstly, the root bridge is selected. The election basis is the bridge ID assembled by bridge priority and bridge MAC. The bridge with the smallest bridge ID will become the root bridge in the network. All ports of the root bridge are connected with the downstream Bridge. Its port becomes the designated port. Next, the downstream bridge connected to the root bridge chooses "the most robust" branch as the path to the root bridge and the corresponding port becomes the root port. This process keeps cycling till reaching the network edge. After the designated port and the root port are confirmed, a tree is generated. After a period of time (30s by default), STP is stable. The designated port and the root port are in forwarding state and other ports are in blocking state. STP BPDUs are periodically sent from the designated port of each bridge to maintain the link status. If the network topology changes, STP is calculated again and the port status changes. This is the basic theory of STP.

Disadvantage of STP

With the development of network technology and further application, the disadvantage of STP has been exposed in applications. The defect of STP is mainly reflected in the convergence rate.

When the topology changes, the new configuration message spreads across the network after a period of time. This delay is called forward delay, which is 15s by default. Before all bridges receive this changing message, there may be a temporary loop if the port in forwarding state in the old topology does not stop transmitting data in the new topology. In order to solve the temporary loop problem, STP uses a timer policy that adds an intermediate state where the port only learns MAC addresses but does not participate in forwarding when the port changes from the blocking state to the forwarding state. The time to switch between two states is the same as the forward delay. This prevents temporary loop when the topology changes. However, this seemingly effective solution results in a convergence time of at least two times the forward delay. For some real-time services (such as voice and video), this convergence time is not acceptable.

11.1.2 Overview of RSTP

Advantages of RSTP

To solve the defect of slow convergence of STP, IEEE defined a Rapid Spanning Tree Protocol (RSTP) based on the IEEE 802.1w standard in 2001. There are three important improvements in RSTP based on STP. It speeds up convergence (the fastest convergence rate can be less than 1s).

- The root port and designated port are configured with two roles for quick switching purposes: alternate port and backup port. When the root port fails, the alternate port quickly switches to the new root port and enters the forwarding state without delay. When the designated port fails, the backup port quickly switches to the new designated port and enters the forwarding state without delay.
- In the point-to-point link only connecting two switch interfaces, the designated port performs handshake only once with the downstream bridge before entering the forwarding state without delay. If three or more bridges are connected by a shared link, the downstream bridge does not respond to the handshake request sent by the designated port of the upstream bridge but it waits for a period two times the forward delay before entering the forwarding state.
- The port that directly connects to a terminal but does not connect to other bridges is an edge port. The edge port can directly enter the forwarding state without delay. Because the bridge cannot know whether the port directly connects to the terminal, the port must be configured manually.

Disadvantages of RSTP

RSTP is improved in many ways compared with STP and is backward compatible with STP. RSTP is applicable to hybrid networks. However, both RSTP and STP belong to Single Spanning Tree (SST). RSTP has disadvantages in the following three aspects:

- Because the entire network has only one spanning tree, the convergence time is long when the network size is large.
- Because RSTP is a type of SST, all VLANs share one tree. Every VLAN in the network must be continuously distributed along the tree path for normal intra-VLAN communication. Otherwise, some VLANs are separated due to internal link blockage, causing a failure of intra-VLAN communication.
- When a link is blocked, it does not carry any traffic and load balancing fails, causing enormous waste of bandwidth.

The Multiple Spanning Tree Protocol (MSTP) with support for VLAN is designed to address these defects of SST.

11.1.3 Overview of MSTP

Advantages of MSTP

Multiple Spanning Algorithm and Protocol (MSTP) is a new spanning tree protocol defined in IEEE 802.1s issued in 2002. Compared with STP and RSTP, MSTP has the following outstanding features:

- MSTP introduces the concept of "domain" to divide one switched network into several domains. There are multiple spanning trees in every domain. These spanning trees are independent of each other. Among these domains, MSTP uses Common and Internal Spanning Tree (CIST) to ensure a loop-free network topology.
- MSTP introduces the concept of "instance" to map multiple VLANs to one instance, which lowers communication costs and reduces the resource occupancy rate. Each instance topology calculation of MSTP is independent (each instance corresponds to a single spanning tree). In these instances, load balancing of VLAN data can be achieved.
- MSTP can implement a rapid migration mechanism of port status similar to that of RSTP.
- MSTP is compatible with STP and RSTP.

MSTP Algorithm

1. Initial state

Each port of each device generates a configuration message that makes it the root bridge at the initial time. The common root and domain root constitute its bridge ID. The external root path cost and internal root path cost are 0. The designated bridge ID is the local bridge ID. The designated port is the local port. The port receiving BPDU packets is Port 0.

2. Port role selection principle

Table 11-1 describes the selection principle of the port role.

Table 11-1 Selection principle of the port role

Port Role	Selection Principle
Root port	The port priority vector takes precedence over the designated priority vector of the port, and the root priority vector of the device derives from the root path priority vector of the port.
Designated port	The designated priority vector of port takes precedence over the port priority vector.
Master port	The domain boundary root port takes the master role in the MSTI instance.
Alternate port	The port priority vector takes precedence over the designated priority vector of the port. However, the root priority vector of the device does not derive from the root path priority vector of the port.
Backup port	The port priority vector takes precedence over the designated priority vector of the port. However, the designated bridge ID in port priority vector is the bridge ID of the local device.

3. Priority vector calculation

The MSTP role of all bridges is computed according to the information carried in the packet. The most important information is the priority vector of the spanning tree. The following describes the CIST priority vector and MSTI priority vector calculation methods.

a) CIST priority vector calculation

In CIST, priority vector is composed of the common root, external root path cost, domain root, internal root path cost, designated bridge ID, designated port ID, and the ID of the port receiving BPDU packets.

The following assumptions are made to facilitate subsequent description:

- In initial condition, the information carried in the packet sent by the PB port of the bridge B includes the common root RB; the external root path cost ERCB; the domain root RRB; the internal root path cost IRCB; the designated bridge ID B; the designated port ID PB; and the ID PB of the port receiving BPDU packet.
- The information carried in the packet that is received by the PB port of the bridge B from the PD port of the bridge D includes the common root RD; the external root path cost ERCD; the domain root RRD; the internal root path cost IRCD; the designated bridge ID D; the designated port ID PD; and the ID PB of the port receiving BPDU packet.
- The priority of the packet received by the PB port of the bridge B from the PD port of the bridge D takes precedence.

Based on the above assumptions, the following describes the calculation method of each priority vector.

(1) Message priority vector

The message priority vector is the priority vector carried in the MSTP packet. The message priority vector received by the PB port of bridge B is {RD : ERCD : RRD : IRCD : D : PD : PB}. If the bridge B and bridge D are not in the same domain, the internal root path cost is meaningless to bridge B and it is set to 0.

(2) Port priority vector

In the initial condition, the port priority vector makes itself the root. The port priority vector of the PB port is {RB : ERCB : RRB : IRCB : B : PB : PB}.

The port priority vector is updated according to the message priority vector received by the port. If the received message priority vector takes precedence over the port priority vector, then the port priority vector is updated to the message priority vector. Otherwise, the port priority vector remains constant. Because the message priority vector received by PB port takes precedence over the port priority vector, the port priority is updated to {RD : ERCD : RRD : IRCD : D : PD : PB}.

(3) Root path priority vector

The root path priority vector is calculated based on the port priority vector.

- If the port priority vector is from the bridge of a different domain, the external root path cost of the root path priority is the sum of the port path cost and the external root path cost of the port priority vector. The domain root of the root path priority vector is the local bridge domain root. The internal root path cost is 0. If the PB port path cost of bridge B is PCPB, the root path priority vector of PB port is {RD : ERCD+ PCPB : B : 0 : D : PD : PB}.
- If the port priority vector is from the bridge of the same domain, the internal path cost of the root path priority vector is the sum of the internal root path cost of the port priority vector and the port path cost. The calculated root path priority vector of the PB port is {RD : ERCD: RRD : IRCD + PCPB : D : PD : PB}.

(4) Bridge priority vector

The common root ID, domain root ID, and designated bridge ID of the bridge priority vector are all the local bridge IDs. The external root path cost and internal root path cost are both 0s. The designated port ID and the receiving port ID are 0s. The bridge priority vector of bridge B is {B : 0 : B : 0 : B : 0 : 0}.

(5) Root priority vector

The root priority vector is the optimal value between the bridge priority vector and the root path priority vector of all the designated bridge IDs different from the local bridge IDs. If the local bridge priority vector is optimal, the local bridge is the CIST common root. If the bridge priority vector of the bridge B is optimal, the root priority vector of the bridge B is {B : 0 : B : 0 : B : 0 : 0}.

(6) Designated priority vector

The designated priority vector of port is calculated based on the root priority vector. The designated bridge ID of the root priority vector is replaced with the local bridge ID and the designated port ID is replaced with its own port ID. The designated priority vector of the PB port of the bridge B is {B : 0 : B : 0 : B : PB : 0}.

b) MSTI priority vector calculation

The calculation rule of each MSTI priority vector is basically the same as the CIST priority vector, only different in the following two aspects:

- There are no common root and external root path cost in the MSTI priority vector. It is only composed of the domain root, internal root path cost, designated bridge ID, designated port ID, and the ID of the port receiving BPDU packets.
- MSTI only processes the message priority vector from the same domain.

4. Role selection process

The following briefly describes the CIST instance calculation process based on the network in Figure 11-1. Assume that the bridge priority of Switch_1 takes precedence over Switch_2, and that of Switch_2 takes precedence over Switch_3; the link path costs are 4, 5, and 10 respectively. Switch_1 and Switch_2 are in the same domain while Switch_3 is in another domain.

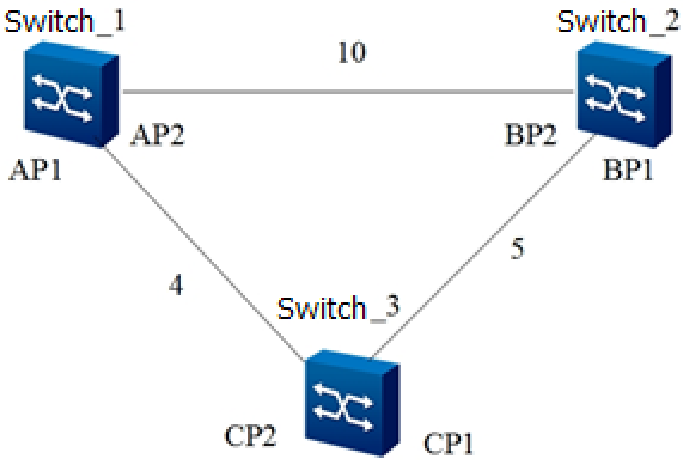


Figure 11-1 Network diagram of MSTP algorithm calculation

The message priority vector carried in the packets sent by the device in the initial state in Figure 11-1 is listed in Table 11-2.

Table 11-2 Initial state of each device

Device	Port	Message Priority Vector
Switch_1	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
Switch_2	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
Switch_3	CP1	{C:0:C:0:C:CP2:0}
	CP2	{C:0:C:0:C:CP2:0}

The port priority vector of all ports of the device is the same as the message priority vector in the initial state.
In the initial state, the port of every device is the designated port and sends the message priority vector announcing its role of the root bridge.

a) Role selection process of Switch_1

The AP1 port and AP2 port of Switch_1 receive packets from Switch_2 and Switch_3 respectively. Switch_1 compares the port priority vector of the AP1 port and AP2 port with the message priority vector from other switches. Because the port priority vector of the AP1 port and AP2 port takes precedence over the message priority vector carried in the packets, the role of the AP1 port and AP2 port remains unchanged and is still the designated port. Switch_1 is the common root as well as the domain root of Switch_1 and Switch_2. After that, the port sends messages announcing its role of the root regularly.

b) Role selection process of Switch_2

After the BP1 port of Switch_2 receives packets from the CP1 port of Switch_3, it compares the message priority vector with the port priority vector. Because the port priority vector takes precedence over the message priority vector, the role of the port is not updated.
After the BP2 port of Switch_2 receives the packets from the AP2 port of Switch_1, BP2 processes the packets as follows:

(1) BP2 compares the message priority vector of the port with the port priority vector. Because the message priority of the port takes precedence over the port priority vector, the port priority vector is updated to the message priority vector {A:0:A:0:A:AP2:BP2}.

(2) BP2 calculates the root path priority vector of the port. Switch_1 and Switch_2 are in the same domain. The port root path priority vector is {A:0:A:10:A:AP2:BP2}.

(3) Calculate the root priority vector of Switch_2. Only the root path priority vector of the BP2 port is from another device. Because the root path priority vector of the BP2 port takes precedence over the bridge priority vector of Switch_2, the root priority vector of Switch_2 is {A:0:A:10:A:AP2:BP2}.

(4) BP2 calculates the designated priority vector. The designated priority vector of the BP1 port is {A:0:A:10:B:BP1:BP2}. The designated priority vector of the BP2 port is {A:0:A:10:B:BP2:BP2}.

BP2 determines the role of the port by comparing the designated priority vector with the port priority vector of the BP1 port and BP2 port. Because the designated priority vector of BP1 takes precedence over the port priority vector, the role of BP1 is the designated port and the BP1 port regularly sends the designated priority vector {A:0:A:10:B:BP1:BP2} that announces Switch_1 as the common root and domain root. Because the port priority vector of BP2 takes precedence over the designated priority vector and the root priority vector is from the root path priority vector of the BP2 port, the role of BP2 is the root port.

c) Role selection process of Switch_3

The CP1 port of Switch_3 receives the message priority vector {B:0:B:0:B:BP1:CP1} of Switch_2 that is not updated. The CP2 port receives the message priority vector {A:0:A:0:A:AP1:CP2} from Switch_1. As a result of comparison, the message priority vectors of CP1 and CP2 take precedence over the port priority vector. Therefore, the port priority vector of CP1 and that of CP2 are updated to {B:0:B:0:B:BP1:CP1} and {A:0:A:0:A:AP1:CP2} respectively. Because Switch_3 is not in the same domain as Switch_1 and Switch_2, the root path priority vector of the CP1 port is {B:5:C:0:B:BP1:CP1} and that of CP2 is {A:4:C:0:A:AP1:CP2}. The root path priority vector of CP2 takes precedence over that of CP1, so the root priority vector is {A:4:C:0:A:AP1:CP2}. The designated priority vectors of CP1 and CP2 are {A:4:C:0:C:CP1:CP2} and {A:4:C:0:C:CP2:CP2} respectively. The CP1 port is calculated to be the designated port and the CP2 port is calculated to be the root port.

The CP1 port of Switch_3 receives the updated message priority vector {A:0:A:10:B:BP1:CP1} from BP1. As a result of comparison, the message priority vector of CP1 takes precedence over its port priority vector. It updates the port priority vector to {A:0:A:10:B:BP1:CP1}. The calculated root path priority vector of the CP1 port is {A:5:C:0:B:BP1:CP1}. Because the message priority vector received by the CP2 port is not changed, according to the above calculation, the root path priority vector of the CP2 port remains to be {A:4:C:0:A:AP1:CP2}. The root path priority vector of CP2 takes precedence over that of CP1, and the root path priority vector is {A:4:C:0:A:AP1:CP2}. The designated priority vectors of CP1 and CP2 port are {A:4:C:0:C:CP1:CP2} and {A:4:C:0:C:CP2:CP2} respectively. The port priority vector of CP1 takes precedence over its designated priority vector, but the root priority vector is not from the root path priority vector of the CP1 port. Therefore, CP1 is the alternate port and CP2 is still the root port.

5. Calculation result

After the roles of the device and ports are determined, the whole tree topology is established. The traffic forwarding path is shown in Figure 11-2 after the above calculation.

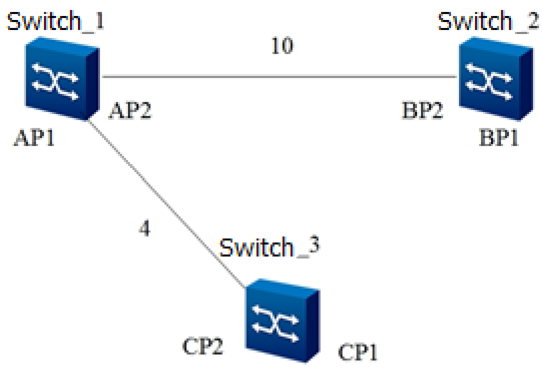


Figure 11-2 Traffic forwarding path after calculation

11.1.4 Configuring a Switch to Join a Designated MST Domain

Background

Two switches belong to the same domain as long as the following configurations of them are the same:

- MST domain name
- MSTI-to-VLAN mapping relationship
- MST domain revision level

Before configuring a switch to join the designated MST domain, configure physical attributes and VLAN features of the port.

Purpose

This section describes how to configure a switch to join the MST domain.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the STP working mode of the switch	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp mode** { **stp** | **rstp** | **mstp** | **default** } command.
Configure an MST domain	1. Access the global configuration view. 2. Access the STP configuration view.

Purpose	Procedure
(You must configure the STP working mode of the switch to MSTP or default first)	3. Run the **stp config-name** *string* command to set an STP domain name. 4. Run the **stp instance** *instance-id* **vlan** *vlan-list* command to configure the applied VLAN of the MSTI. 5. Run the **stp revision-level** { *range* | **default** } command to configure the MSTP revision level.
Enable or disable STP for an interface (You must configure the STP working mode of the switch to MSTP or default first)	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command.
(Optional) Configure the priority of the switch in a designated MSTI	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp instance** *instance-id* **priority** { *priority* | **default** } command.
(Optional) Configure the priority of CIST Instance 0	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp priority** { *priority* | **default** } command.
(Optional) Configure the priority of an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the following commands: ● **stp priority {** *priority* **| default }** ● **stp process** *process-id* **priority {** *priority* **| default }**
(Optional) Configure the management path cost of the current interface in a designated MSTI (MST instance)	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp instance** *instance-id* **path-cost** { *path-cost* | **default** } command.
(Optional) Configure the current interface's priority in a designated MSTI	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp instance** *instance-id* **priority** { *priority* | **default** } command.

11.1.5 Configuring MSTP Parameters

Background

Before modifying MSTP parameters, perform the following tasks:

- Configuring physical attributes of the port
- Configuring the port to join the VLAN
- Configuring the switch to join the designated MST domain

Purpose

This section describes how to change the values of MSTP parameters.

In a specific network environment, you can change the values of MSTP parameters to achieve the optimal result.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the STP forwarding delay	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp forward-delay** { *forward-delay* | **default** } command.
Configure the interval of sending hello packets of the protocol	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp hello-time** { *hello-interval* | **default** } command.
Configure the STP maximum aging time of the switch	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp max-age** { *max-age* | **default** } command.
Configure the maximum hop count of STP in an MST domain	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp max-hop** { *max-hop* | **default** } command.
Enable or disable an edge port	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp edge-port** { **enable** | **disable** } command to enable an interface to be an edge port or disable the settings.

Purpose	Procedure
Enable or disable point-to-point management for an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp point-to-point** { **force-true** | **force-false** | **auto** } command to set the interface link type.
Configure the current interface's priority in a designated MSTI	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp instance** *instance-id* **priority** { *priority* | **default** } command.
Configure the management path cost of the current interface in a designated MSTI (MST instance)	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp instance** *instance-id* **path-cost** { *path-cost* | **default** } command.
Configure the number of times to send packets in a Hello Time interval of STP (that is, the number of BPDUs sent)	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp transmit-limit** { *transmit-limit* | **default** } command.
Configure the management path cost of an interface on Instance 0	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp path-cost {** *cost* | **default } or stp process** *process-id* **path-cost {** *cost* | **default }** command.
Configure the standard to calculate the STP port path cost	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp pathcost-standard { dot1t | dot1d-1998 }** command.

Purpose	Procedure
Configure the current interface to perform the mode check	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp mcheck** command.
Configure an STP migration interval	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp migration-time** { *migration-time* | **default** } command.
Enable or disable the STP trap function	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp trap { enable | disable }** command.
Configure the threshold on the number of TC packets	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp tc-protection threshold** { *threshold-value* | **default** } command.
Delete an STP instance	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **no stp instance** *instance-id* command.
Configure the timeout duration of STP	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp timer-factor** { *timer-value* | **default** } command.
Enable or disable the BPDU filter function	1. Run the **configure** command to access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the stp bpdu-filter { enable | disable } command.
Configure the priority of an interface	1. Run the **configure** command to access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp priority** { *priority* | **default** } command.
Enable or disable the function of STP	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp v-stp { enable | disable }** command.

Purpose	Procedure
entering cross-switch combined work mode	
Clear STP statistics	1. Run the **configure** command to access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 3. Run the **stp** { **enable** | **disable** } command to enable STP. 4. Run the **stp reset statistic** command,
Create an MSTP process and access the view of the created MSTP process	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp process** *process-id* command.
Delete the MSTP process of a specified ID	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **no stp process** *process-id* command.
Configure the maximum hop count of STP in an MST domain	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp max-hops** { *max-hop* | **default** } command.
Enable or disable MAC address refresh for the topology change packets received by a spanning tree	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp flush** { **enable** | **disable** } command.
Enable or disable the edge port feature for all interfaces of the switch	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp edge-default { enable | disable }** command.
Configure the bridge MAC address of the current switch for STP calculation	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp bridge-address** *mac-address* command.
Enable or disable enhanced STP	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp enhance-mode { enable | disable }** command.

11.1.6 Configuring MSTP Protection

Background

- BPDU protection

For access-layer devices, generally, the access port is directly connected to the user terminal (such as PC) or file server. At this time, you can set the access port as the edge port to achieve fast migration of these ports. In normal situations, the edge port does not receive spanning tree configuration messages (BPDU packets). However, if someone forges a configuration message and maliciously attacks the switch, the system automatically sets the edge port as a non-edge port upon receiving the configuration message. This will cause re-calculation of the spanning tree and result in network topology flapping. The BPDU guard function can prevent this problem.

- Loop protection

The status of the root port and other blocked ports is maintained by receiving BPDUs from the upstream switch continuously. When these ports cannot receive BPDUs from the upstream switch because of link congestion or unidirectional link failure, the switch re-selects the root port. The original root port changes to the designated port and the original blocked port migrates to the forwarding state. This leads to a loop in the switched network.

The loop protection function prevents loops. After loop protection is enabled, if the root port cannot receive BPDUs upstream, it is set to the blocked state. The blocked port remains blocked and does not forward messages so that no loop occurs in the network.

- Root protection

The root protection function can be used to prevent unknown BPDUs from changing the network topology.

Due to the incorrect configuration of maintenance engineers or malicious network attacks, the legal root bridge may receive configuration messages with higher priority and thus loses its root bridge role, causing illegal change of the network topology. If the original flow is forwarded over a high-rate link, the illegal change directs the flow from the high-rate link to the low-rate link and causes network congestion. This problem can be avoided by the root protection function.

For ports configured with the root protection function, the port role remains to be designated port. Once such ports receive configuration messages with higher priority, the status of these ports is set to listening and the ports do not forward messages (equivalent to disconnection of the link connected to the port). The port restores to the original state if not receiving configuration messages with higher priority during a long enough period of time.

- TC protection

After receiving TC-BPDU messages, the switch deletes MAC address entries and ARP entries. If somebody forges TC-BPDU packets to attack the switch maliciously, the switch receives a lot of TC-BPDU messages in a short time. Frequent deletion operations cause a great burden on the device and threaten network stability.

After the TC-BPDU message anti-attack function is enabled, the number of times for MSTP to process TC-BPDU packets per unit time can be configured. In a unit time, if the number of TC-BPDU packets received by the MSTP process exceeds the configured threshold, the MSTP process only handles packets for the times specified by the threshold. For other TC-BPDU packets exceeding the threshold, after the timer times out, the MSTP process handles them centrally once. In this way, the TC protection function avoids frequent deletion of MAC address entries and ARP entries in order to protect the switch.

Purpose

This section describes how to configure MSTP protection.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the BPDU protection function of the switch	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp bpdu-guard { enable | disable }** command.
Configure the root protection function of the switch	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp root-guard** { **enable** | **disable** } command.
Configure the TC protection function on the switch	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp tc-protection** { **enable** | **disable** } command to configure the TC protection function of the switch. 4. Run the **stp tc-hold-off** { *time* | **default** } command to set the topology change delay/suppression time.
Enable or disable TC-BPDU packet protection	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp tc-flush-arp { enable | disable }** command.
Enable or disable TC-BPDU packet protection	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp tc-protection { enable | disable }** command.

Purpose	Procedure
Enable or disable the STP loop protection function for an interface	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp loop-guard { enable | disable }** command.
Enable or disable TC-BPDU packet protection	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp tc-protection { enable | disable }** command.
Include interfaces in status calculation by multiple MSTP processes	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp link-share binding process** *process-list* command.
Add the current interface to the STP process of a specified ID	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **stp binding process** *process-id* command.
Remove the current interface from the STP process of a specified ID	1. Access the global configuration view. 2. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 3. Run the **no stp binding process** *process-list* command.
Enable or disable point-to-point link detection	1. Access the global configuration view. 2. Access the STP configuration view. 3. Run the **stp link-detection { enable | disable }** command.

11.1.7 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the MSTP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the STP configuration of the switch	1. Access the common user view. 2. Run the **show stp** command.

Purpose	Procedure
View the STP configuration file information of the switch	1. Access the common user view. 2. Run the **show stp config** command.
View the STP information of the switch	1. Access the common user view. 2. Run the **show stp information** command.
View the STP instance configuration on all interfaces or a designated interface	1. Access the common user view. 2. Run the **show stp instance** *instance-id* **interface** command to display the STP instance configuration on all interfaces. 3. Run the following commands to view the STP configuration information on a designated interface: ● **show stp instance** *instance-id* **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show stp instance** *instance-id* **interface eth-trunk** *trunk-number*
View the STP configuration of all interfaces	1. Access the common user view. 2. Run the **show stp interface** command.
View the STP configuration of a designated interface	1. Access the common user view. 2. Run the following commands: ● **show stp interface { gigaethernet | ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet}** *interface-number* ● **show stp interface eth-trunk** *trunk-number*
View the STP status information on link-up interfaces and protected interfaces	1. Access the common user view. 2. Run the **show stp brief** command.
View the STP status of the current working interface in STP multi-process mode	1. Access the common user view. 2. Run the **show stp process** *process-id* **brief** command.
View specific information about the current interface in STP multi-process mode	1. Access the common user view. 2. Run the following commands: ● **show stp process** *process-id* **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show stp process** *process-id* **interface eth-trunk** *trunk-number*

Purpose	Procedure
	● **show stp process interface**
View statistics on the TC/TCN packets sent and received on interfaces	1. Access the common user view. 2. Run the **show stp tc-bpdu statistic** command.
View topology change statistics	1. Access the common user view. 2. Run the **show stp topology-change** command.
Enable or disable STP debugging	1. Access the privileged user view. 2. Run the following commands: ● **debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **[instance *mst-instance*]** ● **debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface eth-trunk** *trunk-number* **[instance** *mst-instance*] ● **no debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **[instance** *mst-instance*] ● **no debug stp { error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all } interface eth-trunk** *trunk-number* **[instance** *mst-instance*] ● **no debug stp all**

11.1.8 Configuration Example

Network Requirements

Four switches support MSTP: Switch_1, S780E_2, Switch_3, and Switch_4. Configure the basic MSTP functions as shown in the following network diagram.

- Set Switch_1 and Switch_3 in the same domain named Domain 1 and create Instance 1.
- Set Switch_2 and Switch_4 in another domain named Domain 2 and create Instance 1.
- Switch_1 is the CIST common root.
- In Domain 1, Switch_1 is the domain root of CIST and Instance 1. Configure root protection for interfaces GE1/0/1 and GE1/0/2 of Switch_1.
- In Domain 2, Switch_2 is the domain root of CIST and Switch_4 is the domain root of Instance 1.
- Configure the interface GE1/0/1 of Switch_3 and Switch_4 as the edge port and enable the BPDU protection function.

Network Diagram

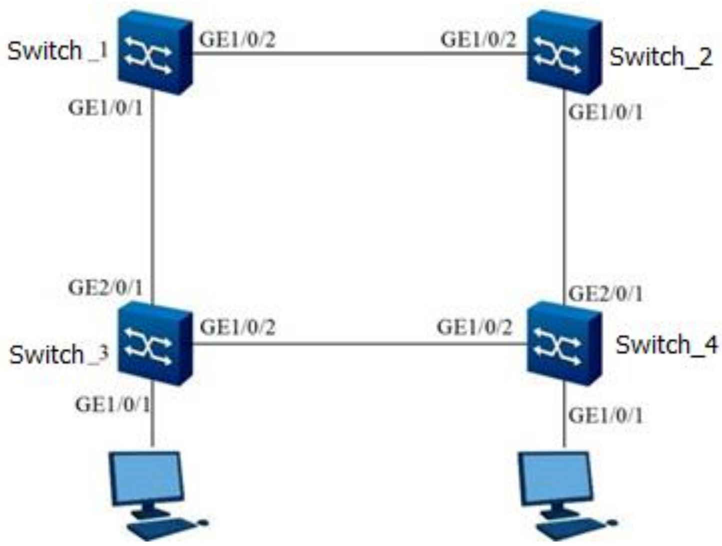


Figure 11-3 MSTP network diagram

Configuration

1. Configure Switch_1.

Add Switch_1 to Domain 1.

```
Switch_1#configure
        %Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Switch_1(config)#stp
Switch_1(config-stp)#stp mode mstp
Switch_1(config-stp)#stp config-name Domain1
Switch_1(config-stp)#stp instance 1 vlan 1-10
Switch_1(config-stp)#stp revision-level 1
```

Configure Switch_1 priority to 0 in Instance 0 to ensure that Switch_1 is the CIST common root.

```
Switch_1(config-stp)#stp priority 0
```

Set Switch_1 priority to 0 in Instance 1 to ensure that Switch_1 is the domain root of Instance 1.

```
Switch_1(config-stp)#stp instance 1 priority 0
```

Create VLAN 2 to VLAN 20 and add interfaces 10GE1/0/1 and 10GE1/0/2 of Switch_1 to VLAN 1 to VLAN 20 respectively. Enable the STP function and root protection function for the interfaces.

```
Switch_1(config)#vlan 2-20
Switch_1(config)#interface 10gigaethernet1/0/1
Switch_1(config-10ge1/0/1)#port link-type trunk
Switch_1(config-10ge1/0/1)#port trunk allow-pass vlan 1-20
Switch_1(config-10ge1/0/1)#stp enable
Switch_1(config-10ge1/0/1)#stp root-guard enable
Switch_1(config-10ge1/0/1)#quit
Switch_1(config)#interface 10gigaethernet1/0/2
Switch_1(config-10ge1/0/2)#port link-type trunk
Switch_1(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
Switch_1(config-10ge1/0/2)#stp enable
Switch_1(config-10ge1/0/2)# stp root-guard enable
Switch_1(config-10ge1/0/2)#quit
Switch_1(config)#
```

2. Configure Switch_2.

Add Switch_2 to Domain 2.

```
Switch_2#configure
        %Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Switch_2(config)#stp
Switch_2(config-stp)#stp mode mstp
Switch_2(config-stp)#stp config-name Domain2
Switch_2(config-stp)#stp instance 1 vlan 1-10
Switch_2(config-stp)#stp revision-level 2
```

Configure Switch_2 priority to 4096 in Instance 0 to ensure that Switch_2 is the CIST common root.

Switch_2(config-stp)#stp priority 4096
Create VLAN 2 to VLAN 20 and add interfaces 10GE1/0/1 and 10GE1/0/2 of Switch_2 to VLAN 1 to VLAN 20 respectively. Enable the STP function and root protection function for the interfaces.
Switch_2(config)#vlan 2-20
Switch_2(config)#interface 10gigaethernet1/0/1
Switch_2(config-10ge1/0/1)#port link-type trunk
Switch_2(config-10ge1/0/1)#port trunk allow-pass vlan 1-20
Switch_2(config-10ge1/0/1)#stp enable
Switch_2(config-10ge1/0/1)#stp root-guard enable
Switch_2(config-10ge1/0/1)#quit
Switch_2(config)#interface 10gigaethernet1/0/2
Switch_2(config-10ge1/0/2)#port link-type trunk
Switch_2(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
Switch_2(config-10ge1/0/2)#stp enable
Switch_2(config-10ge1/0/2)#stp root-guard enable
Switch_2(config-10ge1/0/2)#quit
Switch_2(config)#
3. Configure Switch_3.
Add Switch_3 to Domain 1.
Switch_3#configure
%Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Switch_3(config)#stp
Switch_3(config-stp)#stp mode mstp
Switch_3(config-stp)#stp config-name Domain1
Switch_3(config-stp)#stp instance 1 vlan 1-10
Switch_3(config-stp)#stp revision-level 1
Enable the BPDU protection function.
Switch_3(config-stp)#stp bpdu-gurad enable
Create VLAN 2 to VLAN 20 and add interfaces 10GE1/0/2 and 10GE2/0/1 of Switch_3 to VLAN 1 to VLAN 20 respectively. Enable the STP function for the interfaces and configure interface GE1/0/1 as the edge port.
Switch_3(config)#vlan 2-20
Switch_3(config)#interface 10gigaethernet2/0/1
Switch_3(config-10ge2/0/1)#port link-type trunk
Switch_3(config-10ge2/0/1)#port trunk allow-pass vlan 1-20
Switch_3(config-10ge2/0/1)#stp enable
Switch_3(config-ge2/0/1)#quit
Switch_3(config)#interface 10gigaethernet1/0/2
Switch_3(config-10ge1/0/2)#port link-type trunk
Switch_3(config-10ge1/0/2)#port trunk allow-pass vlan 1-20

Switch_3(config-10ge1/0/2)#stp enable
Switch_3(config-10ge1/0/2)#quit
Switch_3(config)#interface 10gigaethernet1/0/1
Switch_3(config-10ge1/0/1)#stp enable
Switch_3(config-10ge1/0/1)#stp edged-port enable
Switch_3(config-10ge1/0/1)#port hybrid pvid 20
Switch_3(config-10ge1/0/1)#port hybrid vlan 20 untagged
Switch_3(config-10ge1/0/1)#quit
Switch_3(config)#

4. Configure Switch_4.

Add Switch_4 to Domain 2.

Switch_4#configure
%Enter configuration commands. End with Ctrl+Z or command "quit" & "end"
Switch_4(config)#stp
Switch_4(config-stp)#stp mode mstp
Switch_4(config-stp)#stp config-name Domain2
Switch_4(config-stp)#stp instance 1 vlan 1-10
Switch_4(config-stp)#stp revision-level 2

Set Switch_4 priority to 0 in Instance 1 to ensure that Switch_4 is the domain root of Instance 1.

Switch_4(config-stp)#stp instance 1 priority 0

Enable the BPDU protection function.

Switch_4(config-stp)#stp bpdu-gurad enable

Create VLAN 2 to VLAN 20 and add interfaces 10GE1/0/2 and 10GE2/0/1 of Switch_4 to VLAN 1 to VLAN 20 respectively. Enable the STP function for the interfaces and configure interface GE1/0/1 as the edge port.

Switch_4(config)#vlan 2-20
Switch_4(config)#interface 10gigaethernet2/0/1
Switch_4(config-10ge2/0/1)#port link-type trunk
Switch_4(config-10ge2/0/1)#port trunk allow-pass vlan 1-20
Switch_4(config-10ge2/0/1)#stp enable
Switch_4(config-10ge2/0/1)#quit
Switch_4(config)#interface 10gigaethernet1/0/2
Switch_4(config-10ge1/0/2)#port link-type trunk
Switch_4(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
Switch_4(config-10ge1/0/2)#stp enable
Switch_4(config-10ge1/0/2)#quit
Switch_4(config)#interface 10gigaethernet1/0/1
Switch_4(config-10ge1/0/1)#stp enable
Switch_4(config-10ge1/0/1)#stp edged-port enable
Switch_4(config-10ge1/0/1)#port hybrid pvid 10
Switch_4(config-10ge1/0/1)#port hybrid vlan 10 untagged
Switch_4(config-10ge1/0/1)#quit
Switch_4(config)#

11.2 Configuring BFD

11.2.1 Overview of BFD

Basic Concept

Bidirectional Forwarding Detection (BFD) is a set of unified detection mechanisms that are used for detecting communication failures between forwarding devices in the network. BFD provides light-burden and short-time detection of communication failures between neighboring forwarding devices, and also provides real time detection to any media and protocol layer.

BFD Features Supported by Switch

- Multi-hop Detection

  Multi-hop detection detects the IP connectivity of any path between two non-directly connected devices. It is generally used for checking whether there is a reachable route between two devices.

- BFD for VRRP

  BFD is used to detect and monitor the link condition or IP route forwarding condition in the network. After VRRP is bound to a BFD session, BFD announces the session status and triggers VRRP fast switching and processing.

- BFD for OSPF

  After OSPF is bound to a BFD session, BFD announces the session status and OSPF is responsible for processing.

- BFD for IS-IS

  After IS-IS is bound to a BFD session, BFD announces the session status and IS-IS is responsible for processing.

- BFD for BGP

  After BGP is bound to a BFD session, BFD announces the session status and BGP is responsible for processing.

- Dynamic Change of BFD Parameter Values

  After a BFD session is set up, you can still change the values of BFD parameters, such as the expected interval for sending BFD packets, minimum receiving interval, and local detection multiple. Changing parameter values does not affect the current session status.

Echo Function

BFD detection is classified into asynchronous detection mode and on-demand detection mode. The echo function is an additional function of two detection modes.

When the echo function is enabled, a node sends a series of BFD ECHO packets to a neighbor, and the neighbor reflects the packets to the transmit node. If no response ECHO packet is received within a period of time (or a large amount of ECHO packets are lost), the notification session is disabled. When using the echo function, ECHO packets are used for fault detection to decrease the BFD control packet speed (asynchronous mode) or completely stop sending BFD control packets (on-demand mode).

Compared with the echo function, the pure asynchronous mode has an advantage: To reach the same detection duration, the number of BFD control packets used in asynchronous mode is half of that used in the ECHO function. If the echo function cannot be used, the asynchronous mode must be adopted.

The advantage of echo function is that this function detects forwarding path of the neighbor only. This can decrease the round-trip time jitter, shorten the detection, and detect faults that cannot be detected by other methods.

The echo function can be independently enabled in two directions. Precondition for enabling the echo function in a specific direction: The node that implements the echo reflection must indicate the capability of providing the echo function; the node that sends ECHO packets must indicate the will of implementing the echo function.

11.2.2 Configuring BFD

Prerequisite

Before configuring the BFD function, you must configure a VLAN interface and IP address. If you also need to detect connectivity at the network layer, configure a routing protocol.

Background

Currently, Switch does not support the demand mode.

If the BFD function is used independently or with static routing or with VRRP, the **bfd track** command must be configured.

If the BFD function is used with other protocols for dynamic trigger, the **bfd track** command is not required.

When roles are configured, in the initial stage of BFD session setup, the role of both ends (active or passive) is determined by applications, but at least one end takes the active role.

Purpose

This section describes how to configure the BFD function to rapidly detect and monitor the connectivity of IP routing between directly connected devices in the network.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable the BFD function globally	1. Access the global configuration view. 2. Run the **bfd** { **start** | **stop** } command.
Configure a BFD session	1. Access the global configuration view. 2. Run the following commands to add a static BFD session based on IP address: ● **bfd track** *track-number* **subsession link-auto switch** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **vlan** *vlan-id* **one-arm-echo** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **one-arm-echo** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* **one-arm-echo** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*

Purpose	Procedure
	● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* **vlan** *vlan-id* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number.subinterface* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip** *ipv6-address2* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **vlan** *vlan-id* ● **bfd track** track-number **remote-ip6** ipv6-address1
Enable or disable BFD on an interface	1. Access the global configuration view. 2. Access the interface configuration view, VLANIF configuration view, or loopback interface configuration view. 3. Run the **bfd** { **enable** | **disable** } command.

Purpose	Procedure
(Optional) Configure the BFD session status trap function	1. Access the global configuration view. 2. Run the **bfd trap** { **enable** | **disable** } command.
Delete track information from a physical interface	1. Access the global configuration view. 2. Run the following commands: ● **no bfd track all** ● **no bfd track** *track-number* ● **no bfd track** *track-number* **subsession link-auto switch**

11.2.3 Configuring BFD Parameters

Purpose

This section describes how to adjust the expected BFD-packet sending interval, minimum receiving interval, and local detection multiple of the device according to the network status and performance requirements when setting up a BFD session.

Generally, you only need to use the system default settings.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the BFD-packet minimum sending interval, minimum receiving interval, and detection timeout multiple	1. Access the global configuration view. 2. Access the interface configuration view, VLANIF configuration view, or loopback interface configuration view. 3. Run the command **bfd min-tx** *tx-interval* **min-rx** *rx-interval* **multiplier** *timeout-multiple*.
Configure the BFD session minimum sending interval, minimum receiving interval, and detection timeout multiple	1. Access the global configuration view. 2. Access the VLANIF configuration view, loopback interface configuration view, Ethernet bridge interface configuration view, Ethernet routing interface configuration view, or interface configuration view (Trunk). 3. Run the command **bfd track** *track-number* **min-tx** { *tx-interval* | **default** } **min-rx** { *rx-interval* | **default** } **multiplier** *timeout-multiple*.

11.2.4 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the BFD function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View information of a BFD-enabled interface	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, or interface group configuration view. 2. Run the **show bfd interface** command.
View information of a dynamically created BFD session	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, or interface group configuration view. 2. Run the **show bfd session** command.
View information of a static BFD session	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, or interface group configuration view. 2. Run the **show bfd track** *track-number* or **show bfd track** command.
View configuration of a BFD session	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), VLANIF configuration view, or interface group configuration view. 2. Run the **show bfd config** command.

11.2.5 Configuration Example

Caution

When configuring BFD on a VLAN interface, ensure that the two devices can be pinged each other.

11.2.5.1 Applying Multi-hop Detection

Network Requirements

Three switches are connected as shown below. It is required to configure BFD multi-hop detection to detect the multi-hop path between Switch_1 and Switch_3. It is also required to add the interfaces to VLAN, create interface VLANIF, and configure an IP address on it.

Network Diagram

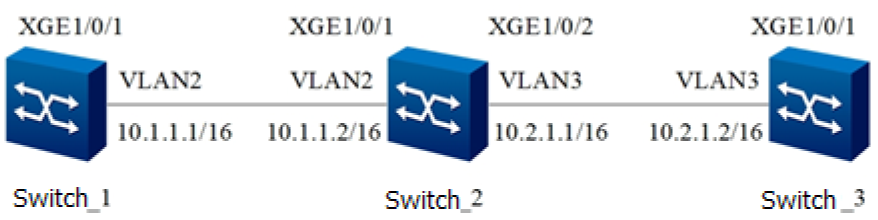


Figure 11-4 BFD multi-hop detection network diagram

Configuration

1. Configure Switch_1.

Add interface xgigaethernet1/0/1 to VLAN 2, and set the IP address to 10.1.1.1/16.

```
Switch_1#configure
Switch_1(config)#interface vlan 2
Switch_1(config-vlan-2)#ip address 10.1.1.1/16
Switch_1(config-vlan-2)#quit
Switch_1(config)#interface xgigaethernet 1/0/1
Switch_1(config-10ge1/0/1)#port hybrid pvid vlan 2
Switch_1(config-10ge1/0/1)#port hybrid vlan 2 untagged
Switch_1(config-10ge1/0/1)#quit
Switch_1(config)#
```

Configure static routing so that the route between Switch_1 and Switch_3 is reachable.

```
Switch_1(config)#ip route-static 10.2.0.0 255.255.0.0 10.1.1.2
```

Configure BFD session parameters at End A (active).

```
Switch_1(config)#bfd start
Switch_1(config)#interface vlan 2
Switch_1(config-vlan-2)#bfd enable
Switch_1(config)#bfd track 1 remote-ip 10.2.1.2 local-ip 10.1.1.1 vlan 2
```

The following are optional configurations.

```
Switch_1(config-vlan-2)#bfd role active
Switch_1(config-vlan-2)#bfd min-tx 300 min-rx 300 multiplier 3
Switch_1(config-vlan-2)#quit
Switch_1(config)#
```

2. Configure Switch_2.
Add interface xgigaethernet1/0/1 to VLAN 2, and set the IP address to 10.1.1.2/16.

```
Switch_2#configure
Switch_2(config)#interface vlan 2
Switch_2(config-vlan-2)#ip address 10.1.1.1/16
Switch_2(config-vlan-2)#quit
Switch_2(config)#interface xgigaethernet 1/0/1
Switch_2(config-10ge1/0/1)#port hybrid pvid vlan 2
Switch_2(config-10ge1/0/1)#port hybrid vlan 2 untagged
Switch_2(config-10ge1/0/1)#quit
Switch_2(config)#
```

Add interface xgigaethernet1/0/2 to VLAN 3, and set the IP address to 10.2.1.1/16.

```
Switch_2(config)#interface vlan 3
Switch_2(config-vlan-3)#ip address 10.2.1.1/16
Switch_2(config-vlan-3)#quit
Switch_2(config)#interface xgigaethernet 1/0/2
Switch_2(config-10ge1/0/2)#port hybrid pvid vlan 3
Switch_2(config-10ge1/0/2)#port hybrid vlan 3 untagged
Switch_2(config-10ge1/0/2)#quit
Switch_2(config)#
```

3. Configure Switch_3.
Add interface xgigaethernet1/0/1 to VLAN 3, and set the IP address to 10.2.1.2/16.

```
Switch_3#configure
Switch_3(config)#interface vlan 3
Switch_3(config-vlan-3)#ip address 10.2.1.2/16
Switch_3(config-vlan-3)#quit
Switch_3(config)#interface xgigaethernet 1/0/1
Switch_3(config-10ge1/0/1)#port hybrid pvid vlan 3
Switch_3(config-10ge1/0/1)#port hybrid vlan 3 untagged
Switch_3(config-10ge1/0/1)#quit
Switch_3(config)#
```

Configure static routing so that the route between Switch_3 and Switch_1 is reachable.

```
Switch_3(config)#ip route-static 10.1.0.0 16 10.2.1.1
```

Configure BFD session parameters at End C (active or passive).

```
Switch_3(config)#bfd start
Switch_3(config)#interface vlan 3
Switch_3(config-vlan-3)#bfd enable
Switch_3(config)#bfd track 1 remote-ip 10.1.1.1 local-ip 10.2.1.2 vlan 3
```

The following are optional configurations.

```
Switch_3(config-vlan-3)#bfd role passive (or active)
Switch_3(config-vlan-3)#bfd min-tx 300 min-rx 300 multiplier 3
Switch_3(config-vlan-2)#quit
Switch_3(config)#
```

11.3 Configuring EFM

11.3.1 Overview of EFM

Usage of EFM

Ethernet in the First Mile (EFM) is a short name of the operations, administration, and maintenance (OAM) part in the IEEE802.3ah protocol. EFM mainly defines the OAM of the subscriber access network and addresses the installation, monitoring, and maintenance of Ethernets and MANs. It can run on any full-duplex point-to-point or simulated point-to-point Ethernet links, but does not support transmission among multiple hops on an Ethernet.

Three Types of Protocol Types Supported by EFM

Switch supports the following three types of EFM packets:

- Information EFM PDU: notifies the remote device of the local EFM information.
- Link Event Notification EFM PDU: notifies the remote device of the poor link performance detected by the EFM instance.
- Remote LoopBack Control EFM PDU: enables or disables the loopback mode on the remote device.

Note:

EFM and Link OAM are common short names of the IEEE 802.3ah protocol.

Ethernet OAM protocol is a type of protocol suite.

11.3.2 Supported EFM Features

Link Discovery

Link discovery refers to the process of establishing a link by the EFM, which is the first period of Ethernet EFM. During the process, the connected Ethernet EFM instances exchange Information PDUs to notify remote devices of their own EFM configuration information and EFM support and capabilities on the local devices. The EFM instance determines whether to establish a connection after receiving the information about the remote device. If both devices are in passive mode, no connection is established. If both devices agree with the EFM information of the other side, the connection is set up successfully and starts to function.

After the EFM connection is set up successfully, the two devices send EFM PDUs to each other at certain intervals to maintain the connection information. If one device fails to receive an EFM PDU from the other side within the link_lost_time period, the connection is considered as failed.

Remote Loopback

An EFM instance can set the remote device to loopback mode by sending a loopback control EFM PDU to the remote device. The loopback mode helps administrators to guarantee link quality in Ethernet installation and inspection at failures. In loopback mode, all received frames, except for EFM PDUs and Pause frames, are sent back from the original port. In the loopback status period, EFM PDUs are sent interactively periodically to maintain the EFM link discovery function.

After receiving the loopback command, the remote EFM instance needs to send an Information EFM PDU containing the loopback status flag configuration to the local device within a time interval; otherwise, the local device considers configuration timeout. Administrators can use it to estimate whether the link satisfies the service needs and to test the latency, jitter, and throughput.

When the interface is in loopback mode, it no longer participates in the operation of L2 and L3 protocols, for example, the STP and OSPF. This is because when both ports are in loopback status, data frames other than EFM PDUs are not sent to the CPU. Non-EFM PDUs are discarded or looped back on the MAC layer.

Caution

Only EFM entities in active mode have permissions to set a remote entity to the loopback mode. If both entities are in active mode and one entity has already sent a loopback command to the other one and yet receives a loopback command from the other entity while it is waiting for response, the MAC addresses of the two entities are compared, and the entity with a greater MAC address enters the loopback status.

Link Monitoring

Link monitoring is used to check and discover faults on the link layer. When a link fault occurs on a local device after the configuration is completed, it sends an Event Notification PDU to the remote device to notify it of the error on the local device and records the error in the error log. Error events include the following four types:

- Incorrect symbol period: Check whether the number of incorrect symbols has exceeded the threshold within the unit time period. According to the IEEE 802.3ah protocol, the check window size is set to the total number of symbols in the unit time period. The error event is equivalent to analyzing the proportion of incorrect symbols among a certain number of symbols.
- Error frame: Check whether the number of error frames among the specified number of frames has exceeded the configured threshold.
- Incorrect frame period: Check whether the number of error frames has exceeded the threshold within the unit time period.
- Error frame second: Check whether the number of error seconds within the specified time period (multiples of seconds) has exceeded the configured threshold.

Link Fault Notification

A link fault notification is a fault message with a special flag bit sent to the remote device when a serious fault occurs on the interface housing the EFM instance. The fault event is also recorded in the log. The remote EFM instance also records the fault event to the log when receiving the fault message.
A remote EFM instance is notified of the following types of faults:

- Link Fault: The receiving side detects signal loss, such as optical signal failure on the remote side. The function is supported only when the link supports independent sending and receiving (one-way transmission). Link fault is not supported for non-one-way transmission at IEEE 802.3ah.
- Dying Gasp: indicates the last moment at a power outage. (The function is not supported in the current version.)
- Critical Event (defined by users): The event types are determined by the manufacturer. At present, Switch supports the following user-defined critical events defined by the IEEE 802.3ah: IEEE 802.3ah disabled on interface (including network management disabling, protocol disabling by force, joining of a physical interface to the convergence interface, and hot swapping) and device hot restart.

11.3.3 Configuring EFM Link Discovery

Background

After the EFM protocol is enabled on an interface, the interface uses the following default settings:

- EFM mode: Active
- Maximum EFM PDU sending rate: 10 EFM PDUs per interval
- Minimum EFM PDU sending interval: 1 second
- EFM discovery timeout time: 5 seconds
- Loopback: unsupported
- Link detection: unsupported

If the EFM mode is configured after EFM discovery is completed, EFM discovery is performed once again. If the interfaces on the two devices are in passive mode, the discover period fails.

Purpose

This section describes how to configure the EFM link discovery function, including enabling and disabling the EFM protocol on an interface and setting the EFM mode on an interface, maximum EFM PDU sending rate, minimum EFM PDU sending interval, EFM discovery timeout duration, and error frame window and threshold.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the EFM protocol on an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm** { **enable** | **disable** } command.
Set the EFM mode on an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm mode** { **active** | **passive** } command.
Set the maximum rate for sending EFM PDUs	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm max-rate** { *rate* | **default** } command.
Set the minimum interval for sending EFM PDUs	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm min-rate** { *rate* | **default** } command.
Set the EFM discovery timeout duration	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm timeout** { *timeout-value* | **default** } command.

Purpose	Procedure
Configure the error frame window and threshold	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame threshold** *threshold-value-rangewindow* **window** { *window-value-range* | **default** }.
Disable error frame detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame** command.
Configure a window and threshold for the error frame detection interval	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame-period threshold** *threshold-value* **window** { *window-value-range* | **default** }.
Disable the error frame period detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame-period** command.
Configure a window and threshold for error frame seconds	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame-seconds threshold** *threshold-value* **window** { *window-value-range* | **default** }.

Purpose	Procedure
Disable error frame second detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame-seconds** command.
Configure the action to be taken upon error occurrence	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor high-threshold action { disable-on-error | trap | all }**.

11.3.4 Configuring EFM Remote Loopback

Background

- To enable remote loopback, you must ensure that the EFM instances on both sides support EFM remote loopback; otherwise, the configuration fails.
- Only EFM instances in active mode can issue remote loopback commands. If an active EFM instance is already in the loopback status, that is, another active EFM instance has set the instance to remote loopback status, starting or stopping remote loopback on the local EFM instance does not take effect. It can only be started or stopped on the remote instance.
- EFM remote loopback supports timeout stopping. This avoids long-time outage of normal forwarding services on the link when the user forgets to stop EFM remote loopback.

Purpose

This section introduces how to configure EFM remote loopback, including starting or stopping loopback and configuring whether to support loopback, loopback response timeout period, and remote loopback duration.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable EFM remote loopback	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm remote-loopback start** command.
Disable EFM remote loopback	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm remote-loopback stop** command.
Configure whether an interface support EFM remote loopback	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm remote-loopback { supported | unsupported }** command.
Set the EFM remote loopback response timeout duration	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm remote-loopback timeout** { *timeout-value* | **default** } command.
Set the EFM remote loopback hold-time	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm remote-loopback start holdtime** { *holdtime-value* | **default** } command.

11.3.5 Configuring EFM Link Monitoring

Purpose

This section introduces how to configure the EFM link monitoring function, including configuring support for link detection and setting the error symbol period window and threshold, error frame window and threshold, error frame period window and threshold, error frame second window and threshold, action (interface linkage) at error occurrence, and latency for automatic restoration to UP on the EFM linkage interface.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure whether to support EFM link detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm link-monitor { supported | unsupported }** command.
Configure a window and threshold for error frames	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame threshold** *threshold value rangewindow* **window** { *window value range* | **default** }.
Disable EFM error frame detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame** command.
Configure a window and threshold for	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the

Purpose	Procedure
the error frame detection interval	**interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame-period threshold** *threshold value rangewindow* **window** { *window value range* | **default** }.
Disable EFM error frame detection interval	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame-period** command.
Configure a window and threshold for error frame seconds	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **efm link-monitor frame-seconds threshold** *threshold value rangewindow* **window** { *window value range* | **default** }.
Disable EFM error frame second detection	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **no efm link-monitor frame-seconds** command.
Configure the action to be taken upon error occurrence	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command e**fm link-monitor high-threshold action { disable-on-error | trap | all }**.
Cancel the action to be taken upon error occurrence	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the

Purpose	Procedure
	interface eth-trunk *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the command **no efm link-monitor high-threshold action { disable-on-error | trap | all }**.
Configure the linkage time of the EFM interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm link-monitor recover-period** { *recover time* | **default** } command.
Cancel the linkage time of the EFM interface (closing the interface permanently)	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm link-monitor never recover** command.

11.3.6 Configuring EFM Link Fault Notification

Purpose

This section introduces how to configure the EFM link fault notification function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure whether an interface supports critical events	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm critical-event supported** command.

Purpose	Procedure
Configure that an interface does not support critical events	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface** { **gigaethernet | xgigaethernet** } *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view, or access the interface group configuration view. 3. Run the **efm critical-event unsupported** command.

11.3.7 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the EFM function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the EFM debugging function	1. Remain in the current privileged user view. 2. Run the **debug efm** { **error** | **event** | **fsm** | **timer** | **in** | **out** | **test** | **system** | **all** } command.
Disable the EFM debugging function	1. Remain in the current privileged user view. 2. Run the **no debug efm { error | event | fsm | timer | in | out | test | system | all }** command.
View the error logs of the local EFM entity	1. Access the corresponding view as follows: ● Run the **disable** command to return to the common user view. ● Run the **configure** command to access the global configuration view. ● Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number command.* ● Run the **interface eth-trunk** *trunk-number* command to access the interface configuration view. ● Remain in the current privileged user view. 2. Run the following commands: ● **show efm fault-logs all** ● **show efm fault-logs interface { gigaethernet | xgigaethernet }** *interface-number*

Purpose	Procedure
View information about the EFM OAM session between a specified interface and the peer end	1. Access the corresponding view as follows: ● Run the **disable** command to return to the common user view. ● Run the **configure** command to access the global configuration view. ● Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number command.* ● Run the **interface eth-trunk** *trunk-number* command to access the interface configuration view. ● Remain in the current privileged user view. 2. Run the following commands: ● **show efm session all** ● **show efm session interface { gigaethernet | xgigaethernet }** *interface-number* ● **show efm session interface eth-trunk** *trunk-number*
View the numbers of all types of EFM PDUs sent and received by the local EFM entity and the total number of errors that occurred at the local and remote ends	1. Access the corresponding view as follows: ● Run the **disable** command to return to the common user view. ● Run the **configure** command to access the global configuration view. ● Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number command.* ● Run the **interface eth-trunk** *trunk-number* command to access the interface configuration view. ● Remain in the current privileged user view. 2. Run the following commands: ● **show efm statistic all** ● **show efm statistic interface { gigaethernet | xgigaethernet }** *interface-number*
View the local interface configuration information.	1. Access the corresponding view as follows: ● Run the **disable** command to return to the common user view. ● Run the **configure** command to access the global configuration view. ● Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number command.* ● Run the **interface eth-trunk** *trunk-number* command to access the interface configuration view. ● Remain in the current privileged user view.

Purpose	Procedure
	2. Run the following commands: ● **show efm status all** ● **show efm status interface { gigaethernet | xgigaethernet }** *interface-number* ● **show efm status interface eth-trunk** *trunk-number*
View the summary of all EFM-enabled interfaces of the local switch	1. Access the corresponding view as follows: ● Run the **disable** command to return to the common user view. ● Run the **configure** command to access the global configuration view. ● Run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-number command.* ● Run the **interface eth-trunk** *trunk-number* command to access the interface configuration view. ● Remain in the current privileged user view. 2. Run the **show efm summary** command.
Clear the EFM logs of an interface	1. Access the interface configuration view (Ethernet or Trunk) or interface group configuration view. 2. Run the **efm fault-logs clear** command.
Clear the device EFM logs	1. Remain in the current privileged user view. 2. Run the **efm fault-logs clear all** command.

11.3.8 Configuration Example

Network Requirements

The user network is connected to the ISP network through Switch A and Switch B. The following functions are required:

- Connectivity fault detection between Switch A and Switch B is supported. The detected errors can be recorded to the logs.
- Switch B can detect the error frame, error frame interface, and error frame second of interface 10gigaethernet1/0/1 on the local device.

Network Diagram

Figure 11-5 EFM configuration topology

Configuration

1. Configure Switch A.

// Enable the EFM protocol for interface 10gigaethernet1/0/1 on Switch A.

SwitchA#configure

SwitchA(config)#interface xge1/0/1

SwitchA(config-10ge1/0/1)#efm enable

// Configure the EFM mode of interface 10gigaethernet1/0/1 to passive.

SwitchA(config-ge1/0/1)#efm mode passive

2. Configure Switch B.

// Enable the EFM protocol for interface 10ge1/0/1 on Switch B.

SwitchB#configure

SwitchB(config)#interface xge1/0/1

SwitchB(config-10ge1/0/1)#efm enable

// (Optional) Configure the default EFM mode of interface 10ge1/0/1 to active.

SwitchB(config-10ge1/0/1)#efm mode active

// Enable interface 10ge1/0/1 to support link detection.

SwitchB(config-10ge1/0/1)#efm link-monitor supported

// Configure to detect the error frame, error frame interface, and error frame second of interface 10ge1/0/1.

SwitchB(config-10ge1/0/1)#efm link-monitor frame threshold 10 window 5

SwitchB(config-10ge1/0/1)#efm link-monitor frame-period threshold 10 window 5

SwitchB(config-10ge1/0/1)#efm link-monitor frame-seconds threshold 10 window 100

11.4 Configuring CFM

11.4.1 Overview of CFM

Introduction to CFM

IEEE 802.1ag Connectivity Fault Management (CFM) defines OAM functions of connectivity fault check, fault confirmation, fault locating, and fault indication based on Ethernet bearer network. It is suitable for end-to-end scenarios of large-scale networking and is a network-level OAM.

Features of CFM

CFM has the following features:

- CFM is an extension of L3 (IP-layer) OAM to L2 Ethernet, and also the objective need for Ethernet to expand to MANs and WANs. Fault management functions of CFM have corresponding L3 OAM functions. For example, BFD corresponds to Continuity Check Protocol, IP Ping corresponds to Loopback Protocol, and IP Trace corresponds to Linktrace Protocol.
- The connectivity fault check function defined by CFM supports a packet transmission frequency of 300 Hz per second, and distinguishes different service instances by the VLAN Tagged field, so it is especially suitable for the protection switching requirements of carrier Ethernet.

11.4.2 Basic CFM Concepts

Basic CFM concepts include:

Maintenance Domain (MD)

- An MD is a network or a part of a network for which Ethernet connectivity fault management is implemented. MD is a VLAN combination for CFM. MD is similar to an autonomous system (AS) in the L3 IP protocol, and CFM packets sent by an MD always start or end in the MD.
- Generally, one bridge is configured with multiple MDs, and CFM packets of each MD can be distinguished by the VLAN tagged field. When the Ethernet traffic flow of the data channels of customers, providers, and operators cannot be distinguished by VLAN tags, the defined eight MD levels can be used to distinguish CFM packets belonging to customers, providers and carriers with mutually nested MDs.

- Among the roles of customer, provider, and carrier, the default distribution of MD levels is as follows:

  Three MD levels are allocated for the customer role: 7, 6, and 5.
  Two MD levels are allocated for the supplier role: 4 and 3.
  Three MD levels are allocated for the carrier role: 2, 1, and 0.

Caution

To divide a network into multiple MDs, it should be noted that the positional relationship of MDs can be nested, tangent or disjoint, but absolutely no intersection is allowed.

When one bridge is configured with multiple MDs, the MDs on the bridge port allow CFM packets with higher level outside the MDs to transparently traverse without any processing, and block CFM packets with the same or lower level outside the MDs.

Maintenance Association (MA)

MA is a part of MD. One MD can be divided into one or multiple Mas. Each MA is mapped to a VLAN. Ethernet CFM performs connectivity fault check for each MA.

Maintenance Association End Point (MEP)

- MEP is an edge point of MA. MEP is used to determine the boundary of each MA in CFM, and send and terminate CFM packets, thus realizing fault management.
- For any bridge running Ethernet CFM in the network, the MEP on this bridge is called the local MEP, and the MEPs on other bridges in the same MA are called RMEPs (Remote Maintenance Association End Points) relative to this bridge.
- On a bridge port without MEP, CFM packets and Ethernet traffic flow with the same VLAN tag have the same forwarding process. On a bridge port configured with MEP, MEP can monitor the Ethernet service flow with the same VLAN tag as itself (for example, check the connectivity of the Ethernet service flow), and realize fault management and performance monitoring by using CFM packets with the same VLAN tag and MD Level as itself. Generally, MEP does not terminate the Ethernet service flow or change its content.

- CFM defines two types of MEPs by direction: UP MEP and DOWN MEP. UP MEP, also called inward MEP, can be understood as an uplink port of Ethernet service flow, which is associated with UNI. UP MEP sends and receives CFM packets through the forwarding and relay function of the bridge (the switches and related products produced by Switch use the MIP corresponding to the MEP), and the port where the UP MEP is located does not send and receive CFM packets. The CFM packets received in this way appear to be terminated in the process of forwarding inside the bridge, so they are called inward MEPs. DOWN MEP, also called outward MEP, can be understood as a downlink port of Ethernet service flow and is associated with NNI. DOWN MEP directly sends and receives CFM packets to the Ethernet through the port where it is located, and does not need to be relayed through MIP (bridge).

Maintenance Association Intermediate Point (MIP)

MIP is an intermediate node in MA and is used to respond to certain CFM packets (fault confirmation CFM packets LBR/LBM, and fault locating CFM packets LTR/LTM). MIP itself does not actively send CFM packets. Except for fault confirmation and fault locating CFM packets that meet the MIP matching conditions, other CFM packets and Ethernet service flows transparently traverse MIP without any processing.

Types of Multicast MAC Addresses Used by CFM

- Multicast Class 1 DA

01:80:C2:00:00:30—01:80:C2:00:00:37

- Multicast Class 2 DA

01:80:C2:00:00:38—01:80:C2:00:00:3F

Note:

CFM has both opcodes using unicast MAC addresses and opcodes using multicast MAC addresses.

11.4.3 Supported CFM Features

CCM

Ethernet Continuity Check (ETH-CC) is an active OAM function, one of the most basic and most important functions in CFM. It provides the possibility for implementing CFM. It can be understood as the extension of the L3 BFD protocol on L2 Ethernet, usually using Class 1 multicast MAC addresses.

It is used to detect loss of continuity (LOC) between any pair of MEPs in an MEP. ETH-CC can also detect undesired connectivity between two MAs (mistake-in), undesired connectivity with an undesired MEP (undesired MEP) within an MA, and other fault conditions (such as undesired MD levels and undesired periods). ETH-CC can be used for fault management (ETH-CC, ETH-RDI, Ethernet remote end fault indication) or protection switching (G.8031/G.8032). CCM frames are used to support the ETH-CC function and ETH-RDI functions. There are 7 types of transmission periods defined by ETH-CC from 3.33 ms to 10 min, and the following 3 types are commonly used:

- Error management: The default transmission period is 1s (1 frame per second).
- Performance monitoring: The default transmission period is 100 ms (100 frames per second).
- Protection conversion: The default transmission period is 3.33 ms (300 frames per second).

Caution

As defined by CFM, MEP or MIP cannot process, send or forward CCM packets exceeding 128 bytes.

LBR/LBM Loopback (CFM Connectivity Fault Confirmation)

CFM fault confirmation, also known as Ethernet fault confirmation (ETH-LB), is an on-demand CFM function, which can be understood as an extension of IP Ping on L2 Ethernet, and is a VLAN-based L2 MAC-Ping protocol. The CFM fault confirmation function detects the connectivity between the local device MEP and the destination device MEP or MIP in the same MA by sending a query packet LBM and receiving a response packet LBR.

The CFM fault confirmation message is sent from an MEP to the designated MEP (MIP) to help the MEP locate the fault located in the MA precisely. The MIP (MEP) before the fault locating can respond to the fault confirmation message, while the MIP (MEP) after the fault locating cannot respond to the fault confirmation message, so that the fault can be located.

CFM fault confirmation can be performed in two ways:

- Unicast ETH-LB is a VLAN-based L2 MAC-Ping-MAC protocol.
- Multicast ETH-LB uses Class 1 multicast MAC addresses. It is a VLAN-based L2 MAC-Ping-MACs-in-VLAN protocol. LBR uses unicast addresses.

LTR/LTM Link Tracing (CFM Connectivity Fault Locating)

CFM fault locating, also known as Ethernet link tracing (ETH-LT), is an on-demand CFM function, which can be understood as an extension of IP Trace on L2 Ethernet, and is a VLAN-based L2 MAC-Trace protocol. The CFM fault confirmation function detects the path from the local device MEP to the destination device MEP or MIP in the same MA or locates the fault point by sending the query packet LTM and receiving the response packet LTR. CFM fault locating LTM uses Class 2 multicast MAC addresses, and LTR uses unicast addresses.

After the local MEP initiates a CFM fault locating query packet, all MIPs in the link and the terminating MEP send a CFM fault locating response packet to the local MEP. The MIPs continue to forward the CFM fault locating query packet until the packet reaches the destination MIP/MEP. Through the CFM fault locating response message, the local MEP can obtain the MAC addresses of all MIPs in the MA and the relative positions of the initiating MEP, as well as the location interval where the link failure occurs.

11.4.4 Configuring Basic CFM Functions

Background

The simplest configuration process for implementing basic CFM functions is as follows:

1. Accessing the CFM configuration view.
2. Creating an MD.
3. Creating MAs and mapping MAs to VLANs.
4. Creating MEPs or MIPs.
5. Enabling ETH-CC.

Note:

Before configuration, you are recommended to add ports of MEPs or MIPs to VLANs of their own MAs and enable the ports. You can also configure this after completing the above steps.

The requirements for creating MEPs in the same MA of the same bridge are as follows:

- MEPs of the inward interface type and MEPs of the outward interface type cannot coexist.
- MEPs and RMEPs in the same MA cannot coexist on the same switch.
- MEPs and MIPs in the same MA cannot coexist on the same interface.
- An interface allows up to one MEP in the same MA.
- If Y.1731 MEPs or MIPs are configured on the same interface, MEPs of CFM cannot be configured.

The requirements for creating MIPs in the same MA of the same switch are as follows:

- MIPs and MEPs in the same MA cannot coexist on the same interface.
- An interface allows up to one MIP in the same MA.
- If Y.1731 MIPs or MEPs are configured on the same interface, MIPs of CFM cannot be configured.

Purpose

This section describes how to configure basic CFM functions when you want to implement point-to-point connectivity check or direct link connectivity check.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create an MD and access the MD configuration view	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to create an MD and access the MD configuration view. If the MD already exists, this command enters the MD configuration view directly.
(Optional) Delete a specified MD or all MDs	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view.

Purpose	Procedure
	3. Run the **no md name** *name* command to delete a specified MD or run the **no md all** command to delete all MDs.
Create an MA, access the MA configuration view, and map MA to a VLAN	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to create an MA and access the MA configuration view. If the MA already exists, this command accesses the MA configuration view directly. Or run the **ma vlan** *vlan-list* command to create multiple MAs at a time.
(Optional) Delete a specified MA or all MAs or delete specified MAs at a time	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **no ma name** *name* command to delete a specified MA or run the **no ma all** command to delete all MAs. Or run the **no ma vlan** *vlan-list* **level** *level-value* command to delete specified MAs at a time.
Create an MEP.	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number*command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* { **inward** | **outward** } or **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
(Optional) Delete an existing MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **no cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
(Optional) Delete all MEPs in a specified MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view.

Purpose	Procedure
	3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **no mep all** command.
Create an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mip vlan** *vlan-id* **level** *level* command.
(Optional) Delete an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **no cfm mip vlan** *vlan-id* **level** *level* command.
(Optional) Delete all MIPs in a specified MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **no mip all** command.
(Optional) Configure the MAC address of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **mac** *mac-address* command.
(Optional) Configure the MAC address of an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mip vlan** *vlan-id* **level** *level* **mac** *mac-address* command.

Purpose	Procedure
(Optional) Create or delete a VLAN mapping table automatically generated by an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **mip auto-config vlan** *vlan-list* command to create a VLAN mapping table automatically generated by an MIP or run the **no mip auto-config vlan** *vlan-list* command to delete a VLAN mapping table automatically generated by an MIP.
(Optional) Create an RMEP in the current MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **remote-mep mep-id** *mep-id* **mac** *mac-address* command to create an RMEP in the current MA or run the **remote-mep mep-id** *mep-id-list* command to create RMEPs in batch in the current MA.
(Optional) Delete an RMEP in the current MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **no remote-mep all** command to delete all RMEPs in a specified MA or run the **no remote-mep mep-id** *mep-id-list* command to delete an RMEP in a specified MA.
Enable or disable MEP CC	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ccm priority** *priority* { **enable** | **disable** } or **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ccm** { **enable** | **disable** } command.

Purpose	Procedure
Enable or disable CC for all MEPs in an MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **ccm** { **enable** | **disable** } command.

Attached table:

Parameter	Description	Value
name	Specifies an MD name.	The value is a character string.
level	Specifies an MD level.	The value is an integer ranging from 0 to 7.
name	Specifies the name of an MA.	The value is a character string.
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
vlan-list	Specifies the VLAN list with MAC address mapping for batch creation.	The value is an integer ranging from 1 to 4094.
level	Specifies an MA level.	The value is an integer ranging from 0 to 7.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
inward	Specifies the up direction.	-
outward	Specifies the down direction.	-
mac-address	Specifies the MAC address of an MEP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
mac-address	Specifies the MAC address of an MIP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.

Parameter	Description	Value
vlan-list	Specifies a VLAN mapping list.	The value is an integer ranging from 1 to 4094.
mep-id	Specifies an RMEP ID.	The value is an integer ranging from 1 to 1891.
mep-id-list	Specifies a list of RMEP IDs.	The value is an integer ranging from 1 to 1891.
mac-address	Specifies the bridge MAC address of the switch where the RMEP is located.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits
all	Specifies all RMEPs in the current MA.	-

11.4.5 Configuring CFM Parameters

Purpose

This section describes how to adjust Ethernet CFM parameters to better implement point-to-point connectivity fault check in Ethernet.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Reset the CFM packet counters of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **reset counter** command.
Configure the CC packet sending interval for MEPs in the current MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view.

Purpose	Procedure
	5. Run the **ccm-interval { 300Hz | 10ms | 100ms | 10s | 1min | 10min | default }** command.
Configure the CC loss threshold for MEPs in the current MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **ccm loss-threshold** { *threshold-value* | **default** } command.
Clear the CFM packet counters of an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **cfm reset counter** command.
Enable or disable static RMEP check	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **cross-check** { **enable** | **disable** } command.
Configure the RMEP activation time	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **cross-check start-delay** { *delay-value* | **default** } command.
Configure the aging time of MIP CCDB	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view.

Purpose	Procedure
	3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **mip-ccdb aging-time** { *aging-time* | **default** } command.
Configure the aging time of a dynamic RMEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **remote-mep aging-time** { *aging-time* | **default** } command.
Clear the CFM packet counters of an MA	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view. 5. Run the **reset counter** command.
Configure the Sender ID TLV type of CFM packets	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **senderid-tlv-type { none | chassis | manage | chassis-manage | defer }** command.
Configure the aging time of LTR responses	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **cfm** command to access the CFM configuration view from the global configuration view. 3. Run the **md name** *name* **level** *level* command to access the MD configuration view. 4. Run the **ma name** *name* **vlan** *vlan-id* command to access the MA configuration view.

Purpose	Procedure
	5. Run the **trace-replay aging-time** { *aging-time* | **default** } command.

Attached table:

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies a local MEP ID.	The value is an integer ranging from 1 to 8191.
threshold-value	Specifies a CC loss threshold.	The value is an integer ranging from 2 to 255, in the unit of CC packet sending intervals.
default	Uses the default CC loss threshold.	The default CC loss threshold is 3.5 times the CC packet sending interval.
delay-value	Specifies an RMEP activation time.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	0s
aging-time	Specifies the aging time of a dynamic RMEP.	The value is an integer ranging from 1 to 65535, in seconds.
default	Uses the default aging time.	1000s
none	Specifies that the sender ID TLV type is not included in sent CFM packets.	-
chassis	Specifies that the chassis ID is included in sent CFM packets.	-
manage	Specifies that the management address is included in sent CFM packets.	-
chassis-manage	Specifies that the chassis ID and management address are included in sent CFM packets.	-

Parameter	Description	Value
defer	Indicates that the Sender ID TLV content is determined by the MD management object.	-
aging-time	Specifies the aging time of LTR responses.	The value is an integer ranging from 1 to 65535, in seconds.
default	Uses the default aging time of LTR responses.	1000s

11.4.6 Configuring CFM Fault Confirmation

Purpose

This section describes how to send a test packet and receive the response packet to check whether the local device can ping the destination device when you need to manually check connectivity of a link between two devices.

Caution

If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the CFM fault confirmation result is unpredictable.

This operation of configuring CFM fault confirmation is performed on the root node of the switch. To stop sending LBM packets, press **Ctrl**+**C**.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure MAC address ping for locating a CFM connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*

Purpose	Procedure
	● **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority-value* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout* ● **cfm ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
Configure remote MEP ping for locating a CFM connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout* ● **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout* ● **cfm ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id*
Configure all remote MEP ping for locating a CFM connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-s** *packet-size* **-t** *packet-timeout* ● **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-s** *packet-size* **-t** *packet-timeout* ● **cfm ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id*

Attached table:

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
mac-address	Specifies the MAC address of a remote MEP or MIP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
mep-id	Specifies the MEP that initiates ping in the local bridge.	The value is an integer ranging from 1 to 1891.

Parameter	Description	Value
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 1891.
priority-value	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-count	Specifies the times of ping.	The value is an integer ranging from 1 to 1024.
packet-size	Specifies the size of a sent ping packet, including the size of the L2 packet header.	The value is an integer ranging from 64 to 1518. The default value is 64.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.

11.4.7 Configuring CFM Fault Locating

Purpose

This section describes how to send a test packet and receive the response packet to check whether the route from the local device to the destination device is reachable or locate the fault point when you need to manually check connectivity of a link between two devices.

Caution

If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the CFM fault confirmation result is unpredictable.

Configure CFM fault locating to perform on the root node of the switch. Tracing results are displayed immediately if they are correct. If tracing results are incorrect, reference results may be displayed after the set timeout time. If you want to stop tracing, press **Ctrl**+**C**.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure MAC address tracing for locating any CFM connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout* { **fdb-only** | **ccdb** } ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **{ fdb-only | ccdb }** ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **{ fdb-only | ccdb }** ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* { **fdb-only** | **ccdb** } ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* ● **cfm trace mac** *mac-address* **mep** vlan *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* **{ fdb-only | ccdb }** ● **cfm trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* { **fdb-only** | **ccdb** }
Configure remote MEP tracing for locating any CFM connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* l**evel** *level* **mepid** *local-mep-id* ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout*

Purpose	Procedure
	● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **-t** *packet-timeout* { **fdb-only** | **ccdb** } ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* { **fdb-only** | **ccdb** } ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* { **fdb-only** | **ccdb** } ● **cfm trace remote-mep** remote-mep-id **mep vlan** vlan-id **level** level **mepid** local-mep-id **-t** packet-timeout ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **-t** *packet-timeout* { **fdb-only** | **ccdb** } ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **priority** *priority* **ttl** *ttl-value* { **fdb-only** | **ccdb** } ● **cfm trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *local-mep-id* **ttl** *ttl-value* **{ fdb-only | ccdb }**

Attached table:

Parameter	Description	Value
mac-address	Specifies the MAC address of a remote MEP or MIP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 1891.
local-mep-id	Specifies the MEP ID of the Trace action initiated by the local network bridge.	The value is an integer ranging from 1 to 1891.

Parameter	Description	Value
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.
ttl-value	Specifies the maximum number of hops for Trace.	The value is an integer ranging from 1 to 255. The default value is 64.
fdb-only	Specifies that only the MAC forwarding table is used for forwarding LTM packets.	-
ccdb	Specifies the use of MIP CCDB for forwarding LTM packets when they cannot be forwarded by using the forwarding table. This is the default option for tracing initiation.	-

11.4.8 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the CFM function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable debugging of the CFM module	1. Remain in the current privileged user view. 2. Run the command **debug cfm module { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lck-out | lck-in | all }**.
Disable debugging of the CFM module	1. Remain in the current privileged user view. 2. Run the command **no debug cfm module { nm | main | trap | os-io | sync | pkt-out | pkt-in | hw-notify | hw-setting | ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lck-out | lck-in | all }**.

Purpose	Procedure
Enable CFM packet transmission debugging	1. Remain in the current privileged user view. 2. Run the following commands: ● **debug cfm packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **debug cfm packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface eth-trunk** *trunk-number*
Disable CFM packet transmission debugging	1. Remain in the current privileged user view. 2. Run the following commands: ● **no debug cfm packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no debug cfm packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | all } interface eth-trunk** *trunk-number*
View the summary of CFM	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm** command.
View the CFM configuration file information	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm config** command.
View the summary or details of MEP ERROR CCDBs	1. Run the **disable** command to return to the common user view. 2. Run the following commands: ● **show cfm error ccdb** ● **show cfm error ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id*
View summary or details or an MA	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm ma** or **show cfm ma** *name* **vlan** *vlan-id* command.
View summary or details or an MD	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm md** or **show cfm md** *name* vlan vlan-id command.
View summary or details or an MEP	1. Run the **disable** command to return to the common user view.

Purpose	Procedure
	2. Run the **show cfm mep** or **show cfm mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command
View the summary or details of an MEP CCDB	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm mep ccdb** or **show cfm mep ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
View information about all MIPs configured for a bridge	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm mip** command.
View the summary of MIP CCDBs	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm mip ccdb** command.
View CFM packet statistics on an interface	1. Run the **disable** command to return to the common user view. 2. Run the following commands: ● **show cfm pdu-statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show cfm pdu-statistic interface eth-trunk** *trunk-number* ● **show cfm pdu-statistic interface**
View summary or details or an RMEP	1. Run the **disable** command to return to the common user view. 2. Run the following commands: ● **show cfm remote-mep** ● **show cfm remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id*
View the results of the last query about fault locating for an MEP of the bridge	1. Run the **disable** command to return to the common user view. 2. Run the **show cfm trace-result mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
Enable or disable the SNMP alarm reporting function for CFM	1. Run the **cfm** command to access the CFM configuration view. 2. Run the **snmp-trap** { **enable** | **disable** } command.

11.4.9 Configuration Example

Network Requirements

This example shows how to configure CFM in multiple MAs.

Allocate devices wh-s7808, cs-s3628, nc-s3628, hf-s3628, and zz-s3628 to MD1 and set the MD level to 1.

Allocate devices cd-s2200, gz-s2200, sh-s2200, and bj-s2200 to MD2 and set the MD level to 6. Each MD can add its own MAs. Since level of MD2 is higher than that of MD1, CFM packets of MD2 can transparently pass through MD1 and the two do not interfere with each other.

After dividing MDs, determine the MD boundaries according to Figure 11-6 and configure interfaces for MEPs in each MD as long as that MEP IDs in the same MD are not duplicate.

To enable CFM for an intermediate point in an MD, configure this point as an MIP. For the interface of MEP in MD1, configure an MIP for MD2.

Network Diagram

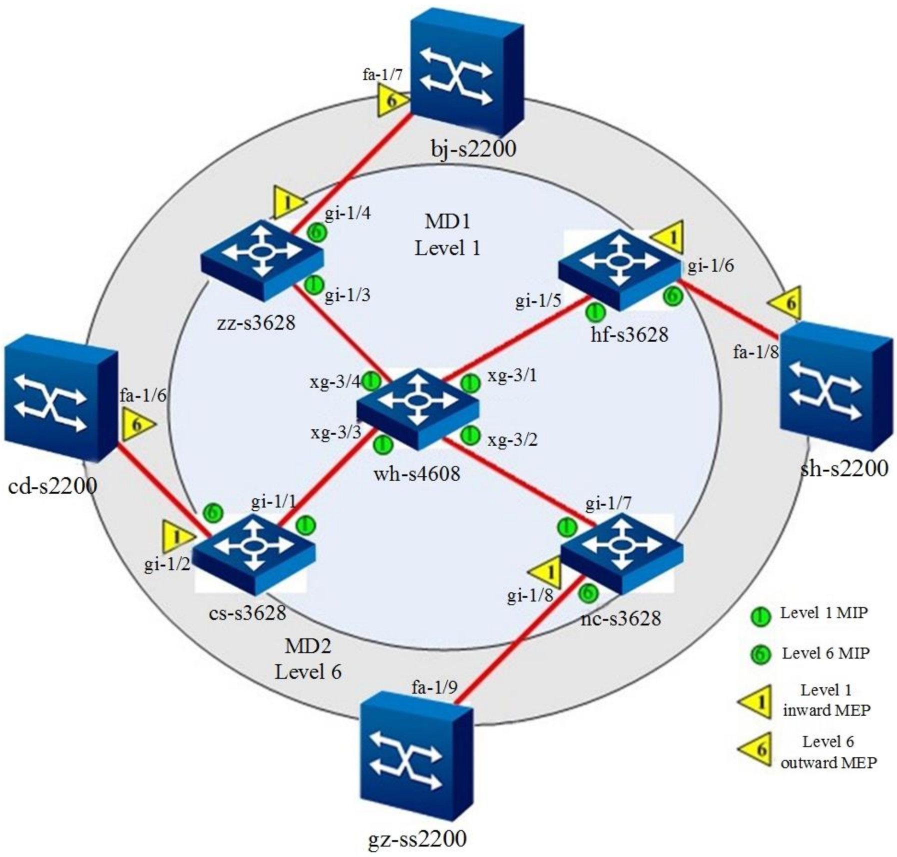


Figure 11-6 CFM configuration network diagram

Configuration

Configure each bridge as follows:

1. Configure MD1.

1) Configure wh-XXXX

```
wh-XXXX#configure
wh-XXXX(config)#cfm
wh-XXXX(config-cfm)#md name md1 level 1
wh-XXXX(config-md-md1)#ma name ma1 vlan 1
wh-XXXX(config-md-md1-ma-ma1)#quit
wh-XXXX(config)#interface xgigaethernet 1/0/1 to xgigaethernet 1/0/4
wh-XXXX(config-xg1/0/1->xg1/0/4)#cfm mip vlan 1 level 1
```

2) Configure cs-s3628

```
cs-s3628#configure
cs-s3628(config)#cfm
cs-s3628(config-cfm)#md name md1 level 1
cs-s3628(config-md-md1)#ma name ma1 vlan 1
cs-s3628(config-md-md1-ma-ma1)#quit
cs-s3628(config-cfm)#md name md2 level 6
cs-s3628(config-md-md2)#ma name ma2 vlan 1
cs-s3628(config-md-md2-ma-ma2)#quit
cs-s3628(config)#interface 10gigaethernet 1/0/1
cs-s3628(config-10ge1/0/1)#cfm mip vlan 1 level 1
cs-s3628(config-10ge1/0/1)#quit
cs-s3628(config)#interface 10gigaethernet 1/0/2
cs-s3628(config-10ge1/0/2)# cfm mip vlan 1 level 6
cs-s3628(config-10ge1/0/2)#cfm mep vlan 1 level 1 mepid 1 inward
cs-s3628(config-10ge1/0/2)#cfm mep vlan 1 level 1 mepid 1 ccm enable
```

3) Configure nc-s3628

```
nc-s3628#configure
nc-s3628(config)#cfm
nc-s3628(config-cfm)#md name md1 level 1
nc-s3628(config-md-md1)#ma name ma1 vlan 1
nc-s3628(config-md-md1-ma-ma1)#quit
nc-s3628(config-cfm)#md name md2 level 6
nc-s3628(config-md-md2)#ma name ma2 vlan 1
nc-s3628(config-md-md2-ma-ma2)#quit
nc-s3628(config)#interface 10 gigaethernet 1/0/7
nc-s3628(config-10ge1/0/7)#cfm mip vlan 1 level 1
```

```
nc-s3628(config-10ge1/0/7)#quit
nc-s3628(config)#interface 10gigaethernet 1/0/8
nc-s3628(config-10ge1/0/8)# cfm mip vlan 1 level 6
nc-s3628(config-10ge1/0/8)#cfm mep vlan 1 level 1 mepid 100 inward
nc-s3628(config-10ge1/0/8)#cfm mep vlan 1 level 1 mepid 100 ccm enable
```

4) Configure hf-s3628

```
hf-s3628#configure
hf-s3628(config)#cfm
hf-s3628(config-cfm)#md name md1 level 1
hf-s3628(config-md-md1)#ma name ma1 vlan 1
hf-s3628(config-md-md1-ma-ma1)# quit
hf-s3628(config-cfm)#md name md2 level 6
hf-s3628(config-md-md2)#ma name ma2 vlan 1
hf-s3628(config-md-md2-ma-ma2)# quit
hf-s3628(config)#interface 10gigaethernet 1/0/5
hf-s3628(config-10ge1/0/5)#cfm mip vlan 1 level 1
hf-s3628(config-10ge1/0/5)# quit
hf-s3628(config)#int 10gigaethernet 1/0/6
hf-s3628(config-10ge1/0/6)# cfm mip vlan 1 level 6
hf-s3628(config-10ge1/0/6)#cfm mep vlan 1 level 1 mepid 1000 inward
hf-s3628(config-10ge1/0/6)#cfm mep vlan 1 level 1 mepid 1000 ccm enable
```

5) Configure zz-s3628

```
zz-s3628#configure
zz-s3628(config)#cfm
zz-s3628(config-cfm)#md name md1 level 1
zz-s3628(config-md-md1)#ma name ma1 vlan 1
zz-s3628(config-md-md1-ma-ma1)#quit
zz-s3628(config-cfm)#md name md2 level 6
zz-s3628(config-md-md2)#ma name ma2 vlan 1
zz-s3628(config-md-md2-ma-ma2)#quit
zz-s3628(config)#interface 10gigaethernet 1/0/3
zz-s3628(config-ge1/0/3)#cfm mip vlan 1 level 1
zz-s3628(config-ge1/0/3)#quit
zz-s3628(config)#interface 10gigaethernet 1/0/6
zz-s3628(config-10ge1/0/4)# cfm mip vlan 1 level 6
zz-s3628(config-10ge1/0/4)#cfm mep vlan 1 level 1 mepid 7777 inward
zz-s3628(config-10ge1/0/4)#cfm mep vlan 1 level 1 mepid 7777 ccm enable
```

2. Configure MD2.

1) Configure cd-s2200

```
cd-s2200#configure
cd-s2200(config)#cfm
cd-s2200(config-cfm)#md name md2 level 6
cd-s2200(config-md-md2)#ma name ma2 vlan 1
cd-s2200(config-md-md2-ma-ma2)#quit
cd-s2200(config)#interface fastethernet 1/0/6
cd-s2200(config-fe1/0/6)#cfm mep vlan 1 level 6 mepid 1
cd-s2200(config-fe1/0/6)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

2) Configure gz-s2200

```
gz-s2200#configure
gz-s2200(config)#cfm
gz-s2200(config-cfm)#md name md2 level 6
gz-s2200(config-md-md2)#ma name ma2 vlan 1
gz-s2200(config-md-md2-ma-ma2)#quit
gz-s2200(config)#interface fastethernet 1/0/9
gz-s2200(config-fe1/0/9)#cfm mep vlan 1 level 6 mepid 1
gz-s2200(config-fe1/0/9)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

3) Configure sh-s2200

```
sh-s2200#configure
sh-s2200(config)#cfm
sh-s2200(config-cfm)#md name md2 level 6
sh-s2200(config-md-md2)#ma name ma2 vlan 1
sh-s2200(config-md-md2-ma-ma2)#quit
sh-s2200(config)#interface fastethernet 1/0/8
sh-s2200(config-fe1/0/8)#cfm mep vlan 1 level 6 mepid 1
sh-s2200(config-fe1/0/8)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

4) Configure bj-s2200

```
bj-s2200#configure
bj-s2200(config)#cfm
bj-s2200(config-cfm)#md name md2 level 6
bj-s2200(config-md-md2)#ma name ma2 vlan 1
bj-s2200(config-md-md2-ma-ma2)#quit
bj-s2200(config)#interface fastethernet 1/0/7
bj-s2200(config-fe1/0/7)#cfm mep vlan 1 level 6 mepid 1
bj-s2200(config-fe1/0/7)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

11.5 Configuring Y.1731

11.5.1 Y.1731 Overview

Introduction to Y.1731 Fault Management Protocol

Ethernet was used for LAN environments and had a poor operation, administration, and management (OAM) capability. To achieve the same level of services as traditional bearer transport networks, Y.1731 was developed by ITU-T SG13, which defines OAM functions of connectivity fault check, fault confirmation, fault locating, and fault indication based on Ethernet bearer network. It is suitable for end-to-end scenarios of large-scale networking and is a network-level OAM.

IEEE, ITU-T and MEF unify a multi-domain OAM network model, as shown in Figure 11-7 OAM multi-domain network model. Bearer Ethernet is divided into three maintenance levels: user, provider, and carrier, which correspond to different management domains. The provider is responsible for end-to-end service management, and the carrier provides service delivery.

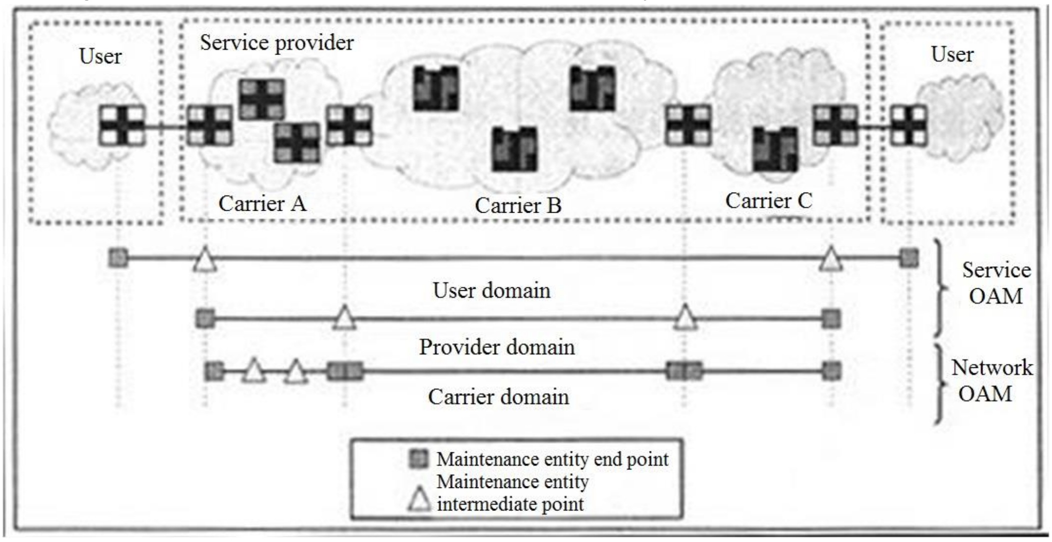


Figure 11-7 OAM multi-domain network model

Features of Y.1731 Fault Management Technology

The Y.1731 fault management technology provides the following features:

- Y.1731 is an extension of L3 (IP-layer) OAM to L2 Ethernet, and also the objective need for Ethernet to expand to MANs and WANs. Fault management functions of Y.1731 have corresponding L3 OAM functions. For example, BFD corresponds to continuity check, IP Ping corresponds to Y.1731 loopback, and IP Trace corresponds to Y.1731 linktrace.

- The connectivity fault check function defined by ITU-T Y.1731 supports a packet transmission frequency of 300 Hz per second, and distinguishes different service instances by the VLAN Tagged field, so it is especially suitable for the protection switching requirements of carrier Ethernet.
- The Y.1731 connectivity check packet has become the connectivity check standard of the G.8031/G.8032 standard proposed by I-TUT. In theory, it can provide a unified connectivity check standard for Ethernet blocking protocols (such as Ethernet Ring and Smart Link) defined by device providers, which can enable intercommunication between Ethernet block protocols defined by device providers and reduce the carrier network running, operation, and maintenance costs.

11.5.2 Basic Concepts of Y.1731 Fault Management Instance

Maintenance Entity Group (MEG)

MEG is a virtual network for Y.1731 fault management, which can be understood as a service instance (the mapping VLAN of MEG in Y.1731 fault management) represented by a character string (MEG ID in Y.1731 fault management).

Caution

To divide a network into multiple MEGs, it should be noted that the positional relationship of MEGs can be nested, tangent or disjoint, but absolutely no intersection is allowed.

MEG Name (MEG ID)

The name of an MEG has several formats, which is specifically identified by the MEG ID format field. Y.1731-based MEG ID is in the format of International Telecommunication Union (ITU) carrier code (ICC). An ICC-based MEG ID consists of two subfields: ICC and UMC. ICC consists of 1-8 characters, letters, or first letters on the left followed by numbers. UMC is a unique MEG ID, consisting of 7-12 letters and NULL (0), making the MEG ID exactly 13 characters. Figure 11-8 shows the format of an ICC-based MEG ID in an ETH-CC packet.

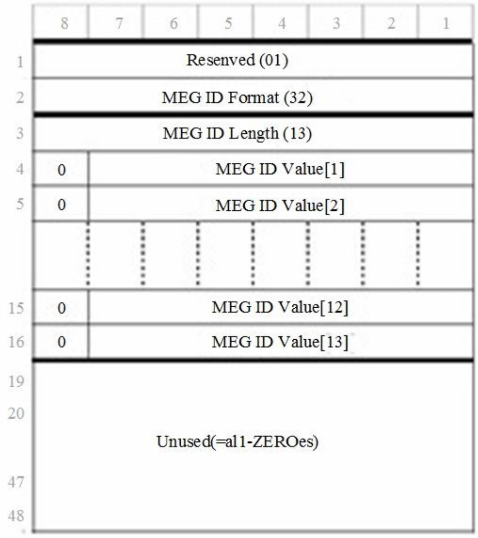


Figure 11-8 Format of an ICC-based MEG ID

MEG Level (MEL)

Generally, a bridge configured with multiple MEGs uses the VLAN tag field to distinguish Y.1731 data frames of different MEGs. When data frames cannot be distinguished by VLAN tags, the Y.1731 data frames of multiple MEGs can be distinguished by the MEG levels.

Y.1731 defines 8 MEG levels to distinguish Y.1731 frames of mutually nested MEGs belonging to customers, providers and carriers to meet different scenarios of network deployment.

Among the roles of customer, provider, and carrier, the default distribution of MEG levels is as follows:

- Three MEG levels are allocated for the customer role: 7, 6, and 5.
- Two MEG levels are allocated for the supplier role: 4 and 3.
- Three MEG levels are allocated for the carrier role: 2, 1, and 0.

Caution

When one bridge is configured with multiple MEGs, the MEGs on the bridge port allow Y.1731 packets with higher MEL outside the MEGs to transparently traverse without any processing, and block Y.1731 packets with the same or lower MEL outside the MEGs.

MEG Point (MEP)

MEP is a point of an MEG and is used to determine the boundary of each MEG for Y.1731 fault management. It sends and terminates Y.1731 data frames for fault management and performance monitoring.

On a bridge port without MEP, Y.1731 packets and Ethernet service flow with the same VLAN tag have the same forwarding process.

On a bridge port configured with MEP, MEP can monitor the Ethernet service flow with the same VLAN tag as itself and generally does not terminate the Ethernet service flow or modifies the content of the Ethernet service flow. It realizes fault management and performance monitoring by using Y.1731 packets with the same VLAN tag and MEL.

MEP Direction

Y.1731 defines two types of MEPs by direction: UP MEP and DOWN MEP.

- UP MEP, also called inward MEP, can be understood as an uplink port of Ethernet service flow, which is associated with UNI. UP MEP sends and receives Y.1731 frames through the forwarding and relay function of the bridge (the current device uses the MIP corresponding to the MEP), and the port where the UP MEP is located does not send and receive Y.1731 frames. The Y.1731 packets received in this way appear to be terminated in the process of forwarding inside the bridge, so they are called inward MEPs.
- DOWN MEP, also called outward MEP, can be understood as a downlink port of Ethernet service flow and is associated with NNI. DOWN MEP directly sends and receives Y.1731 frames to and from the Ethernet through the port where it is located, and does not need to be relayed through MIP (bridge).

MEG Intermediate Point (MIP)

MIP is an intermediate node in MEG and is used to respond to certain Y.1731 packets (fault confirmation Y.1731 packets LBR/LBM, and fault locating Y.1731 packets LTR/LTM). MIP itself does not send Y.1731 frames. Except for fault confirmation and fault locating Y.1731 packets that meet the MIP matching conditions, other Y.1731 packets and Ethernet service flows transparently traverse MIP without any processing.

MAC Address of a Y.1731 Frame (DA)

Y.1731 has both opcodes using unicast MAC addresses and opcodes using multicast MAC addresses. There are two types of multicast MAC addresses in Y.1731:

- Multicast Class 1 DA

01:80:C2:00:00:30—01:80:C2:00:00:37

- Multicast Class 2 DA

01:80:C2:00:00:38—01:80:C2:00:00:3F

OAM Type	DAs for frames with OAM PDU
CCM	Multicast Class 1 DA or Unicast DA
LBM	Unicast DA or Multicast Class 1 DA
LBR	Unicast DA
LTM	Multicast Class 2 DA
LTR	Unicast DA
AIS	Multicast Class 1 DA or Unicast DA
LCK	Multicast Class 1 DA or Unicast DA
TST	Unicast DA or Multicast Class 1 DA
Linear APS	Multicast Class I DA or Unicast DA
Ring APS	Multicast Class 1 DA or UnicastDA
MCC	Unicast DA or Multicast Class 1 DA
LMM	Unicast DA or Multicast Class 1 DA
LMR	Unicast DA
1DM	Unicast DA or Multicast Class 1 DA
DMM	Unicast DA or Multicast Class 1 DA
DMR	Unicast DA
EXM.EXR.VSM.VSR	Outside the scope of this Recommendation

Figure 11-9 MAC addresses corresponding to Y.1731 opcodes

11.5.3 Supported Y.1731 Features

Caution

Switches and related products of Switch cannot process ETH-CC/ETH-LTR/ETH-LTM/ETH-AIS/ETH-LCK packets exceeding 256 bytes.

ETH-CC

ETH-CC is a proactive OAM function. It can detect Loss of Continuity (LOC) between any pair of MEPs in an MEG, an incorrect connection between two MEGs, a connection to an incorrect MEP in an MEG, and other faults. The CC message can be used for fault management (ETH-CC, ETH-RDI, and Ethernet remote end fault indication), performance monitoring (dual-end ETH-M), or protection switching (G.8031/G.8032).

There are 7 types of transmission periods defined by ETH-CC from 3.33 ms to 10 min, and the following 3 types are commonly used:

- Error management: The default transmission period is 1s (1 frame per second).
- Performance monitoring: The default transmission period is 100 ms (100 frames per second).
- Protection conversion: The default transmission period is 3.33 ms (300 frames per second).

Caution

As defined by Y.1731, MEP or MIP cannot process, send or forward CCM packets exceeding 128 bytes.

ETH-LBR/LBM Ethernet Fault Confirmation

Ethernet confirmation is an on-demand OAM function. The Y.1731 fault confirmation function detects the connectivity between the local device MEP and the destination device MEP or MIP in the same MEG by sending a query packet LBM and receiving a response packet LBR.

There are two types of Y.1731 fault confirmation:

- Unicast ETH-LB is a VLAN-based L2 MAC-Ping-MAC protocol.
- Multicast ETH-LB uses Class 1 multicast MAC addresses. It is a VLAN-based L2 MAC-Ping-MACs-in-VLAN protocol. LBR uses unicast addresses.

The Y.1731 fault confirmation message is sent from an MEP to the designated MEP (MIP) to help the MEP locate the fault located in the MEG precisely. The MIP (MEP) before the fault locating can respond to the fault confirmation message, while the MIP (MEP) after the fault locating cannot respond to the fault confirmation message, so that the fault can be located. Figure 11-10 and Figure 11-11 show the working principle of Y.1731 fault confirmation in unicast and multicast modes respective.

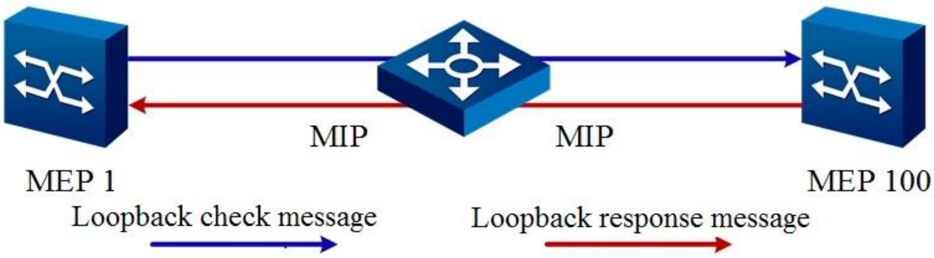


Figure 11-10 Working principle of Y.1731 unicast fault confirmation

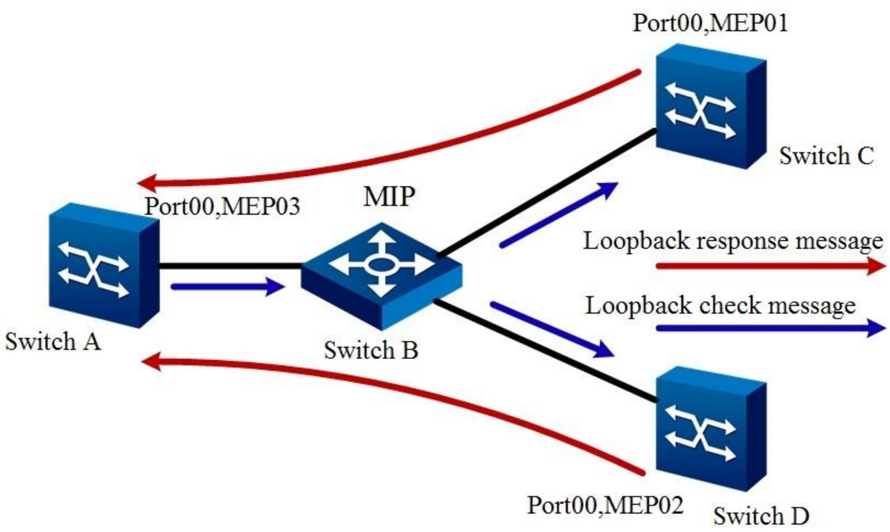


Figure 11-11 Working principle of Y.1731 multicast fault confirmation

ETH-LTR/LTM Ethernet Fault Locating

Y.1731 fault locating is also known as Ethernet link tracing (ETH-LT) and is an on-demand OAM function. The Y.1731 fault locating function detects the route from the local device MEP to the destination device MEP or MIP in the same MEG or locates the fault point by sending the query packet LTM (using the Class 2 MAC address) and receiving the response packet LTR (using the unicast address).

After the local MEP initiates a Y.1731 fault locating query packet, all MIPs in the link and the terminating MEP send a Y.1731 fault locating response packet to the local MEP. The MIPs continue to forward the Y.1731 fault locating query packet until the packet reaches the destination MIP/MEP. Through the Y.1731 fault locating response message, the local MEP can obtain the MAC addresses of all MIPs in the MEG and the relative positions of the initiating MEP, as well as the location interval where the link failure occurs, as shown in Figure 11-12.

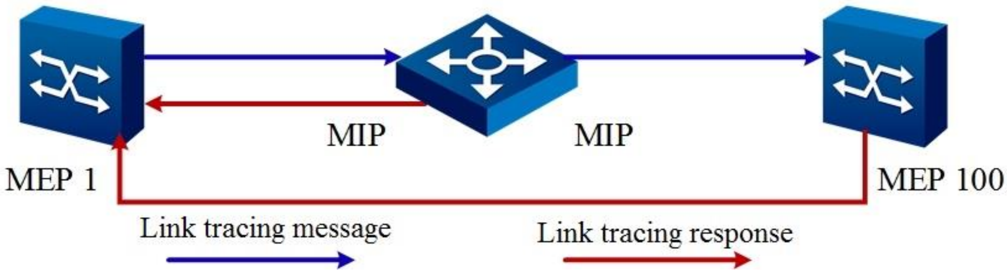


Figure 11-12 Basic principle of Y.1731 fault locating

Ethernet Alarm Indication Signal (ETH-AIS)

ETH-AIS uses a Class 1 multicast MAC address to suppress alarms (traps) after the service layer (sublayer) detects a connectivity fault. Y.1731 frames carrying ETH-AIS are sent or terminated on an MEP or server MEP. ETH-AIS is not applicable to STP environments.

Y.1731 frames carrying ETH-AIS are sent at the customer's MEG level when the MEP (or server MEP) detects a fault. As shown in Figure 11-13, the data flow in red is an ETH-AIS. The MEL of ETH-AIS is always higher than that of the MEP that sends the ETH-AIS.

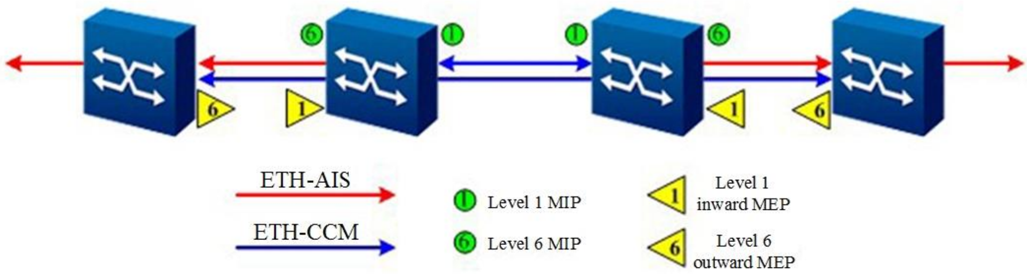


Figure 11-13 Basic principle of Y.1731 alarm indication information/

Faults are divided into the following two types as an example:

1. Abnormal signal in the case of ETH-CC execution in an MEG, mainly including"

- Loss of continuity (LOC) between any pair of MEPs in an MEG;
- Undesired connectivity between two MEGs (with error contained and different MEG IDs);
- Undesired connectivity between an MEG and an undesired MEP (undesired MEP);
- Undesired MEG level (the local MEP detects a lower MEL for ETH-CC);
- Unexpected cycles (cycles of the local MEP and remote MEP in an MEG are inconsistent);
- ETH-CC hysteresis (the local MEP in an MEG receives its own ETH-CC information);

2. When ETH-CC is turned off in an MEG, the AIS or LCK generally needs to be triggered by other Ethernet link check protocols. Currently, AIS can be triggered only after the IEEE 802.3ah discovery function fails.

Caution

For the two faults mentioned above, to meet the ETH-AIS transmission requirements, ensure that the interface of the MEP transmitting AIS is configured with an MIP with a level higher than the MEP level.

Ethernet Lock Signal (ETH-LCK)

ETH-LCK is used to announce the administrative lock of a server-layer (sub-layer) MEP and the subsequent interruption of the data service flow destined for the MEP that expects to receive the service flow. It enables MEPs receiving frames with ETH-LCK information to distinguish between faults and administrative locking actions of server-layer (sub-layer) MEPs. ETH-LCK uses Class1 multicast MAC address as its destination MAC address.

When LCK is enabled for an MEP, the Ethernet service flow is automatically interrupted at the port of the MEP. In this case, the MEP will send an LCK packet to a higher-level MEP. After the higher-level MEP receives the LCK packet, it will automatically interrupt all Ethernet service flows on the port where the MEP is located. The Ethernet service flow is automatically resumed after LCK is disabled.

Caution

In environments where blocking protocols are running, LCK may lead to ambiguity between the port forwarding state and the actual expected port forwarding state. Therefore, restrict the use of LCK in scenarios where blocking protocols are running.

11.5.4 Configuring Basic Y.1731 Functions

Background

The simplest configuration process for implementing basic Y.1731 functions is as follows:

1. Accessing the Y.1731 configuration view.
2. Creating an MEG.
3. (Optional) Creating MEPs or MIPs.
4. Enabling ETH-CC.

Note:

Before configuration, you must create a VLAN to which the MEG is mapped, then add the interface of MEPs or MIPs to the VLAN of the corresponding MEG, and then run the **no shutdown** command to enable this interface. You can also configure this after completing the above steps.

- The MIP and MEP in the same MEG cannot coexist in an interface.
- Only one MIP in the same MEG can exist in an interface.
- If the MIP or MEP of the CFM is configured in an interface, the MIP of Y.1731 cannot be configured in the interface any more.

Purpose

This section describes how to configure basic Y.1731 functions when you want to implement end-to-end connectivity check or direct link connectivity check.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create an MEP.	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the following commands: ● **y1731 mep vlan** *vlan-id* **level** *level* ● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* ● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* **{ inward | outward }**
(Optional) Enable or Disable AIS for an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the following commands: ● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ais { enable | disable }** ● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ais priority** ***priority*** **{ enable | disable }**
(Optional) Enable or Disable external triggering for AIS	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ais 8023ah-cause { enable | disable }** command.
Enable or Disable CCM for an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the following commands: ● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* **ccm { enable | disable }**

Purpose	Procedure
	● **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* **ccm priority** *priority* **{ enable | disable }**
(Optional) Configure the MAC address of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* **mac** *mac-address* command.
Create an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 mip vlan** *vlan-id* **level** *level* command.
(Optional) Configure the MAC address of an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 mip vlan** *vlan-id* **level** *level* **mac** *mac-address* command.
(Optional) Configure a VLAN mapping table automatically generated by an MIP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **mip auto-config vlan** *vlan-list* command.
(Optional) Enable or Disable CCM for an MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ccm** { **enable** | **disable** } command.
(Optional) Enable or	1. Run the **configure** command in the privileged user view to access the global configuration view.

Purpose	Procedure
Disable AIS for an MEG	2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ais** { **enable** | **disable** } command.
(Optional) Enable or disable static RMEP check	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **cross-check { enable | disable }** command.
(Optional) Enable or Disable LCK for an MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **lock** { **enable** | **disable** } command.
(Optional) Create an RMEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **remote-mep mep-id** *mep-id* **mac** *mac address* command.
(Optional) Create RMEPs in batch	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **remote-mep mep-id** *IDLIST* command.

Attached table:

Parameter	Description	Value
interface-number	Specifies the ID of a physical interface.	The value is an integer in the range of <1-12>/<1-48>.
trunk-number	Specifies an aggregation interface number.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies the VLAN ID corresponding to a single created MEG.	The value is an integer ranging from 1 to 4094.
VLANLIST	Specifies multiple VLAN IDs corresponding to batch created MEGs.	The value is an integer ranging from 1 to 4094. Multiple VLAN IDs are separated by a hyphen (-), for example, vlan 1-100.
level	Specifies an MEG level. A total of 8 levels are supported.	The value is an integer ranging from 0 to 7. By default, MEG levels are classified as follows: Three MEG levels are allocated for the customer role: 7, 6, and 5. Two MEG levels are allocated for the supplier role: 4 and 3. Three MEG levels are allocated for the carrier role: 2, 1, and 0.
Icc string	Specifies the International Telecommunication Union (ITU) carrier code (ICC).	The value consists of 1-8 characters, letters or a letter at the first place and then all numbers.
umc string	Specifies the unique MEG ID code.	The value consists of 7-12 characters and then NULL (0).

11.5.5 Configuring Y.1731 Parameters

Purpose

This section describes how to adjust Y.1731 parameters to better implement point-to-point connectivity fault check in Ethernet.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Delete all MEGs	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **no meg all** command.
Enable or disable the SNMP alarm reporting function for Y.1731	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **snmp trap** { **enable** | **disable** } command.
Clear the Y.1731 frame count of an MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mepid-id* **reset counter** command.
Clear the Y.1731 frame count of an interface	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **interface gigaethernet** *interface-number* command to access the Ethernet interface configuration view or run the **interface eth-trunk** *trunk-number* command to access the Trunk interface configuration view. 3. Run the **y1731 reset counter** command.
Configure the AIS loss threshold of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view.

Purpose	Procedure
	3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ais loss-threshold** { *loss-threshold* | **default** } command.
Configure the AIS transmission period of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ais-interval** { **1s** | **1min** } command.
Configure the CCM loss threshold of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ccm loss-threshold** { *loss-threshold* | **default** } command.
Configure the CCM transmission period of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **ccm-interval { 300Hz | 10ms | 100ms | 1s | 10s | 1min | 10min | default }** command.
Configure the activation time of a static RMEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **cross-check start-delay** { *start-delay-time* | **default** } command.
Configure the LCK loss threshold of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG.

Purpose	Procedure
	4. Run the **lock loss-threshold** { *loss-threshold* | **default** } command.
Configure the LCK transmission period of an MEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **lock-interval** { **1s** | **1min** } command.
Delete an RMEP or all RMEPs of a specified MEG or delete all RMEPs of an MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **no remote-mep** *mep-id* command. Or run the **no remote-mep all** command to delete all RMEPs of an MEG.
Delete all MEPs of a specified MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **no y1731 mep all** command.
Delete all MIPs of a specified MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **no y1731 mip all** command.
Configure the aging time of a dynamic RMEP	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **remote-mep aging-time** { *aging-time* | **default** } command.

Purpose	Procedure
Configure the aging time of LTR responses	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **trace-reply aging-time** { *aging-time* | **default** } command.
Clear the Y.1731 frame count of an MEG	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the **reset counter** command.
Configure the Sender ID TLV type of Y.1731 packets	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **y1731** command in the global configuration view to access the Y.1731 configuration view. 3. Run the **meg vlan** *vlan-id* **level** *level* **icc** *icc string* **umc** *umc string* command to access the configuration view of an existing MEG. 4. Run the command **senderid-tlv-type { none | chassis | manage | chassis-manage | defer }**.

Attached table:

Parameter	Description	Value
interface-number	Specifies the ID of a physical interface.	The value is an integer in the range of <1-12>/<1-48>.
trunk-number	Specifies an aggregation interface number.	The value is an integer ranging from 1 to 128.
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
level	Specifies an MA level.	The value is an integer ranging from 0 to 7.
mepid-id	Specifies an MEG corresponding to an MEP. The default MEP is an outward MEP.	The value is an integer ranging from 1 to 8191.

Parameter	Description	Value
loss-threshold	Specifies the AIS loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default AIS loss threshold.	3.5
loss-threshold	Specifies the CCM loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default CCM loss threshold.	3.5
start-delay-time	Specifies the activation time of a static RMEP.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default activation time.	0
loss-threshold	Specifies an AIS loss threshold.	The value is an integer ranging from 2 to 255.
default	Specifies the default LCK loss threshold.	3.5
aging-time	Specifies the aging time of a dynamic RMEP.	The value is an integer ranging from 1 to 65535, in seconds.
default	Specifies the default value.	1000s
aging-time	Specifies the aging time of LTR responses.	The value is an integer ranging from 1 to 65535.
default	Specifies the default aging time of LTR responses.	1000s

11.5.6 Configuring Y.1731 Fault Configuration

Purpose

This section describes how to send a test packet and receive the response packet to check whether the local device can ping the destination device when you need to manually check connectivity of a link between two devices.

Caution

If a local MEP in the up direction is associated with two or more MIPs, ensure that the network to which the MIPs are connected contains only one L2 data service channel (this is typically ensured by the STP protocol or an Ethernet ring protocol). Otherwise, the Y.1731 fault locating result is unpredictable.

Use this command to test whether a Y.1731 fault occurs. The test is performed on the root node of the switch. To stop sending LBM packets, press **Ctrl**+**C**.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure MAC address ping for locating a Y.1731 connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* ● **y1731 ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout* ● **y1731 ping mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
Configure remote MEP ping for locating a Y.1731 connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* ● **y1731 ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*

Purpose	Procedure
	● **y1731 ping remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-c** *packet-count* **-s** *packet-size* **-t** *packet-timeout*
Configure all remote MEP ping for locating a Y.1731 connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* ● **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-s** *packet-size* **-t** *packet-timeout* ● **y1731 ping all remote-mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-s** *packet-size* **-t** *packet-timeout*

Attached table:

Parameter	Description	Value
vlan-id	Specifies the VLAN ID to be mapped to an MA.	The value is an integer ranging from 1 to 4094.
level	Specifies an MA level.	The value is an integer ranging from 0 to 7.
mep-id	Specifies an MEP ID.	The value is an integer ranging from 1 to 8191.
remote-mep-id	Specifies a remote MEP ID.	The value is an integer ranging from 1 to 8191.
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-size	Specifies the size of a sent ping packet, including the size of the L2 packet header.	The value is an integer ranging from 64 to 1518.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60.
packet-count	Specifies the times of ping.	The value is an integer ranging from 1 to 1024.

11.5.7 Configuring Y.1731 Fault Locating

Purpose

This section describes how to send a test packet and receive the response packet to check whether the route from the local device to the destination device is reachable or locate the fault point when you need to manually check connectivity of a link between two devices.

Caution

To associate with two or more local UP MEPs, ensure that the network connecting the MIP has only one L2 data service channel, which is generally guaranteed by the spanning tree or Ethernet ring protocol. Otherwise, the Y.1731 fault locating result is unpredictable.

Configure the Y.1731 fault locating to be performed on the root node of the device, and the trace result to be automatically displayed after the timeout interval is set. To terminate the trace operation in advance, press Ctrl+C.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure MAC address tracing for locating a Y.1731 connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-t** *packet-timeout* ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **t** *packet-timeout* ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **ttl** *ttl-value* ● **y1731 trace mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-ttl** *ttl-value*

Purpose	Procedure
Configure remote MEP tracing for locating a Y.1731 connectivity fault	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-t** *packet-timeout* ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **-t** *packet-timeout* ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* **ttl** *ttl-value* ● **y1731 trace remote-mep** *remote-mep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **ttl** *ttl-value*

Attached table:

Parameter	Description	Value
mac-address	Specifies the MAC address of a remote MEP or MIP.	The value is in the AA:BB:CC:DD:EE:FF format, where A to F are hexadecimal digits.
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
level	Specifies a level.	The value is an integer ranging from 0 to 7.
remote-mep-id	Specifies the MEP ID of a remote network bridge.	The value is an integer ranging from 1 to 8191.
mep-id	Specifies the MEP ID of the Trace action initiated by the local network bridge.	The value is an integer ranging from 1 to 8191.
priority	Specifies a priority.	The value is an integer ranging from 0 to 7.
packet-timeout	Specifies a wait timeout duration of response packets.	The value is an integer ranging from 1 to 60, in seconds. The default value is 5 seconds.
ttl-value	Specifies the maximum number of hops for Trace.	The value is an integer ranging from 1 to 255. The default value is 64.

11.5.8 Configuring Bidirectional Throughput Test

Purpose

This section describes how to configure bidirectional throughput test to test the throughput between links of physical interfaces of a pair of MEPs.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure bidirectional throughput test	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 lbtst-throughput mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* -s *packet-size* ● **y1731 lbtst-throughput mac** *mac-address* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **priority** *priority* -s *packet-size*
	1. Remain in the current privileged user view. 2. Run the following commands: ● **y1731 lbtst-throughput remote-mep** *remotemep-id* **mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* **-s** *packet-size* ● **y1731 lbtst-throughput remote-mep** *remotemep-id* **mep vlan** *vlan-id* **level** ***level*** **mepid** *mep-id* **priority** *priority* **-s** *packet-size*

11.5.9 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the Y.1731 function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable debugging of Y.1731 interface packets	1. Remain in the current privileged user view. 2. Run the following commands: ● **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out**

Purpose	Procedure
	| dmr-in | dmm-out | dmm-in | exp | vsp | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet } *interface-number* ● **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface eth-trunk** *trunk-number*
Disable debugging of Y.1731 interface packets	1. Remain in the current privileged user view. 2. Run the following commands: ● **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all } interface eth-trunk** *trunk-number*
Enable debugging of the Y.1731 module	1. Remain in the current privileged user view. 2. Run the command **debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all }**.
Disable debugging of the Y.1731 module	1. Remain in the current privileged user view. 2. Run the command **no debug y1731 packet { ccm-out | ccm-in | lbr-out | lbr-in | lbm-out | lbm-in | ltr-in | ltr-out | ltm-in | ltm-out | ais-out | ais-in | lock-out | lock-in | tst-out | tst-in | mcc-out | mcc-in | lmr-out | lmr-in | lmm-out | lmm-in | 1dm | dmr-out | dmr-in | dmm-out | dmm-in | exp | vsp | all }**.
View the Y.1731 global configuration	1. Run the **disable** command to access the common user view. 2. Run the **show y1731** command.

Purpose	Procedure
View the summary or details of an MEP CCDB	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 ccdb** or **show y1731 ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
View the Y.1731 configuration file information	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 config** command.
View the error CCDB summary of all MEPs configured for the switch or the error CCDB details of a specified MEP	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 error ccdb or show y1731 error ccdb** *remote-mep-id* **vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
View all MEGs configured for the switch	1. Run the **disable** command to access the common user view. 2. Run the following commands: ● **show y1731 meg** ● **show y1731 meg vlan** *vlan-id* **level** *level*
View the summary and details of an MEP	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 mep** or **show y1731 mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.
View information about all MIPs configured for the switch	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 mip** command.
View Y.1731 frame statistics on an interface	1. Run the **disable** command to access the common user view. 2. Run the following commands: ● **show y1731 pdu-statistic interface** or **show y1731 pdu-statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show y1731 pdu-statistic interface eth-trunk** *trunk-number*
View the summary of all remote MEPs configured for the switch or the details of a remote MEP	1. Run the **disable** command to access the common user view. 2. Run the **show y1731 remote-mep or show y1731 remote-mep vlan** *vlan-id* level *level* **mepid** *mep-id* command.
View the results of the last query about fault locating for an MEP configured for the switch	1. Run the **disable** command to access the common user view. 2. Run the s**how y1731 trace-result mep vlan** *vlan-id* **level** *level* **mepid** *mep-id* command.

11.5.10 Configuration Example

Network Requirements

This example shows how to configure Y.1731 connectivity fault management in multiple MEGs.

Allocate wh-s4608, cs-s3628, nc-s3628, hf-s3628, and zz-s3628 to the MEG **icc v1 umc fhn1** and configure the MEG level to 1.

Allocate cd-s2200, gz-s2200, sh-s2200, and bj-s2200 to the MEG **icc v1 umc fhn6** and configure the MEG level to 6. Since this MEG has a level higher than **icc v1 umc fhn1**, Y.1731 packets of **icc v1 umc fhn6** can transparently pass through **icc v1 umc fhn1** and the two do not interfere with each other.

After dividing MEGs, determine the MEG boundaries according to Figure 11-14 and configure interfaces for MEPs in each MEG as long as that MEP IDs in the same MEG are not duplicate.

To enable Y.1731 fault management for a maintenance entity intermediate point, configure this point as an MIP. Configure MIPs of **icc v1 umc fhn6** at the interface of MEPs of **icc v1 umc fhn1**.

Network Diagram

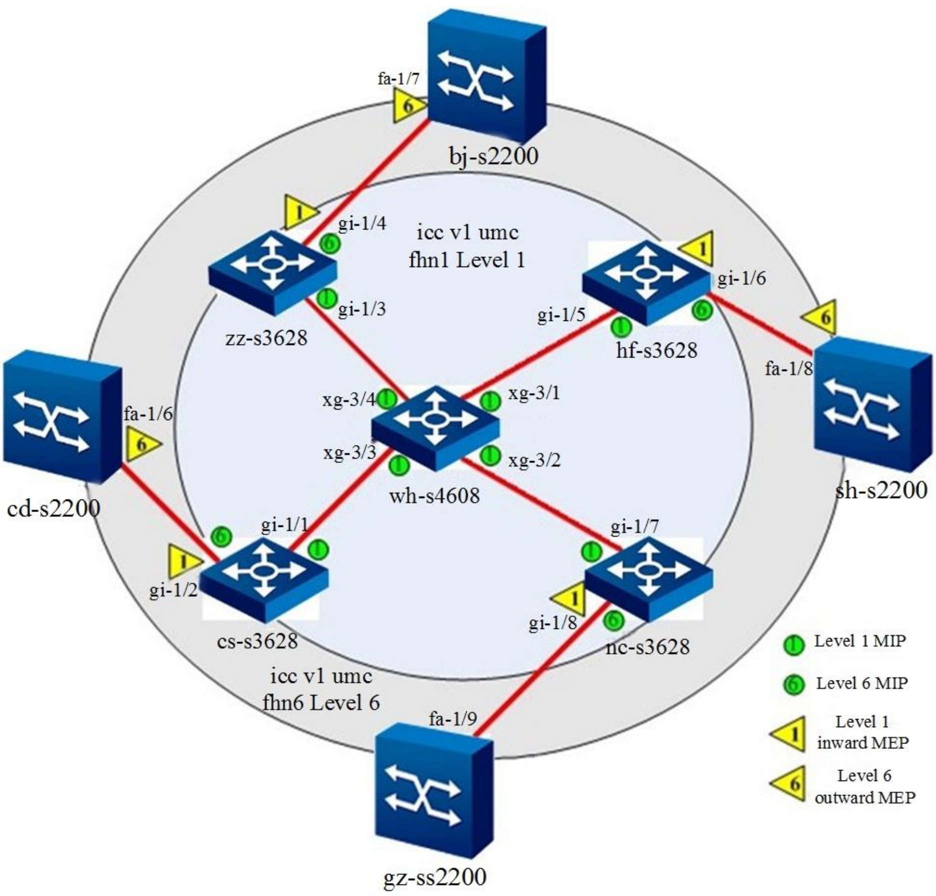


Figure 11-14 Y1731 configuration network diagram

Configuration

Configure each bridge as follows:

1. Configure **icc v1 umc fhn1**.

1) Configure wh-s4608

wh-s4608#configure
wh-s4608(config)#y1731
wh-s4608(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
wh-s4608(config-meg-v1-fhn1)#quit
wh-s4608(config)#interface xgigaethernet 3/0/1 to xgigaethernet 3/0/4
wh-s4608(config-xg3/0/1->xg3/0/4)#y1731 mip vlan 1 level 1

2) Configure cs-s3628

cs-s3628#configure
cs-s3628(config)#y1731
cs-s3628(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
cs-s3628(config-meg-v1-fhn1)#quit
cs-s3628(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
cs-s3628(config-meg-v1-fhn6)#quit
cs-s3628(config)#interface 10gigaethernet 1/0/1
cs-s3628(config-10ge1/0/1)#y1731 mip vlan 1 level 1
cs-s3628(config-10ge1/0/1)#quit
cs-s3628(config)#interface 10gigaethernet 1/0/2
cs-s3628(config-10ge1/0/2)#y1731 mip vlan 1 level 6
cs-s3628(config-10ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 inward
cs-s3628(config-10ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 ccm enable
cs-s3628(config-10ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 ais enable

3) Configure nc-s3628

nc-s3628#configure
nc-s3628(config)#y1731
nc-s3628(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
nc-s3628(config-meg-v1-fhn1)#quit
nc-s3628(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
nc-s3628(config-meg-v1-fhn6)#quit
nc-s3628(config)#interface 10gigaethernet 1/0/7
nc-s3628(config-10ge1/0/7)#y1731 mip vlan 1 level 1
nc-s3628(config-10ge1/0/7)#quit
nc-s3628(config)#interface 10gigaethernet 1/0/8
nc-s3628(config-10ge1/0/8)#y1731 mip vlan 1 level 6
nc-s3628(config-10ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 inward

nc-s3628(config-10ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 ccm enable
nc-s3628(config-10ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 ais enable

4) Configure hf-s3628
hf-s3628#configure
hf-s3628(config)#y1731
hf-s3628(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
hf-s3628(config-meg-v1-fhn1)#quit
hf-s3628(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
hf-s3628(config-meg-v1-fhn6)#quit
hf-s3628(config)#interface 10gigaethernet 1/0/5
hf-s3628(config-10ge1/0/5)#y1731 mip vlan 1 level 1
hf-s3628(config-10ge1/0/5)#quit
hf-s3628(config)#interface 10gigaethernet 1/0/6
hf-s3628(config-10ge1/0/6)# y1731 mip vlan 1 level 6
hf-s3628(config-10ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 inward
hf-s3628(config-10ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 ccm enable
hf-s3628(config-10ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 ais enable

5) Configure zz-s3628
zz-s3628#configure
zz-s3628(config)#y1731
zz-s3628(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
zz-s3628(config-meg-v1-fhn1)#quit
zz-s3628(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
zz-s3628(config-meg-v1-fhn6)#quit
zz-s3628(config)#interface 10gigaethernet 1/0/3
zz-s3628(config-10ge1/0/3)#y1731 mip vlan 1 level 1
zz-s3628(config-10ge1/0/3)#quit
zz-s3628(config)#interface10 gigaethernet 1/0/4
zz-s3628(config-10ge1/0/4)#y1731 mip vlan 1 level 6
zz-s3628(config-10ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 inward
zz-s3628(config-10ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 ccm enable
zz-s3628(config-10ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 ais enable

2. Configure **icc v1 umc fhn6**.
6) Configure cd-s2200
cd-s2200#configure
cd-s2200(config)#y1731
cd-s2200(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6

cd-s2200(config-meg-v1-fhn6)#quit
cd-s2200(config)#interface fastethernet 1/0/6
cd-s2200(config-fe1/0/6)#y1731 mep vlan 1 level 6 mepid 1
cd-s2200(config-fe1/0/6)#y1731 mep vlan 1 level 6 mepid 1 ccm enable

7) Configure gz-s2200
gz-s2200#configure
gz-s2200(config)#y1731
gz-s2200(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
gz-s2200(config-meg-v1-fhn6)#quit
gz-s2200(config)#interface fastethernet 1/0/9
gz-s2200(config-fe1/0/9)# y1731 mep vlan 1 level 6 mepid 10
gz-s2200(config-fe1/0/9)#y1731 mep vlan 1 level 6 mepid 10 ccm enable

8) Configure sh-s2200
sh-s2200#configure
sh-s2200(config)#y1731
sh-s2200(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
sh-s2200(config-meg-v1-fhn6)#quit
sh-s2200(config)#interface fastethernet 1/0/8
sh-s2200(config-fe1/0/8)#y1731 mep vlan 1 level 6 mepid 100
sh-s2200(config-fe1/0/8)#y1731 mep vlan 1 level 6 mepid 100 ccm enable

9) Configure bj-s2200
bj-s2200#configure
bj-s2200(config)#y1731
bj-s2200(config-y1731)# meg vlan 1 level 6 icc v1 umc fhn6
bj-s2200(config-meg-v1-fhn6)#quit
bj-s2200(config)#interface fastethernet 1/0/7
bj-s2200(config-fe1/0/7)#y1731 mep vlan 1 level 6 mepid 1000
bj-s2200(config-fe1/0/7)#y1731 mep vlan 1 level 6 mepid 1000 ccm enable

11.6 Configuring G.8032

11.6.1 Overview of G.8032

Advantages of G.8032

ITU-T G.8032 defines the automatic protection switching mechanism of Ethernet ring network and overcomes two weaknesses of IETF RFC3619 EAPS:

- In case of loss of fault notification or failure of triggering fault notification, the polling mechanism takes a long time to detect and discover the fault, and cannot meet the protection switching time requirement of 50 ms.
- If the link fault is unidirectional, the polling mechanism may fail to detect the fault and does not trigger protection switching.

Basic Concepts of G.8032

Under normal conditions, a blocked link must be set in the ring network to prevent loops. When other link is faulty, the blocked link is enabled and traffic is switched to the path at the other end of the ring for transmission to implement protection switching. In ITU-T G.8032, the blocked link is called a ring protection link (RPL), and the two nodes on both ends used for blocking this link are called RPL owner and RPL node respectively. The nodes communicate via the RAPS packets, and the channel used for transmitting RAPS packets is called RAPS channel. Service traffic is transmitted in the traffic channel, which has the same forwarding status as the RAPS channel. G.8032 provides simple loop protection and implements multi-level loop protection via the sub-ring model.

G.8032 Terms

- Ethernet ring: A ring that physically corresponds to an Ethernet topology formed by connected ring nodes. It is a set of Ethernet switches that are interconnected to form a ring.
- ERP instance: An entity that protects a VLAN set on the Ethernet ring.
- Interconnection node: It connects multiple rings.
- Major ring: It is an Ethernet ring that connects two ports of interconnection nodes.
- R-APS virtual channel: It is the R-APS signaling channel of a sub-ring between interconnection nodes.
- Ring MEL: It is the level of the MEG that corresponds to the R-APS signaling channel of a ring.

- Ring protection link (RPL): A blocked link on a ring. When another link fails, this link is unlocked to take over traffic forwarding from the failed link.
- RPL neighbor node: A node that blocks a port of RPL.
- RPL owner node: It connects to one end of the RPL and controls the RPL's forwarding status.
- Sub-ring: A sub-ring is formed when a ring or network is connected to another ring or network via interconnection nodes. The sub-ring is not closed, and interconnection nodes do not belong to the sub-ring.
- Sub-ring link: A link connecting nodes on a sub-ring.
- Wait to block (WTB) timer: It is used by the RPL owner node to delay recovery after manual or forced switching is cleared.

Ring Protection Parameters

1. In G.8032, a ring node has five states.
   1) Pending state: A state prior to recovery to the normal state.
   2) Idle state: Indicates no protection request exists in the loop.
   3) Protect state: Indicates a link of the loop is faulty.
   4) Manual switch state: Indicates manual protection switching.
   5) Forced switching: Indicates forced protection switching.
2. Ring-based protection switching is triggered in two modes: link protection request and manual protection request.
   - Link protection request includes:
   1) Signal fail (SF): Indicates a link is faulty.
   2) No request (NR): Indicates there is no local protection request.
   - A manual protection request is served in command line mode and includes:
   1) Forced switch (FS): This command blocks the request initiating port to enable service switching.
   2) Manual switch (MS): It blocks the request initiating port to enable service switching if the Ethernet ring is free of link faults or is not in the FS state. The priority is relatively low.

3) Clear: This command has the following functions: a. Clears the manual protection request command FS or MS; b. Recovers to the normal state before the WTR or WTB timer times out if recovery is permitted; c. Triggers loop recovery in irrecoverable mode.

3. G.8032 defines two protection switching modes: recoverable and irrecoverable.

11.6.2 G.8032 Fault Detection Mechanism

G.8032 uses the continuity and connectivity check (CC) defined in Y.1731 or IEEE 802.1ag to perform bidirectional forwarding detection of links, which can locate the fault and check whether the fault is unidirectional or bidirectional. When used for protection switching, the CC frame has a default transmission period of 3.33 ms (transmission rate of 300 frames per second), as shown in Figure 11-15.

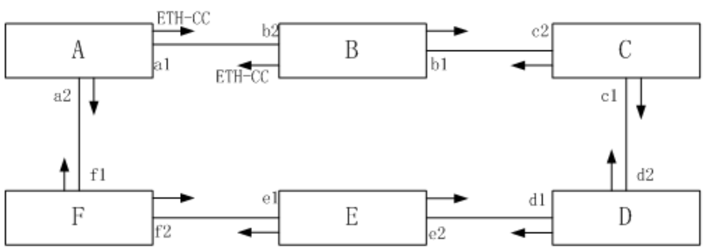


Figure 11-15 Neighboring nodes sending CC frames for fault detection

Two neighboring nodes periodically send CC frames from a physical port for fault detection. When one node detects CC frame loss in the specific time, a fault is detected. If Node A and Node B cannot receive the CC frame sent by each other, the respective ports a1 and b2 are faulty, as shown in Figure 11-16.

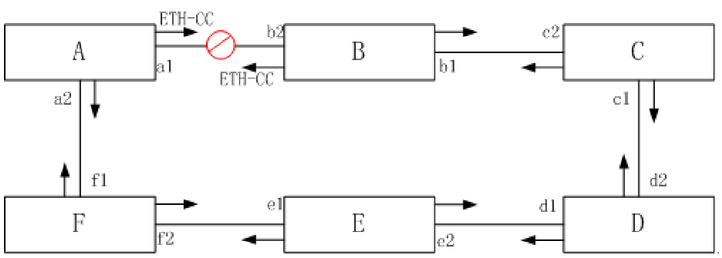


Figure 11-16 Detecting CC frame loss

The node sends the remote defect indication (RDI) frame from the port with a fault detected. If the fault is unidirectional, the downlink node of the link detects the RDI frame. Node B detects the CC frame loss of Node A, detects the fault of port b2, and advertises the RDI to Node A, as shown in Figure 11-17.

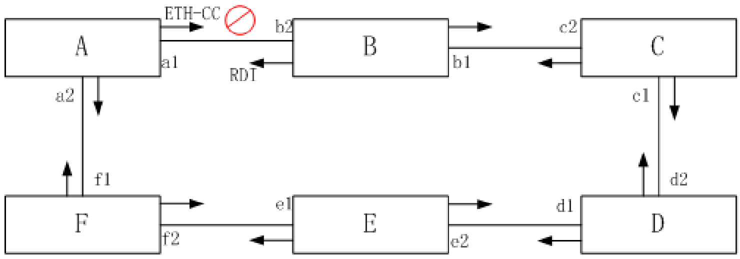


Figure 11-17 Unidirectional link fault detection

If the node is faulty, the neighboring nodes at both ends of the faulty node detect CC frame loss in the specific time, as shown in Figure 11-18.

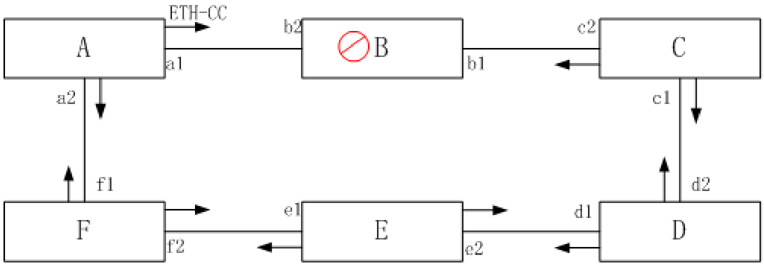


Figure 11-18 Node fault

11.6.3 G.8032 Single-ring Protection Switching

The RPL is blocked in normal state, as shown in Figure 11-19.

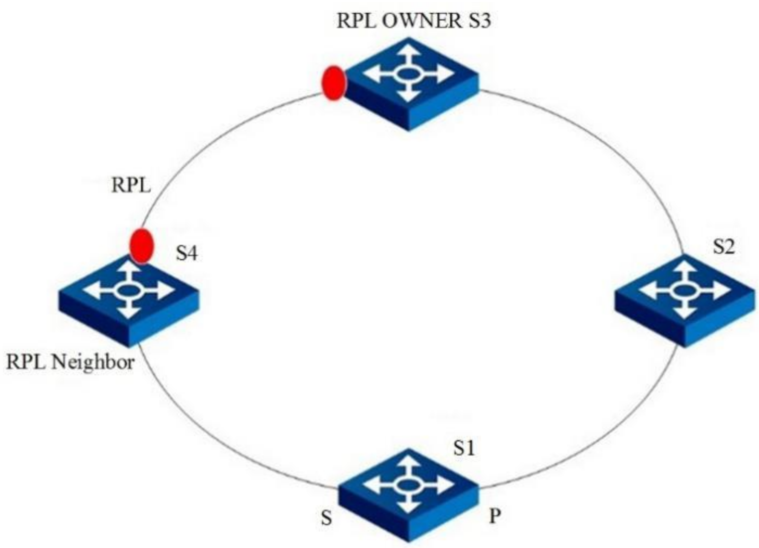


Figure 11-19 Singe-ring link normal state

Loop switching can be performed in three modes: forced switch, link failure, and manual switch, in descending order of priority.

11.6.3.1 Forced Switch

When the loop is in idle state, if forced switch is performed on a node of the ring, the port is blocked and the other port is enabled. If the other port has been enabled, no processing is performed on this port. If no command of a higher priority is executed, the FS message is sent from both ports and MAC addresses are updated.

After other nodes of the ring receive the RAPS-MS message, if there is no request of a higher priority, the nodes enable all non-failing blocked ports and update MAC addresses according to the corresponding mechanism. In this way, the RPL is enabled and switching is complete.

Figure 11-19 shows the loop in normal state. After forced switch is performed on the S port of S1, this port is blocked and a RAPS-FS message is sent to notify other nodes of the ring. After receiving the RAPS-FS message, the owner node enables the RPL blocked port to switch traffic to the RPL. Switching is complete, as shown in Figure 11-20.

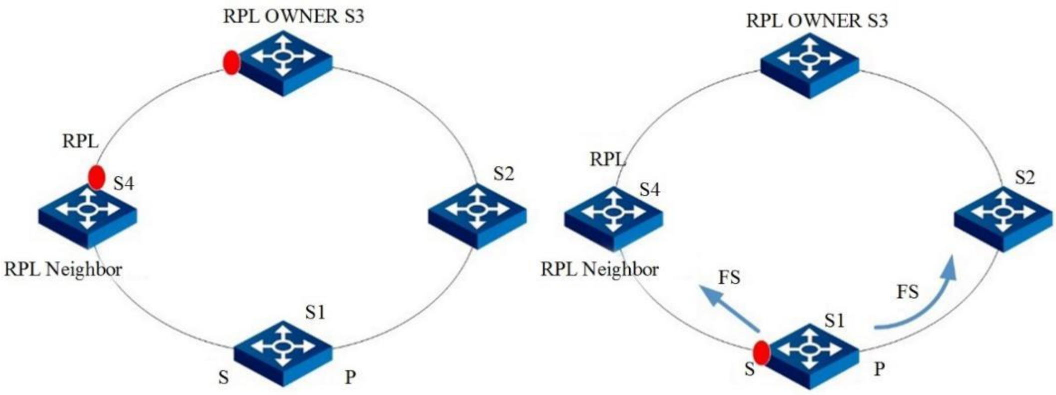


Figure 11-20 State change after forced switch on S1 in idle state

Caution

1. If the forced switch command has been entered on one port of a node, forced switch cannot be performed on the other port. As shown in Figure 5, after forced switch is performed on the S port of S1, forced switch cannot be performed on the P port.

2. If forced switch has been performed on a node of the loop, forced switch can still be performed on other nodes. However, this causes multiple links of the loop to be blocked, resulting in traffic interruption.

The forced switch state can be cleared using the **Clear** command. After S1 receives the **Clear** command, it still blocks the S port and sends an NR message.

In recoverable mode, the RPL owner node starts the WTB timer after receiving the RAPS-NR message. The WTB Expires signal is generated after the WTB timer times out. After receiving the signal, the owner node blocks the RPL port and sends the NR and RB messages. Other nodes receive the NR and RB messages and enable non-failing blocked ports. The loop recovers to idle state.

In irrecoverable mode, the RPL owner node does not perform processing after receiving the RAPS-NR message. If the **Clear** command is manually entered on the RPL owner node, the irrecoverable mode is cleared and processing is initiated in recoverable mode.

11.6.3.2 Automatic Protection Switching via Link Failure Detection

When a link failure is detected, the faulty port is blocked and the SF signal is sent. Other nodes of the ring receive the RAPS-SF signal and enable non-failing ports. In this way, the RPL owner node enables the blocked port to switch traffic to the RPL link. Protection switching is complete. The ring runs in protected state, as shown in Figure 11-21.

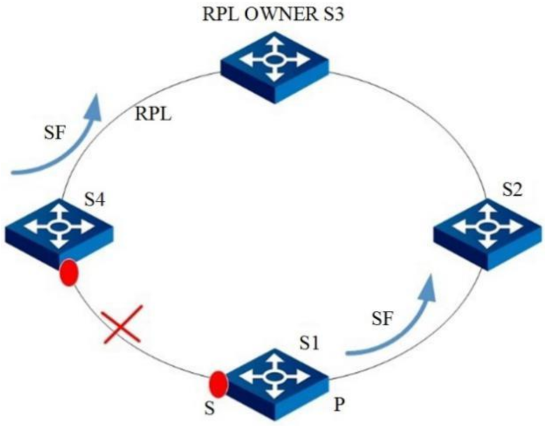


Figure 11-21 Ring status upon link fault

In recoverable mode, after the faulty link recovers, the two neighboring nodes at both ends of the link still block ports and send the RAPS (NR) message to notify that the fault is cleared. Other ring nodes receive and forward the RAPS (NR) message. After receiving the RAPS (NR) message, the RPL owner node starts the WTR timer, blocks the RPL port when the timer times out, and sends the RAPS (NR, RB) message. At this time, the ring is in pending state, as shown in Figure 11-22.

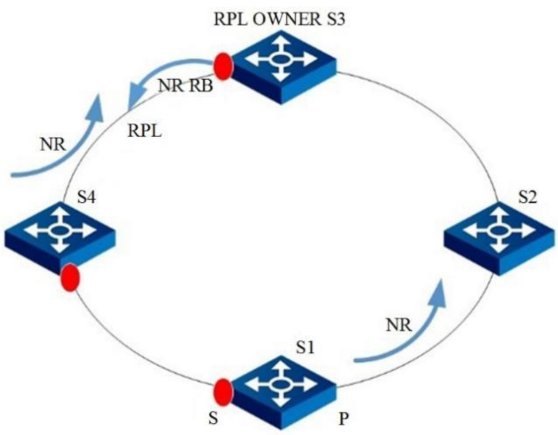


Figure 11-22 RPL Owner node blocks the RPL port and sends a notification when the link recovers

After receiving the RAPS (NR, RB) message, other nodes of the ring update FDB and cancel port blocking, and the non-RPL owner node at the other end of the RPL blocks the RPL port and updates FDB. The ring recovers to idle state, as shown in Figure 11-23.

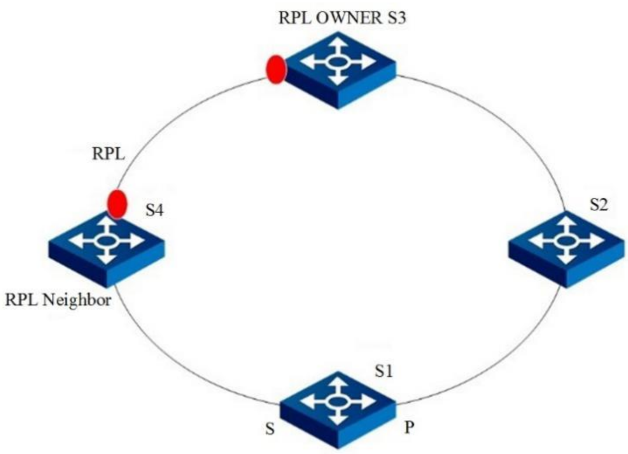


Figure 11-23 Ring recovers to the idle state after the WTR timer times out

In irrecoverable mode, after the faulty link recovers, the two neighboring nodes at both ends of the link still block ports and send the RAPS-NR message to notify that the fault is cleared. Other nodes receive the RAPS-NR messages and perform no processing. The ring is still in pending state.
If the **Clear** command is manually entered, the irrecoverable mode is cleared and processing is initiated in recoverable mode.

11.6.3.3 Manual Switch

When the loop is in idle state, if manual switch is performed on a node of the ring, the port is blocked and the other port is enabled. If the other port has been enabled, no processing is performed on this port. If no command of a higher priority is executed, the MS message is sent from both ports and MAC addresses are updated.
After other nodes of the ring receive the RAPS-MS message, if there is no request of a higher priority, the nodes enable all non-failing blocked ports and update MAC addresses according to the corresponding mechanism. In this way, the RPL is enabled and switching is complete.
Figure shows the loop in normal state. After manual switch is performed on the S port of S1, this port is blocked and a RAPS-MS message is sent to notify other nodes of the ring. After receiving the RAPS-MS message, the owner node enables the RPL blocked port to switch traffic to the RPL. Switching is complete, as shown in Figure 11-24.

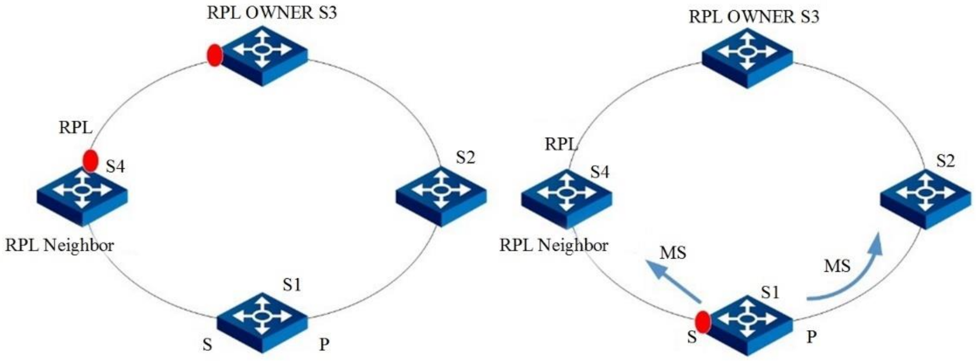


Figure 11-24 State change after manual switch on S1 in idle state

Caution

1. If manual switch is performed on other nodes when the ring is in manual switch state, the switch request is denied.

2. If the node that initiates the manual switch request receives a command of a higher priority, it clears the manual switch request and processes the request of a higher priority. Manual switch has the lowest priority.

The manual switch state can be cleared using the **Clear** command. After S1 receives the **Clear** command, it still blocks the S port and sends an NR message.

In recoverable mode, the RPL owner node starts the WTB timer after receiving the RAPS-NR message. The WTB Expires signal is generated after the WTB timer times out. After receiving the signal, the owner node blocks the RPL port and sends the NR and RB messages. Other nodes receive the NR and RB messages and enable non-failing blocked ports. The loop recovers to idle state.

In irrecoverable mode, the RPL owner node does not perform processing after receiving the RAPS-NR message. If the Clear command is manually entered on the RPL owner node, the irrecoverable mode is cleared and processing is initiated in recoverable mode.

11.6.4 G.8032 Multi-ring Protection Switching Mechanism upon Single Point of Failure

G.8032 can provide link protection switching for the multi-ring topology where rings are intersecting via a single-point or multi-ring topology where rings are connected via a shared link. For the multi-ring topology where rings are intersecting via a single point, the protection switching of each ring complies with the protection switching mechanism of a simple ring. The multi-ring topology where rings are connected via a shared link can be divided into major ring and sub-ring. The shared link belongs to the major ring, the nodes at both ends of the shared link are called interconnection nodes, and the section between interconnection nodes in the sub-ring is called the sub-ring link. The virtual link of the sub-ring in the major ring via interconnection nodes and the sub-ring link constitute a closed ring. See Figure 11-24 for details.

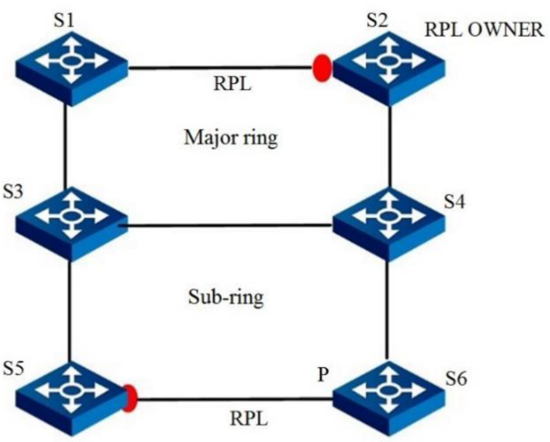


Figure 11-25 Intersecting ring without link fault

In Figure 11-25, S3 and S4 are interconnection nodes, and the link between S3 and S4 is a shared link that belongs to the major ring. S1-S2-S4-S3-S1 is a link of the major ring. The sub-ring is not a closed loop. The sub-ring link is S5-S6. The sub-ring, together with the sub-ring link and the virtual link of the major ring, forms a ring. The virtual link is a redundant link of the major link and connects interconnection nodes. The major ring and sub-ring must be configured with the RPL owner node respectively; otherwise, a loop is formed.

If the shared link fails, the major link handles the failure because the shared link belongs to the major ring. Similar to single-ring link failure handling, the major link enables the RPL blocked port to switch traffic. The sub-ring does not take any action, as shown in 11-26.

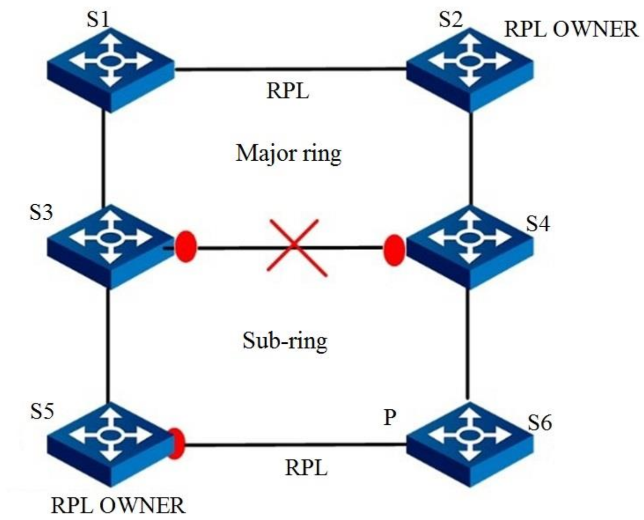


Figure 11-26 Shared link fault

If the sub-ring link fails, the failure is also handled according to the single-ring failure protection switching mechanism.

Forced switch and manual switch are also applicable to the multi-ring topology, and the handling mechanism is the same as the single-ring handling mechanism.

11.6.5 G.8032 Intersecting Ring Protection Switching Mechanism upon Multi-Point Fault

11.6.5.1 Virtual Link Fault Detection Mechanism

G.8032 uses the continuity and connectivity check (CC) defined in Y.1731 to perform bidirectional forwarding detection of links, which can locate the fault and check whether the fault is unidirectional or bidirectional. When used for protection switching, the CC frame has a transmission period of 3.33 ms.

A virtual link is a link connecting interconnection nodes. As shown in Figure 11-27, there are two virtual links: C-D, and C-A-B-D. If the link C-D fails, the major ring enters the protected state and the sub-ring state remains unchanged. If any link among nodes C, A, B, and D fails before the link C-D is restored, a virtual link fault occurs. In this case, the sub-ring enters the protected state and nodes on the major ring communicate with each other through the sub-ring.

According to Y.1731, if a node does not receive a CC response from the peer end within a time 3.5 times of the CC sending interval, the link fails. In actual situations, the ring can hardly perform protection switching within 10 ms (3.33 x 3.5). Then, a problem occurs. As shown in Figure 11-27, if the major ring does not enter the protected state within 10 ms after the C-D link fails, CC determines that the link A-B in the major ring fails. Then, the sub-ring regards that the virtual link fails and enters the protected state. When the major ring completes protection switching, a ring of A-C-E-F-D-B-A will be formed, that is, a super-ring.

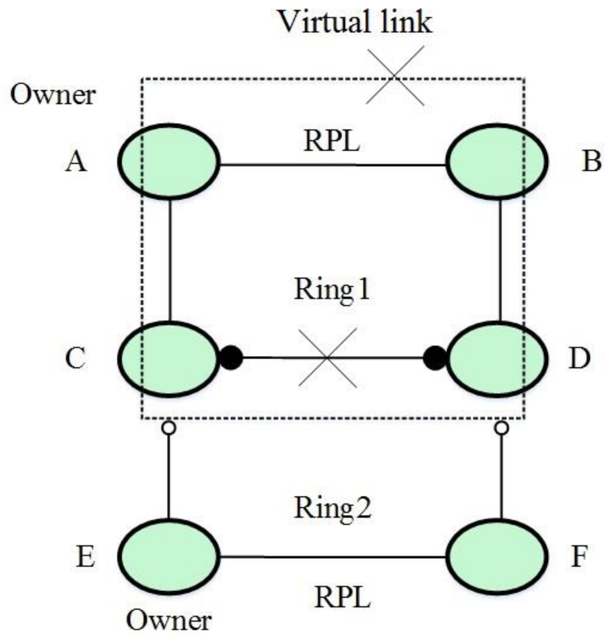


Figure 11-27 Generation of a super-ring when the major rink link fails

To avoid this problem, a holdoff timer is added to the original detection mechanism. As shown in Figure 11-27, the holdoff timer is started when the ring detects a virtual link fault. Sub-ring does not perform any action during the running period of the timer, so that the major ring has sufficient time to complete protection switching. This can avoid the above problem. If a link fault is still detected after the timer times out, the fault is advertised as usual.

11.6.5.2 Protection Switching Mechanism upon Multiple Points of Failure

When a virtual link fails, the sub-ring enters the protected state and nodes on the major ring communicate with each other through the sub-ring.

When the virtual link is restored, to avoid generation of a super-ring, when the interconnected nodes C and D detect that the virtual link is restored, they block ports c3 and d3 and advertise RAPS (NR), and the node E serves as an RPL owner and starts a WTR timer, as shown in Figure 11-28.

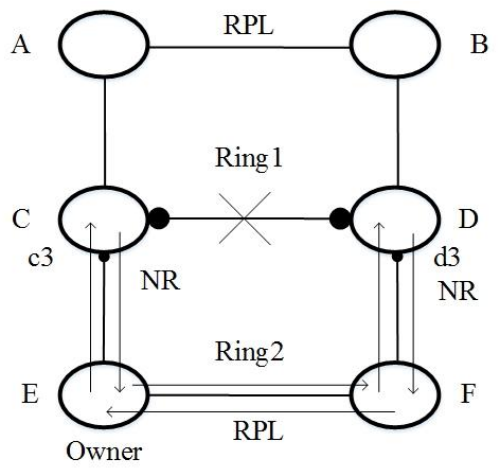


Figure 11-28 Sub-ring message advertisement on the virtual link

Then, since C and D have blocked c3 and c4, the sub-ring virtual link disconnects from the major ring. To solve this problem, a new mechanism is introduced. When a ring node receives the RAPS (NR) or RAPS (SF) message, if the MAC address of the peer is greater than its own MAC address, the node opens non-faulty blocked ports. According to the introduced new mechanism, after receiving the RAPS (NR) message, nodes C and D compare their own MAC addresses with peer ends' MAC addresses. If the MAC address of node D is greater than that of node C, node c opens port c3, as shown in Figure 11-29.

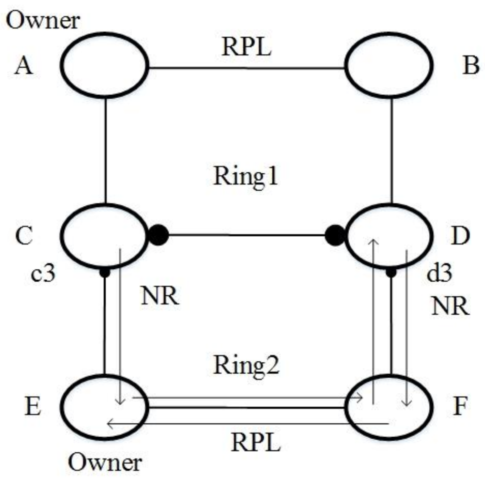


Figure 11-29 Island link prevention during virtual link recovery

When the WTR of node E times out, the RPL port is blocked and the RAPS (NR, RB) message is advertised. The system processes the problem as a simple ring recovery process. In this way, virtual link protection is implemented.

11.6.6 Configuring the Basic G.8032 Functions

Purpose

This section describes how to configure the basic functions of G.8032.

Prerequisite

All links are up; otherwise, the G.8032 instance to be configured is in Protect state and manual switch cannot be performed on a port of the instance.

Run the **show g8032 instance** command and the information shows that the G.8032 instance is activated; otherwise, the interface cannot be configured to port1 or port2 of the instance.

The network topology is a single ring; otherwise, the switch does not need to be configured with a virtual channel. If a virtual channel is configured, VC-mep must be configured and then the G.8032 instance can be activated.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a node role for a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* role { **rpl-owner-node** | **neighbor** | **none** } command.
Configure a control channel for a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **channel** *channel-number* command.
Configure a VLAN list mapped to a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **vlan** *vlan-list* command.
Delete a VLAN list mapped to a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **no g8032 instance** *instance-num* **vlan** *vlan-list* command.
Configure Port 1 or Port 2 of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the following commands: ● **g8032 instance** *instance-num* **{ port1 | port2 } { gigaethernet | xgigaethernet }** *interface-number* ● **g8032 instance** *instance-num* **{ port1 | port2 } eth-trunk** *trunk-number*
Perform forced switch on a port of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view.

Purpose	Procedure
	3. Run the **g8032 instance** *instance-number* { **port1** | **port2** } **fs** command.
Perform manual switch on a port of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* { **port1** | **port2** } **ms** command.
Configure an RPL port for a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **rpl** { **port1** | **port2** | **none** } command.
Configure a virtual channel for a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **virtual-channel** *virtual-channel-number* command.

11.6.7 Configuring the G.8032 Timer Parameters

Purpose

This section describes how to configure the G.8032 timer parameters to adapt the timer to the network demand.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the timeout duration of the virtual channel hold-off timer of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-num* **vc-holdoff-timer** { *vc-holdoff-timer* | **default** } command.

Purpose	Procedure
Configure the WTR timer cycle of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **wtr-timer** { *wtr-timer* | **default** } command.
Configure the guard timer cycle of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **guard-timer** { *guard-timer* | **default** } command.
Configure the hold-off timer cycle of a G.8032 instance	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **hold-off-timer** { *hold-off-timer* | **default** } command.

11.6.8 Maintenance and Debugging

Purpose

This section describes how to configure the G.8032 optional functions according to the actual condition.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose

This section describes how to check, debug or locate the fault when the G.8032 function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**.

Purpose	Procedure
Enable G.8032 debugging	1. Remain in the current privileged user view. 2. Run the **debug g8032** { **in** | **out** | **packet** | **sm** | **timer** | **event** | **all** } command.
Disable G.8032 debugging	1. Remain in the current privileged user view. 2. Run the **no debug g8032** { **in** | **out** | **packet** | **sm** | **timer** | **event** | **all** } command
View all information about a G.8032 instance	1. Run the **disable** command to return to the common user view, or run the **configure** command to access the global configuration view, or run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-numbe* or **g8032** command in the global configuration view to access the G.8032 configuration view, or remain in the current privileged user view. 2. Run the **show g8032** command.
View the information about a G.8032 instance or all instances	1. Run the **disable** command to return to the common user view, or run the **configure** command to access the global configuration view, or run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-numbe* or **g8032** command in the global configuration view to access the G.8032 configuration view, or remain in the current privileged user view. 2. Run the **show g8032 instance** *instance-num* **or show g8032 instance** command.
View the interface information of a G.8032 instance	1. Run the **disable** command to return to the common user view, or run the **configure** command to access the global configuration view, or run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-numbe* or **g8032** command in the global configuration view to access the G.8032 configuration view, or remain in the current privileged user view. 2. Run the **show g8032 instance** *instance-num* **interface or show g8032 instance interface** command.
View information about a G.8032 interface	1. Run the **disable** command to return to the common user view, or run the **configure** command to access the global configuration view, or run the **interface** { **gigaethernet** | **xgigaethernet** } *interface-numbe* or **g8032** command in the global configuration view to access the G.8032 configuration view, or remain in the current privileged user view. 2. Run the **show g8032 interface** command.
Clear the G.8032 instance status	1. Run the **configure** command in the privileged user view to access the global configuration view. 2. Run the **g8032** command to access the G.8032 configuration view from the global configuration view. 3. Run the **g8032 instance** *instance-number* **clear** command.

11.7 Configuring UDLD

11.7.1 Configuring UDLD Functions

Purpose

This section introduces how to configure the basic UDLD functions for unidirectional link fault detection.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a UDLD working mode	1. Run the **configure** command to access the global configuration view. 2. Run the **udld work-mode { normal | aggressive }** command.
Configure the interface shutdown mode for unidirectional links	1. Run the **configure** command to access the global configuration view. 2. Run the **udld uni-shutdown { manual | auto }** command.
Set the sending interval for Advertisement packets	1. Run the **configure** command to access the global configuration view. 2. Run the **udld advertise-interval** { *adver-interval* | **default** } command.
Enable or disable the UDLD protocol on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **udld** { **enable** | **disable** } command.
Enable or disable the UDLD aggressive mode on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **udld aggressive { enable | disable }** command.
Enable or disable the verification code type on an interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** } *interface-number* command to access the interface configuration view.

Purpose	Procedure
	3. Run the **udld cisco-checksum { enable | disable }** command.
Configure an UP delay time for UDLD interfaces globally	1. Run the **configure** command to access the global configuration view. 2. Run the **udld global up-delay** { *delay-value* | **default** } command.
Configure an Rx event listening mode for a UDLD interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **udld rxmode { normal | rxloss }** command.
Configure an UP delay time for a UDLD interface	1. Run the **configure** command to access the global configuration view. 2. Run the **interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** } *interface-number* command to access the interface configuration view. 3. Run the **udld up-delay** { *delay-value* | **default** } command.

11.7.2 Maintenance

Purpose

This section describes how to troubleshoot UDLD faults.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	**Procedure**
Display UDLD local information	1. Run the corresponding command to access the common user view. 2. Run the **show udld local** command.
Display UDLD interface information	1. Run the corresponding command to access the common user view. 2. Run the **show udld interface** command.
Display UDLD peer information	1. Run the corresponding command to access the common user view. 2. Run the **show udld peer** command.

Purpose	Procedure
Display the UDLD configuration	1. Run the corresponding command to access the common user view. 2. Run the **show udld config** command.

11.7.3 Configuration Example

Network Requirements

Switch 1 and Switch 2 are connected to each other with two pairs of fiber optical cables. Both switches support UDLD.

Assume that the link between the two switches fails and a unidirectional link is detected through the UDLD function. The unidirectional link is required to be disconnected automatically (in automatic mode).

Network Diagram

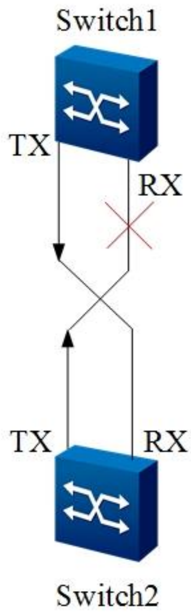


Figure 11-1 UDLD network diagram

Configuration Suggestion

Set the global shutdown mode to Automatic on Switch 1.

Set the global shutdown mode to Automatic on Switch 2.

Enable UDLD for gigaethernet 1/0/1 of Switch 1.

Enable UDLD for gigaethernet 1/0/2 of Switch 2.

Simulate the unidirectional status.

Configuration

Switch1:

Switch1(config)#udld uni-shutdown auto

Switch1(config)#interface 10gigaethernet 1/0/1

Switch1(config-ge1/0/1)#udld enable

Switch2:

Switch2(config)#udld uni-shutdown auto

Switch2(config)#interface 10gigaethernet 1/0/2
Switch2(config-10ge1/0/2)#udld enable

Chapter 12 Configuring Device Management

This chapter describes the basic content, configuration procedure, and configuration examples of the device management of the Switch.

12.1 Configuring Device Hardware

12.1.1 Overview

The hardware configuration for the Switch indicates the operations on the hardware resource using the commands during the device operation after the hardware is installed. The hardware resources include CPU, fan, memory, and temperature module.

Hardware configuration facilitates usage and improves the reliability of hardware resources.

12.1.2 Configuring the Device CPU

Purpose

This section describes how to configure the monitoring and alarm report functions and configure the upper and lower limits of CPU usage to understand the CPU running condition or control CPU usage.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the CPU monitoring function and CPU alarm reporting function	1. Access the global configuration view. 2. Run the **cpu monitor { enable | disable }** command to enable or disable the CPU monitoring function. 3. Run the **cpu all trap** { **enable** | **disable** } command to enable or disable the CPU alarm reporting function.
Set the upper and lower limits of CPU usage	1. Access the global configuration view. 2. Run the **cpu** { *cpu-number* | **all** } **low-threshold** *low-threshold* **high-threshold** *high-threshold* command.

Purpose	Procedure
Check the configuration result	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show cpu** command to view the CPU usage and configuration. 3. Run the **show cpu config** command to view the current configuration file information of the device CPU. 4. Run the **show cpu statistic** command to view CPU usage statistics.

12.1.3 Configuring the Device Fan

Purpose

This section describes how to set the fan speed threshold and to understand the current running condition of the device fan via the fan monitoring and alarm report functions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the fan monitoring and alarm reporting functions	1. Access the global configuration view. 2. Run the **fan monitor** { **enable** | **disable** } command to enable or disable the fan monitoring function. 3. Run the **fan** { *fan-number* | **all** } **trap** { **enable** | **disable** } command to enable or disable the fan alarm reporting function.
Set a fan speed threshold	1. Access the global configuration view. 2. Run the **fan** { *fan-number* | **all** } **threshold low-threshold** *low-threshold* **high-threshold** *high-threshold* command.
View the configuration result	1. Access the privileged user view or global configuration view. 2. Run the **show fan** command to view the fan status and configuration.

12.1.4 Configuring the Device Memory

Purpose

This section describes how to set the upper and lower limit of memory usage, and to understand the current memory usage of the device using the memory monitoring and alarm report functions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the memory monitoring and alarm reporting functions	1. Access the global configuration view. 2. Run the **memory monitor { enable | disable }** command to enable or disable the memory monitoring function. 3. Run the **memory** { *memory-pool-number* | **all** } **trap** { **enable** | **disable** } command to enable or disable the memory alarm reporting function.
Set the upper and lower limits of memory usage	1. Access the global configuration view. 2. Run the **memory** { *memory-pool-number* | **all** } **low-threshold** *low-threshold* **high-threshold** *high-threshold* command.
View the configuration result	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show memory pool** command to view the memory usage of all in-position cards.

12.1.5 Configuring the Device Temperature

Purpose

This section describes how to enable or disable alarm reporting upon device temperature change and configure the temperature threshold for triggering alarm reporting.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Set the temperature monitoring function and temperature alarm reporting function	1. Access the global configuration view. 2. Run the **temperature monitor** { **enable** | **disable** } command to enable or disable the temperature monitoring function. 3. Run the **temperature** { *temperature-number* | **all** } **trap** { **enable** | **disable** } command to enable or disable the temperature alarm reporting function.
View the configuration result	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show temperature** command to view the temperature information of all the cards and the fan. 3. Run the **show temperature config** command to view the device temperature configuration file information.
Configure a device temperature threshold	1. Access the global configuration view. 2. Run the **temperature** { *temperature-number* | **all** } **low-threshold** *low-threshold* **high-threshold** *high-threshold* command.

12.1.6 Viewing the Device CPU Usage

Purpose

You can run this command to display the device component type and system status.

Procedure

Perform the corresponding steps, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Display the current CPU usage	1. Access the common user view. 2. Run the **show cpu statistic** command.

12.1.7 Maintenance and Debugging

Purpose

This section describes how to debug the device hardware parameters and locate the fault.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the version information	1. Access the privileged user view or global configuration view. 2. Run the **show version** command.
View the power status	1. Access the common user view. 2. Run the **show power** command.

12.2 Configuring the Mirroring Function

12.2.1 Overview of Mirroring

Mirroring indicates copying data flows to a destination port. The mirroring technology is mainly used to implement the data flow monitoring function to eliminate network faults.

Switch supports Trunk mirroring and mirroring to Trunk.

Switch supports up to 8 observing interfaces.

Switch allows you to mirror packets of multiple ports to an observing interface.

Switch can run at most 3 observing interfaces at a time. If one port is used to mirror both upstream traffic and downstream traffic, it is deemed that 2 observing interfaces are used.

Switch allows you to mirror the inbound and outbound flows of a port to 2 different observing interfaces and does not support mirror mirrored packets.

12.2.2 Mirroring Classification

Switch supports port mirroring and flow mirroring.

Port mirroring includes local mirroring and remote mirroring.

- Local port mirroring, also called local switched port analyzer (SPAN), indicates that the source mirroring port and destination mirroring port are on the same switch.
- Remote port mirroring, also called remote SPAN (RSPAN), indicates that the source mirroring port and destination mirroring port are on different switches.

Note

- Source switch: Switch on which the monitored port is located. It mirrors traffic to the remote VLAN and forwards traffic to the intermediate switch via the L2 network.
- Intermediate switch: Switch located between the source switch and destination switch. It transmits traffic to the next intermediate switch or destination switch via the remote VLAN. If the source switch and destination switch are connected directly, the intermediate switch is not required.
- Destination switch: Switch on which the destination port of remote mirroring is located. It forwards the mirroring traffic received from the remote VLAN to the monitoring device via the mirroring destination port.

Flow mirroring includes mirroring to CPU and mirroring to port.

- Flow mirroring to CPU: Copies the message that complies with the match rules and passes through the interface configured with flow mirroring, and sends the message to the CPU for analysis and diagnosis.
- Flow mirroring to port: Copies the message that complies with the match rules and passes through the interface configured with flow mirroring, and sends the message to the destination port for analysis and diagnosis.

Note:

Similar to port mirroring, flow mirroring includes local flow mirroring and remote flow mirroring.

12.2.3 Configuring Local Port Mirroring

Purpose

This section describes how to configure the local port mirroring function to monitor or analyze the messages passing through a port on the device in the case that the source mirroring port and destination mirroring port are on the same device.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure local port mirroring	1. Access the global configuration view. 2. Run the following commands to create a local mirror group and its observation interface: ● **mirror group** *groupnum* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **mirror group** *groupnum* **eth-trunk** ***trunk-number*** **3. Access the interface configuration view or interface group configuration view**. 4. Run the **mirror** { **ingress** | **egress** | **both** } **group** *groupnum* command to enable the mirroring function on an interface at the mirroring source interface
Disable the local port mirroring function and delete the local mirror group and its observing interface	1. Access the interface configuration view or interface group configuration view. 2. Run the **no mirror** { **ingress** | **egress** | **both** } **group** *groupnum* command to cancel the mirroring function on the interface. 3. Access the global configuration view. 4. Run the **no mirror group** [*groupnum*] command to delete the local mirroring group and its observing interface.
View the configuration result	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Eth-Trunk), VLAN configuration view, or interface group configuration view. 2. Run the **show mirror config** command to view the configuration file information of the mirroring function. 3. Run the **show mirror group** command to view mirroring group information. 4. Run the **show mirror interface** command to view the mirrored port information.

12.2.4 Configuring Flow Mirroring

Purpose

This section describes how to configure the flow mirroring function to monitor or analyze the messages with some specific features that pass through the device.

Note:

Before configuring remote flow mirroring, make sure the L2 network between devices is connected or the L3 network is reachable.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure local flow mirroring	1. Access the global configuration view. 2. Run the following commands to create a local mirror group and its observation interface: ● **mirror group** *groupnum* **{ ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **mirror group** *groupnum* **eth-trunk** *trunk-number* 3. Run the **filter-list** *acl-number* [**name** *filter-name*] command to create an ACL and access the ACL view. 4. Select the proper flow classification rules according to the actual situation. For details, see chapter 7.1 "ACL Configuration." 5. Run the following commands to configure the flow mirroring action: ● **filter** *rule-number* **action mirror cpu** ● **filter** *rule-number* **action mirror group** *group-number* 6. Run the **quit** command or **exit** command to exit the ACL view and access the global configuration view. 7. Access the interface configuration view, interface group configuration view, or VLAN configuration view. 8. Run the **filter-list-{ l2 | ipv4 | ipv6 | hybrid } { in | out }** *acl-name* command to apply the ACL to the physical port or Trunk interface.

Purpose	Procedure
	9. Run the **mirror** { **ingress** | **egress** | **both** } **group** *group-list* command to configure the mirroring function on the source mirroring port.
Disable the flow mirroring function and delete the local mirror group and its observing interface	1. Access the interface configuration view or interface group configuration view. 2. Run the **no filter-list-{ l2 | ipv4 | ipv6 | hybrid } { in | out }** command and then run the **no mirror** { **ingress** | **egress** | **both** } *group-list* command to cancel the local mirroring function for the interface. 3. Access the global configuration view. 4. Run the **no mirror group** [*groupnum*] command to delete the local mirroring group and its observing interface.
View the configuration result	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), VLAN configuration view, or interface group configuration view. 2. Run the **show mirror config** command to view the configuration file information of the mirroring function. 3. Run the **show mirror group** command to view mirroring group information. 4. Run the **show mirror interface** command to view the mirrored port information. 5. Run the **show filter-list config** command to view mirroring rules.

12.2.5 Configuration Example

12.2.5.1 Example of Configuring Local Port Mirroring

Network Requirements

Department 1 and Department 2 of a group enterprise are connected to Switch over interfaces 10GE1/0/1 and 10GE1/0/2 respectively. The data monitoring device connects to Switch through interface 10GE1/0/3, You need to use the local port mirroring function to monitor packets that the two departments send to Switch with the data monitoring device, as shown in Figure 12-1.

Network Diagram

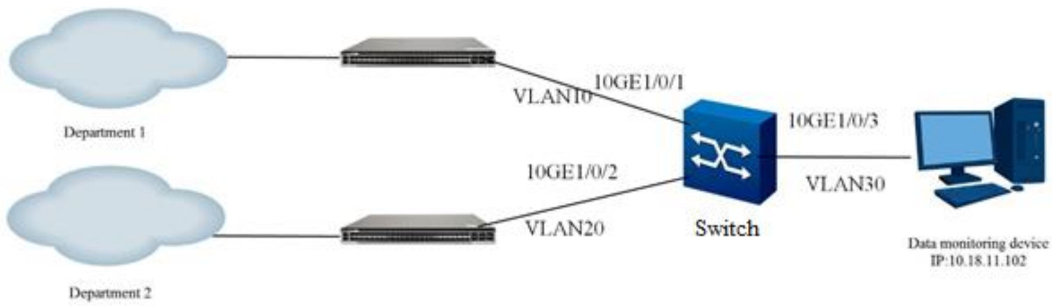


Figure 12-1 Network diagram of configuring local port mirroring

Configuration

1. Configure each interface to allow both departments to communicate with the data monitoring device.

Create VLAN 10, VLAN 20, and VLAN 30, and add interfaces 10GE1/0/1, 10GE1/0/2, and 10GE1/0/3 to VLAN 10, VLAN 20, and VLAN 30 respectively.

```
Switch#configure
Switch(config)#vlan 10
Switch(config-vlan-10)#quit
Switch(config)#vlan 20
Switch(config-vlan-20)#quit
Switch(config)#vlan 30
Switch(config-vlan-30)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port link-type trunk
Switch(config-10ge1/0/1)#port trunk pvid 10
Switch(config-10ge1/0/1)#port trunk allow-pass vlan 10
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)# port link-type trunk
Switch(config-10ge1/0/2)#port trunk pvid 20
Switch(config-10ge1/0/2)#port trunk allow-pass vlan 20
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)# port link-type trunk
Switch(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30
Switch(config-10ge1/0/3)#quit
Switch(config)#interface vlan 30
```

```
Switch(config-vlan-3)#ip address 10.18.11.1/24
Switch(config-vlan-3)#quit
Switch(config)#
```

2. Create a local mirror group and its observing interface.

Create the local mirror group 1 on Switch and configure its observing interface to 10GE1/0/3.

```
Switch(config)#mirror group 1 10gigaethernet 1/0/3
```

3. Configure the mirroring function of the source mirroring port.

Configure interfaces 10GE1/0/1 and 10GE1/0/2 as the source mirroring ports on Switch to monitor the data packets transmitted by Department 1 and Department 2.

```
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#mirror ingress group 1
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#mirror ingress group 1
Switch(config-10ge1/0/2)#quit
Switch(config)#
```

4. Configuration is complete.

12.2.5.2 Example of Configuring Local Flow Mirroring

Network Requirements

Department 1 and Department 2 of a group enterprise are connected to Switch over interfaces 10GE1/0/1 and 10GE1/0/2 respectively. The data monitoring device connects to Switch through interface 10GE1/0/3, It is required to use the local flow mirroring function to implement monitoring of the packets (with any source MAC address and the destination MAC address 00:00:00:01:02:03) transmitted from Department 1 and Department 2 to Switch, as shown in Figure 12-2.

Network Diagram

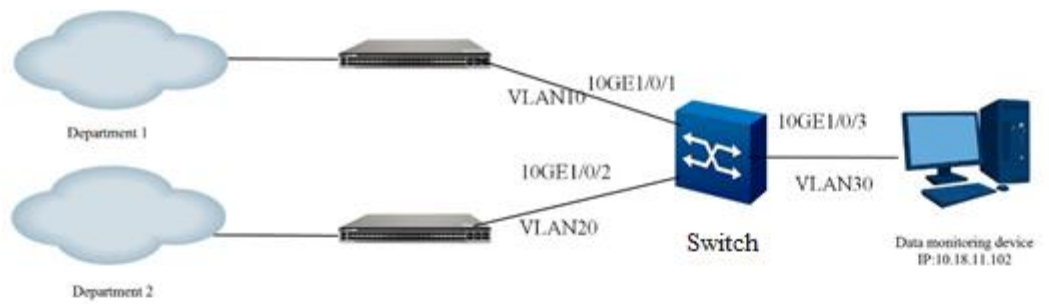


Figure 12-2Network diagram of configuring local flow mirroring

Configuration

1. Configure each interface to allow both departments to communicate with the data monitoring device.

Create VLAN 10, VLAN 20, and VLAN 30, and add interfaces 10GE1/0/1, 10GE1/0/2, and 10GE1/0/3 to VLAN 10, VLAN 20, and VLAN 30 respectively.

```
Switch#configure
Switch(config)#vlan 10
Switch(config-vlan-10)#quit
Switch(config)#vlan 20
Switch(config-vlan-20)#quit
Switch(config)#vlan 30
Switch(config-vlan-30)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#port link-type trunk
Switch(config-10ge1/0/1)#port trunk pvid 10
Switch(config-10ge1/0/1)#port trunk allow-pass vlan 10
Switch(config-10ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#port link-type trunk
Switch(config-10ge1/0/2)#port trunk pvid 20
Switch(config-10ge1/0/2)#port trunk allow-pass vlan 20
Switch(config-10ge1/0/2)#quit
Switch(config)#interface 10gigaethernet 1/0/3
Switch(config-10ge1/0/3)#port link-type trunk
Switch(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30
Switch(config-10ge1/0/3)#quit
Switch(config)#interface vlan 30
```

```
Switch(config-vlan-3)#ip address 10.18.11.1/24
Switch(config-vlan-3)#quit
Switch(config)#
```

2. Create a local mirror group and its observing interface.

Create the local mirror group 1 on Switch and configure its observing interface to 10GE1/0/3.

```
Switch(config)#mirror group 1 10gigaethernet 1/0/3
```

3. Configure the flow classification rules and flow mirroring processing action, and apply the policy to the source mirroring port.

Create ACL 100 on Switch, configure the match rules and processing action, and then apply ACL 100 to the source mirroring port.

```
Switch(config)#filter-list 100
Switch(configure-filter-l2-100)#filter 1 mac any 00:00:00:01:02:03/48
Switch(configure-filter-l2-100)#filter 1 action mirror group 1
Switch(configure-filter-l2-100)#quit
Switch(config)#interface 10gigaethernet 1/0/1
Switch(config-10ge1/0/1)#filter-list-l2 in 100
Switch(config-ge1/0/1)#quit
Switch(config)#interface 10gigaethernet 1/0/2
Switch(config-10ge1/0/2)#filter-list-l2 in 100
Switch(config-10ge1/0/2)#quit
Switch(config)#
```

4. Configuration is complete.

12.3 Configuring Log Management

12.3.1 Overview of Log Management

To monitor system operation and status, you can enable the log function. Then you can obtain the system status by checking logs and take appropriate actions. The log file can save 4000 consecutive records. When the number of records exceeds 4000, the system automatically deletes the earliest records. To prevent loss of log files, you are advised to export log files regularly.

12.3.2 Configuring Log Management

12.3.2.1 Enable or Disable the Logging Function

Purpose

This section describes how to enable or disable the logging function of the switch.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable the logging function of the system	1. Access the global configuration view. 2. Run the **logging on** command.
Disable the logging function of the system	1. Access the global configuration view. 2. Run the **no logging on** command.

12.3.2.2 Displaying or Clearing the Log Information

Purpose

This section describes how to display or clear the log information.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display log information of a specified module in the log buffer	1. Access the common user view. 2. Run the command **show { logbuffer | trapbuffer } module { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | dos-antiattack | uinetsck | slot}.**
Display the log buffer and alarm buffer of the	1. Access the common user view. 2. Run the **show { logbuffer | trapbuffer } module policy-route** command.

Purpose	Procedure
system running information	
Clear abnormal logs	1. Access the privileged user view. 2. Run the **clear abnormal-log** command.
Clear the log buffer	1. Access the global configuration view. 2. Run the **clear logging {logbuffer|trapbuffer}** command.
Clear all the content in a log file	1. Access the global configuration view. 2. Run the **clear logging logfile all** command.
Clear the default content in a log file	1. Access the global configuration view. 2. Run the **clear logging logfile default** command.
Clear log information of a specified module	1. Access the global configuration view. 2. Run the command **clear logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | dos-antiattack | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot }.**

12.3.2.3 Configuring Action Information

Purpose

This section describes how to configure action information.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the priority	1. Access the global configuration view. 2. Run the following commands:

Purpose	Procedure
threshold for a specified type of logs for a specified action of a specified module	**logging source** { **aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client |did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot** } **action** { **console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp** } { **log** | **debug** | **trap** } **level** { **emergencies** | **alert** | **critical** | **error** | **warning** | **notification** | **information** | **debugging** | **default** } **logging source** { **aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client |did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot** } **action** { **console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp** } { **log** | **debug** | **trap** } **state** { **enable** | **disable** | **default** } **logging source** { **aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client |did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power |**

Purpose	Procedure
	pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot } **action** { **console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp** } { **log** | **debug** | **trap** } **state** { **enable** | **disable** | **default** } **level** { **emergencies** | **alert** | **critical** | **error** | **warning** | **notification** | **information** | **debugging** | **default** }
Cancel the priority threshold for a specified type of logs for a specified action of a specified module	1. Access the global configuration view. 2. Run the command **no logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client |did | diffserv | dot1x | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot } action { console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp }.**

12.3.2.4 Configuring the Syslog Server

Background

The syslog server receives log information from clients to facilitate unified log management and view, helping you monitor the switch.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a syslog server	1. Access the global configuration view. 2. Run the **syslog server** *ipv4-address* [*server-port*] command.
Delete a syslog server	1. Access the global configuration view. 2. Run the **no syslog server** *ipv4-address* command.

12.3.2.5 Configuring Log Files

Purpose

The section describes how to configure a log file size and quantity.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the log file size for each module	1. Access the global configuration view. 2. Run the command **logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | counter | cpu | cpu-defend | ddm | default | devcomm | did | diffserv | dos-antiattack | dot1x | evpn | fan | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | l3vpn | lacp | link-flap | lldp | llt | loopcheck | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | ndp | nd-snooping | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route-policy | scheduleprofile | slot | snmp | soa | ssh | stg | stp | system | tcp | tcp6 | temperature | time-range | udld | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vrrp | vtp | vxlan } logfile size kbytes {** *file_size* | **default }.**
Configure the maximum number of log files for each module	1. Access the global configuration view. 2. Run the command **logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | counter | cpu | cpu-defend | ddm | default | devcomm | did | diffserv | dos_antiattack | dot1x | evpn | fan | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | lldp | llt | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | ndp | nd-snooping | ntp | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | rawip | rawip6 | rip | rlink | route-policy | scheduleprofile | slot | snmp | soa | ssh | stg | stp | system | tcp | tcp6 | temperature | time-range | udld | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vrrp | vtp | vxlan } max-number {** *file_num* | **default }**.

12.3.2.6 Saving Log Files

Purpose

This section describes how to save log files.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Manually save log files	1. Access the global configuration view. 2. Run the **save logging logfile** command.

12.3.2.7 Viewing the Log Configuration

Purpose

This section describes how to check whether the configuration is correct after configuring the log management function and relevant parameters.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the system log information	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show logging** command.
View the detailed content of the system logging action	1. Access the common user view, privileged user view, or global configuration view. 2. Run the following commands: ● **show logging action;** ● **show logging action { console | monitor | logfile | logbuffer | trap | syslog | smtp };** ● **show logging source { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | dos-antiattack | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6**

Purpose	Procedure
	| isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot }.
View the system log statistics	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show logging statistics** command.
Display log file information of different modules	1. Access the common user view. 2. Run the command **show logfile** *file-name* **module { aaa | acl | antiattack | arp | arp-antiattack | arp-probe | bfd | bgp | cli | counter | cpu | cpu-defend | ddm | default | devcomm | dhcp | dhcp-client | did | diffserv | dot1x | dos-antiattack | evpn | fan | hwbd | hwroute | hwvp | hwvrf | icmp | icmp6 | ifm | igmp | igmp-snooping | ip | ipsg | ip-subnet-vlan | ipv6 | isis | iss | lacp | link-flap | llt | lldp | loopcheck | l3vpn | mac-vlan | mad | mam | memory | mirror | mlag | mld | mld-snooping | mlink | mvrp | nd-snooping | ndp | ntp | ospf | ospf6 | patch | pim | port-isolate | power | pppoeplus | protocol-vlan | policy-route | rawip | rawip6 | rip | rlink | route | route-policey | scheduleprofile | snmp | soa | ssh | stg | stp | storm-control | storm-suppression | system | temperature | tcp | tcp6 | time-range | udp | udp6 | udr | uinetsck | virtual-cable-test | vlan-mapping | vlan-stacking | vtp | vxlan | slot }**.
Display the syslog server configuration file	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show syslog config** command.
Display the syslog server information	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show syslog server** command.
View information recorded in the log buffer	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show logbuffer** command.

12.4 Configuring DDM

12.4.1 DDM Overview

In an optical fiber link, locating the location of the fault is crucial to rapid recovery of services. Digital Diagnostic Monitoring (DDM), an intelligent optical module, can be used to allow network management units to monitor the temperature, supply power voltage, laser bias current, and transmit and receive optical power of the transceiver module in real time. These parameters help management units to locate the fault position in the optical fiber link, simplifying the maintenance work and improving the reliability of the system.

In conclusion, the digital diagnostic function helps locating the faults. During fault locating, you need to comprehensively analyze the warning and alarm states of Tx_power, Rx_power, Temp, Vcc, and Tx_Bias.

12.4.2 Configuring Basic DDM Functions

Purpose

This section describes how to enable an interface to monitor the temperature, supply power voltage, laser bias current, and transmit and receive optical power of an optical module in real time, so as to quickly locate the fault in an optical fiber link.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable obtaining the optical module parameters	1. Access the global configuration view. 2. Run the **ddm** { **enable** | **disable** } command.
Configure an interval for obtaining the optical module parameters	1. Access the global configuration view. 2. Run the **ddm interval** { *value* | **default** } command.
Configure the time of automatic recovery link up after the optical power of an interface is too low and the status changes to down	1. Access the global configuration view. 2. Run the **error-down auto-recovery cause transceiver-power-low interval** *interval* command.

Purpose	Procedure
Configure the bias current thresholds of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser bias-current-threshold** *low-threshold high-threshold* command.
Configure to automatically obtain the bias current thresholds of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser bias-current-threshold auto** command.
Configure the thresholds for receiving optical power of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser rx-power-threshold** *rx-low-threshold rx-high-threshold* command.
Configure to automatically obtain the thresholds for receiving optical power of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser rx-power-threshold auto** command.
Configure the temperature threshold of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser temperature-threshold** *low-threshold high-threshold* command.
Configure to automatically obtain the temperature thresholds of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser temperature-threshold auto** command.
Enable or disable the trap reporting function for an optical module	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser trap { enable | disable }** command.
Configure the thresholds for sending optical power of an optical module port.	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser tx-power-threshold** *tx-low-threshold tx-high-threshold* command.
Configure to automatically obtain the thresholds for sending optical power of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser tx-power-threshold auto** command.
Configure the voltage threshold of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser voltage-threshold** *low-threshold high-threshold* command.

Purpose	Procedure
Configure to automatically obtain the voltage thresholds of an optical module port	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **laser voltage-threshold auto** command.
Enable or disable the Error-Down function triggered when the optical power received by the specified Ethernet optical interface is too low	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **transceiver power low trigger error-down { enable | disable }** command.
Configure the DDM reporting polling interval	1. Access the global configuration view. 2. Run the **ddm report interval** { *value* | **default** } command.

12.4.3 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the DDM function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the DDM information configured in all views, including current and voltage thresholds	1. Access the common user view. 2. Run the **show ddm config** command.
View the general hardware information about all modules with ports inserted with optical modules	1. Access the common user view. 2. Run the **show laser hardware** command.
View the detailed hardware information about all modules with ports inserted with optical modules	1. Access the common user view. 2. Run the **show laser hardware detailed** command.
View the general hardware information about the module with a specific optical module port	1. Access the common user view. 2. Run the command **show laser hardware { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.

Purpose	Procedure
View the detailed hardware information about the module with a specific optical module port	1. Access the common user view. 2. Run the command **show laser hardware { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* detailed.
Enable or disable DDM debugging	1. Access the privileged user view. 2. Run the **debug ddm { poll | event | all } or no debug ddm { poll | event | all }** command.

12.5 Configuring Patches for System or a Specified Line Card

12.5.1 Overview of Patches for System or a Specified Line Card

This device allows you to install patches for the system or for a line card in a specified slot.

A patch is software that is compatible with system software and is used to resolve system software bugs.

The device supports three patch states: LOAD, ACTIVE, and DEACTIVE.

12.5.2 Loading Patches for a Single Board

Background

Before loading patches, the system needs to parse the patch package, check whether the patch files in the package are valid, and obtain the patch file attributes, including the patch type, board type, and version information.

When loading a patch for a single board, the system searches for a matching patch file in the patch package according to the attributes of the patch file. If a matching patch file is found, the system loads the patch file. Otherwise, the system does not load any patch file.

The patch file must be in the root directory of the master control board.

When patches are loaded during registration of the standby master control board (not registered), the system prompts a message asking you whether to continue patch loading.

Purpose

This section describes how to load patch files.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**.

Purpose	Procedure
Load a patch file downloaded to the device to the system	1. Access the global configuration view. 2. Run the **patch** *patch-number* **load** *filename* command to load a patch in the patch package matching the board on the active/standby master control board.
View the configuration result	1. Remain in the current privileged user view. 2. Run the **show patch information** command to view all patches in the system.

12.5.3 Activating a Patch

Preparations

Before activating a patch, you must load the patch for a board, as shown in 12.5.2

Background

The current patch function can load patches for software on the master control board and line card. As long as the master control software system is started, patches can be loaded or activated. Only when the line card is online, can patches be loaded and the slot number of the line card be specified in the command.

When you deactivate patches, the patches must exist and be activated.

Purpose

This section describes how to activate patches.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Activate a patch and configure whether the patch is	1. Access the global configuration view. 2. Run the **patch** *patch-number* **active { permanent | temporary }** command to activate a specified loaded patch (activated patch) on the

Purpose	Procedure
activated permanently or temporarily	active/standby master control board and set its mode to permanent. Permanent patches are still active after the device is restarted.
View the configuration result	1. Access the privileged user view. 2. Run the **show patch information** command to view all patches in the system.

12.5.4 Deactivating a Patch

Preparations

Before deactivating a patch, you must activate the patch, as shown in 0

Purpose

This section describes how to deactivate a running patch.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Deactivate a patch	1. Access the global configuration view. 2. Run the **patch** *patch-number* **deactive** command to deactivate a patch on the active/standby master control board.
View the configuration result	1. Access the privileged user view. 2. Run the **show patch information** command to view all patches in the system.

12.5.5 Deleting a Patch

Purpose

This section describes how to delete a patch. Before deleting an activated patch, you must deactivate the patch first and then delete it.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Delete a patch file directly	1. Access the global configuration view. 2. Run the **patch** *patch-number* **delete** command to delete a patch file on the active/standby master control board.
View the configuration result	1. Access the privileged user view. 2. Run the **show patch information** command to view all patches in the system.

12.6 Configuring STG

12.6.1 STG Overview

An STP Group (STG) is a forwarding control set of all interface VLANs. The STG protocol module is a switch chip API.

12.6.2 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the STG function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable STG debugging	1. Remain in the current privileged user view. 2. Run the **debug stg { error | event | notification | sync | all } or no debug stg { error | event | notification | sync | all }** command.
Clear all STG error statistics	1. Run the **disable** command to return to the common user view. 2. Run the **reset stg error** command.
View the STG function information	1. Run the **disable** command to return to the common user view. 2. Run the show stg { all | brief | error | memory } command.
View information about an STG instance	1. Run the **disable** command to return to the common user view. 2. Run the **show stg instance** { *instance-id* | **all** } command.
View information about an STG interface	1. Run the **disable** command to return to the common user view. 2. Run the s**how stg interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* **or show stg interface all** command.
View the STG protocol information	1. Run the **disable** command to return to the common user view. 2. Run the **show stg protocol { all | stp | alb | cfm | g8032 | lacp | mad | mlink | rlink | y1731 }** command.

Chapter 13 Configuring O&M Management

This chapter describes the basic content, configuration procedure, and configuration examples of the O&M management of the Switch.

13.1 Configuring NTP

13.1.1 NTP Overview

Network Time Protocol (NTP) provides the switch with the network clock synchronization function, which includes an NTP server and an NTP client. By configuring NTP, the clocks of devices on a network can be kept consistent.

Four Running Modes Supported by NTP

- Unicast mode

  In this mode, the system performs the following operation: The unicast client periodically sends an NTP request packet to the server, and expects to receive a request response packet from the server. After receiving the response packet from the server, the client calculates the local clock compensation value according to the round-trip propagation delay between the server and the client. The client calculates the time according to the relationship between the server's time and the local clock compensation value calculated based on the round-trip propagation delay and sets it as local time. The server waits for the request sent periodically by the client, constructs a request message response packet according to the address of the received request message and sends the packet. The server does not automatically send advertisement packets periodically.

- Peer mode

  In this mode, active peers and passive peers can synchronize with each other, and peers with a lower level (large number of layers) synchronize to peers with a higher level (small number of layers). The active peer sends a synchronization request packet to the passive peer, and the Mode field in the packet is set to 1 (active peer). After receiving the request packet, the passive peer automatically works in passive peer mode and sends a response packet with the Mode field in the packet set to 2 (passive peer).

- Multicast mode

  The client listens to the multicast message packet from the server. After receiving the first multicast message packet, to estimate the network delay, the client first enables a short server/client mode to exchange messages with the remote server. The client enters the multicast mode, continues to listen to the arrival of multicast message packets, and synchronizes the local clock according to the incoming multicast message packets. The IPv4 server periodically sends clock synchronization packets to the multicast destination address 224.0.1.1.

- Broadcast mode

  The client listens to broadcast message packets from the server. After receiving the first broadcast message packet, to estimate the network delay, the client first enables a short server/client mode to exchange messages with the remote server. The client enters the broadcast mode, continues to listen to the arrival of broadcast message packets, and synchronizes the local clock according to the incoming broadcast message packets. The IPv4 server periodically sends clock synchronization packets to the broadcast destination address 255.255.255.255 or the subnet broadcast address.

Advantages of NTP

- It supports sending protocol packets in unicast, multicast or broadcast mode.
- It supports MD5 authentication.
- It uses the stratum method to define the clock accuracy, and thus the time of each device in the network can be quickly synchronized.

13.1.2 Configuring Basic NTP Functions

Purpose

This section describes how to configure basic NTP functions to know how to configure NTP working modes.

Preparation

You have configured the link layer protocol, network layer IP address, or routing protocol of devices on the network to ensure that NTP packets between devices are reachable.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure the switch as the master clock	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **master** command.
Configure the NTP hierarchy	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **stratum** { *layer-number* | **default** } command. The layer number of the server (master clock) must be smaller than that of the client clock; otherwise, the client clock cannot synchronize with the server clock.
Configure the NTP unicast mode	Configure an NTP client (after a unicast server is specified, the local switch automatically works in the client mode. Perform Step 3 or 4 according to the actual condition.) 1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the following commands: ● **ntp unicast-server** *ipv4-address* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **source-interface loopback** *loopback-id*

Purpose	Procedure
	● **ntp unicast-server** *ipv4-address* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 }** ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface vlan** *vlan-id*
	Configure an NTP server You only need to configure the NTP master clock for the server.
Configure the NTP broadcast mode (applicable for LANs)	Configure the NTP broadcast client: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp broadcast-client** ● **ntp broadcast-client** *ipv4-address*
	Configure the NTP broadcast server: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp broadcast-server** ● **ntp broadcast-server** *ipv4-address* ● **ntp broadcast-server authentication-keyid** *key-id* ● **ntp broadcast-server authentication-keyid** *key-id ipv4-address* ● **ntp broadcast-server version { 1 | 2 | 3 | 4 }** ● **ntp broadcast-server version { 1 | 2 | 3 | 4 }** *ipv4-address* ● **ntp broadcast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 }** ● **ntp broadcast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 }** *ipv4-address*
Configure the NTP multicast mode	Configure the NTP multicast client: 1. Access the global configuration view. 2. Access the VLANIF configuration view.

Purpose	Procedure
	3. Run the following commands: ● **ntp multicast-client** ● **ntp multicast-client** *ipv4- address*
	Configure the NTP multicast server: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp multicast-server** ● **ntp multicast-server** *ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* ● **ntp multicast-server authentication-keyid** *key-id ipv4-address* ● **ntp multicast-server version { 1 | 2 | 3 | 4 };** ● **ntp multicast-server version { 1 | 2 | 3 | 4 }** *ipv4-address* ● **ntp multicast-server ttl** *ttl-value* ● **ntp multicast-server ttl** *ttl-value ipv4-address* ● **ntp multicast-server version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server version { 1 | 2 | 3 | 4 } ttl** *ttl-value ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server authentication-keyid *key-id* version { 1 | 2 | 3 | 4 } ttl** *ttl-value ipv4-address*
Add or modify an IPv4 NTP active peer. The command supports peer configuration in multiple VPN instance	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the following commands: ● **ntp unicast-peer** *ipv4-address* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 }** ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id*

Purpose	Procedure
	● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface vlan** *vlan-id*
Configure the interval for updating the NTP client	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **client update-interval** { *update-interval-time* | **default** } command
Configure the broadcast interval of the NTP server	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **server broadcast-interval** { *interval* | **default** } command

13.1.3 Configuring the NTP Security Mechanism

Purpose

This section describes how to configure the NTP security mechanism for reliable clock synchronization in networks with high security requirements.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable or disable MD5 authentication globally	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **authentication { enable | disable }** command.
Configure an NTP authentication key	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **authentication-keyid** *key-id* **md5 key** *key-string* command.

Purpose	Procedure
Enable or disable trusting of any MD5 authentication key	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **trusted-keyid** *trusted-keyid time* { **enable** | **disable** } command.
Enable or disable the concurrency mechanism in the process of synchronizing packet interaction	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the **oncesync** { **enable** | **disable** } command.
Configure the authentication mode for NTP unicast mode	Configure an NTP client (after a unicast server is specified, the local switch automatically works in the client mode. Perform Step 3 or 4 according to the actual condition.) 1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the following commands: ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** ***key-id*** ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*
	Configure an NTP server You only need to configure the NTP master clock for the server.
Configure the authentication mode for NTP broadcast mode (applicable for LANs)	Configure the NTP broadcast client: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp broadcast-client** ● **ntp broadcast-client** *ipv4-address*
	Configure the NTP broadcast server: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp broadcast-server authentication-keyid** *key-id* ● **ntp broadcast-server authentication-keyid** *key-id* *ipv4-address*

Purpose	Procedure
	● **ntp broadcast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 }** ● n**tp broadcast-server authentication-keyid** *key-id* version **{ 1 | 2 | 3 | 4 }** *ipv4-address*
Configure the authentication mode for NTP multicast mode	Configure the NTP multicast client: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● **ntp multicast-client** *key-id* ● **ntp multicast-client** *key-id ipv4-address*
	Configure the NTP multicast server: 1. Access the global configuration view. 2. Access the VLANIF configuration view. 3. Run the following commands: ● n**tp multicast-server authentication-keyid** *key-id* ● **ntp multicast-server authentication-keyid** *key-id ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value ipv4-address*
Configure the authentication mode for NTP peer mode	1. Access the global configuration view. 2. Access the NTP configuration view. 3. Run the following commands: ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*

13.1.4 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the NTP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the global NTP configuration	1. Access the global configuration view, NTP configuration view, or VLAN configuration view. 2. Run the **show ntp** command.
View the NTP service information	1. Access the global configuration view, NTP configuration view, or VLAN configuration view. 2. Run the **show ntp service** command.
View the details of NTP service configuration	1. Access the global configuration view, NTP configuration view, or VLAN configuration view. 2. Run the **show ntp service verbose** command.

13.1.5 Configuration Example

Network Requirements

NTP is a typical protocol that works in the server-client mode. The client is connected to the server, and the client obtains the current time from the server, as shown in Figure 13-1.

Network Diagram

Figure 13-1 NTP configuration network diagram

Configuration

Step 1: (omitted) Configure a VLAN and interface for the NTP server and client and that the server can ping the client.

Step 2: Configure the NTP server as the master clock and configure its number of layers.

Server(config-ntp)#master

Server(config-ntp)#stratum 2

Step 3: Configure the number of layers for the NTP client.

Client(config-ntp)#stratum 9

Step 4: Configure the mode and IP address (unicast mode) for the NTP client.

Client(config-ntp)#ntp unicast-server A.B.C.D (IP address of the server)

Caution

You can configure other modes in a similar way, with only the difference of specifying the multicast or broadcast mode on the server.

13.2 Configuring RMON

13.2.1 RMON Overview

Introduction

Remote Monitor (RMON) is a monitoring standard that enables network monitors and console systems to exchange network monitoring data. RMON gives network administrators more flexibility to select consoles and network monitors that meet special network requirements.

Currently, RMON has two versions: RMON v1 and RMON v2. RMON v1 is applied to commonly used network hardware and defines nine MIB groups that provide services to basic network monitoring. RMON v2 is an extension of RMON v1 intended for traffic layers (covering IP traffic and program-layer traffic) above the MAC layer. RMON v2 allows network management programs to monitor packets at all network layers, whereas RMON v1 only allows monitoring of packets at the MAC layer and lower layers.

Caution

Currently, Switch devices use RMON v1, which supports Groups 1, 2, 3, and 9 (statistics, history, alarm, and event).

RMON1 MIB Group

RMON1 MIB Group	Item	Element
Statistics	The monitor collects statistics on each monitoring interface of the device.	Dropped packet, sent packet, broadcast packet, CRC error, size block, conflict, and counter packet. The ranges include 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518, in bytes.
History	Periodically collects statistics on network value records and stores the statistics to facilitate subsequent retrieval.	Sampling cycle, sample quantity, and items; statistical history on network segment traffic, error packets, broadcast packets, utilization rate, and collision times.
Alarms	Periodically selects statistical examples from the monitor's variables and	Alarm type, interval, upper limit, and lower limit.

	compares the examples with the configured threshold.	
Host	Includes the host-related statistics that are discovered in the network.	Host address, packet, received byte, transmitted byte, and broadcast transmission.
HostTop N	Prepares a host description list, with the listed elements sorted based on a statistical value.	Statistical value, host, start and end of a cycle, base rate, and duration.
Truth table	Records information of the traffic between two hosts in a subnet. The information is stored as a matrix.	Source and destination address pair, packet, byte, and each error pair.
Filter	Allows the monitor to observe the packets matched with a filter.	Byte filter type and filter expression.
Packet capture	Captures packets after they pass through a channel.	Captures all packets that pass through the filter or records the packet statistics.
Event	Controls event generation and reporting.	Event type, description, and last time of event sending
Token ring	The token ring is supported.	The token ring is not frequently used.

13.2.2 Configuring a Statistical Table

Purpose

This section describes how to configure RMON to collect statistics on interface traffic.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure control for the RMON statistics record	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **rmon statistics** *statistics-id* [*owner*] command.
Delete control for the RMON statistics record	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **no rmon statistics** *statistics-id* command.

13.2.3 Configuring a Control History Table

Purpose

This section describes how to configure RMON to periodically collect statistics on the specified port and save the collected statistics to the history table.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure RMON historical record control	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **rmon history** *history-id sampling-interval sample-number* [**owner**] command.
Delete the configuration of RMON historical record control	1. Access the global configuration view. 2. Access the interface configuration view. 3. Run the **no rmon history** *history-id* command.

13.2.4 Configuring an Alarm Table

Purpose

This section describes how to configure RMON to monitor the alarm variable specified by OID at the designated sampling interval. When the value of monitored data exceeds the defined threshold, an alarm is generated.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a RMON alarm entry	1. Access the global configuration view. 2. Run the command **rmon alarm** *alarm-id object-id query-interval* { **absolute** | **delta** } *rising-threshold rising-event falling-threshold falling-event* [owner].
Delete a configured RMON alarm entry	1. Access the global configuration view. 2. Run the **no rmon alarm** *alarm-id* command.

13.2.5 Configuring an Event List

Purpose

This section describes how to configure RMON to enable the device to record a log and (or) generate an alarm when an event exceeds the alarm threshold.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure a RMON event control entry	1. Access the global configuration view. 2. Run the **rmon event** *event-id* { **log** | **trap** | **both** } [*description*] command.
Delete t configured RMON event control entry	1. Access the global configuration view. 2. Run the **no rmon event** *event-id* command.

13.2.6 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the RMON function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View configuration of RMON alarm control entries	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon alarm** command.
View configuration of RMON events	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon config** command.

Purpose	Procedure
View configuration of RMON event control entries	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon event** command.
View configuration of RMON historical control entries	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon history** [*history-id*] command.
View statistics on RMON historical record control entries	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon history statistics** command.
View logs of RMON events	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon log** command.
View the RMON statistical table	1. Access the common user view, privileged user view, global configuration view, interface configuration view (Ethernet or Trunk), interface group configuration view, or batch interface configuration view. 2. Run the **show rmon statistics** command.

13.3 Configuring SNMP

13.3.1 Overview of SNMP

Introduction

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol and industry standard. It guarantees the transmission of management information between any two points, helping network administrators query information, modify configurations, isolate and diagnose faults, plan capacity, and generate reports on any network node. SNMP uses a polling mechanism and provides only a basic set of functions, making it suitable for small-scale, fast, and low-cost environments. SNMP is implemented over the connectionless transport layer protocol UDP and is supported by many products.

SNMP is divided into two parts: the manager and the agent. The agent is server-side software running on a network device. The manager sends GetRequest, GetNextRequest, and SetRequest packets to the agent. Upon receiving a request, the agent reads or writes data based on the packet type, generates a response packet, and sends it back. When an error occurs on the device (such as a reboot), the agent sends a trap packet to report the issue.

Supported SNMP Version and MIB

To uniquely identify the management variable of the device in the SNMP packet, SNMP identifies management objects using a hierarchical naming scheme. The collection of the management objects named by the hierarchical scheme is like a tree, in which the nodes indicate the management objects, as shown in the following figure. The management objects can be identified uniquely along the path starting from the root.

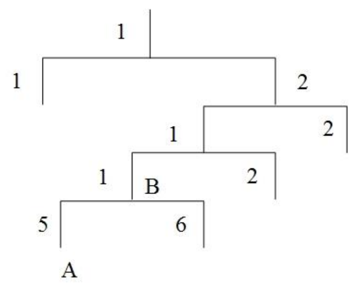


Figure 13-2 MIB tree structure

The management information base (MIB) is used to describe the tree hierarchy. It is a collection of the standard variable definitions of the monitored network device. In the figure above, management object B can be identified uniquely by a string of number {1.2.1.1}. The string of number is the object identifier of the management object.

The SNMP Agent of Switch supports SNMP V1, SNMP V2, and SNMP V3. The common supported MIB is as follows.

Table 13-1 Common MIB supported by Switch

MIB Attribute	MIB Content	Reference
Public MIB	MIB II based on TCP/IP network devices	RFC1213
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	IF MIB	RFC1573
Private MIB	DHCP MIB	-
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	Device management	
	Interface management	

13.3.2 Configuring the SNMP Maintenance Information

Purpose

This section describes how to configure the SNMP maintenance information to facilitate device maintenance using the network management system.

You can send the SNMP maintenance information to a local maintenance engineer when the switch is faulty and needs an urgent solution.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Designate an administrator contact method	1. Access the global configuration view. 2. Run the **snmp contact** *contact-info* command.
Designate the location of a managed device	1. Access the global configuration view. 2. Run the **snmp location** *location-info* command.
Configure the supported SNMP version	1. Access the global configuration view. 2. Run the **snmp version** { **v1** | **v2** | **v3** | **all** } command.
Cancel the configured SNMP version	1. Access the global configuration view. 2. Run the **no snmp version** { **v1** | **v2** | **v3** | **all** } command.

13.3.3 Configuring Basic SNMP Functions

Purpose

This section describes how to configure the basic SNMP functions to implement normal communication between the agent.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Configure an SNMP community name	1. Access the global configuration view. 2. Run the following commands: ● s**nmp community** *name* **{ ro | rw }** ● **snmp community** *name* { **ro** | **rw** } **view** *view-name*
(Optional) Enable the community name write function	1. Access the global configuration view. 2. Run the **snmp rw-community enable** command.
Configure the SNMP view	1. Access the global configuration view. 2. Run the following commands to create different MIB views, assigning different access permissions for the device : ● **snmp view** *view-name oid-tree* { **included** | **excluded** } ● **snmp view** *view-name oid-tree* { **included** | **excluded** } **mask** *subtreemask*
Configure the SNMP group information	1. Access the global configuration view. 2. Run the **snmp group** *group-name* **read-view** *read-view* **write-view** *write-view* **notify-view** *notify-view* command.

Purpose	Procedure
Create an SNMP user	1. Access the global configuration view. 2. Run the following commands to create user information to enable the user in the designated group to access the device: ● **snmp user** *user-name* **group** *group-name* **no-auth-no-priv** ● **snmp user** *user-name* **group** *group-name* **auth { md5 | sha }** *authkey* **priv no-priv** ● **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv des** *privkey*
(Optional) Configure the SNMP re-authentication interval	1. Access the global configuration view. 2. Run the **snmp reauth-interval** *interval* command.
(Optional) Configure the number of SNMP authentication failures	1. Access the global configuration view. 2. Run the **snmp fail-count** *count* command.
(Optional) Configure the number of an SNMP port	1. Access the global configuration view. 2. Run the **snmp port** { *port-number* | **default** } command.
Delete an SNMP community name	1. Access the global configuration view. 2. Run the **no snmp community** *name* command.
(Optional) Disable the community name write function	1. Access the global configuration view. 2. Run the **snmp rw-community disable** command,
Delete an SNMP user	1. Access the global configuration view. 2. Run the **no snmp user** *user-name* command.
Delete the SNMP group information	1. Access the global configuration view. 2. Run the **no snmp group** *group-name* command.
Delete an SNMP view	1. Access the global configuration view. 2. Run the **no snmp view** *view-name* or **no snmp view** *view-name oid-tree* command to delete a configured SNMP view.
Configure the maximum number of variable bindings in an SNMP Get Bulk request	1. Access the global configuration view. 2. Run the **snmp bulk max-varbind** { *varbind-number* | **default** } command.

13.3.4 Configuring the Trap Sending Function

Background

The trap message is actively sent by the managed device to reort critical events. The managed device sends this message only after being configured with the trap function.

Purpose

This section describes how to configure the device to send the trap message actively.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
(Optional) Enable the function of sending a trap message after authentication fails	1. Access the global configuration view. 2. Run the **snmp auth-trap enable** command.
(Optional) Enable the SNMP rich alarm function	1. Access the global configuration view. 2. Run the **snmp rich-trap enable** command.
(Optional) Configure the SNMP alarm log operation	1. Access the global configuration view. 2. Run the **snmp trap-log action { terminal | syslog | smtp | history | all | default }** command.
(Optional) Configure the priority of the SNMP alarm log	1. Access the global configuration view. 2. Run the **snmp trap-log priority** { *priority* | **default** } command.
Specify the IP address of the Ethernet interface, Eth-Trunk interface, loopback interface or VLAN interface as the release address of SNMP trap messages	1. Access the global configuration view. 2. Run the following commands: ● **snmp trap-source** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **snmp trap-source { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **snmp trap-source eth-trunk** *trunk-number* ● **snmp trap-source loopback** *loopback-number*

Purpose	Procedure
	● **snmp trap-source vlan** *vlan-id*
Designate the destination host for receiving SNMP trap messages	1. Run the **configure** command to access the global configuration view. 2. (IPv4) Run the following commands: ● **snmp trap-server** *ipv4-address security-name* { **v1** | **v2** | **v3** } ● **snmp trap-server** *ipv4-address port security-name* { **v1** | **v2** | **v3** } ● **snmp trap-server** *ipv4-address security-name* **v3** { **auth** | **priv** } ● **snmp trap-server** *ipv4-address port security-name* **v3** { **auth** | **priv** }
(Optional) Configure the size of the SNMP alarm history table	1. Access the global configuration view. 2. Run the **snmp trap-history** *history-table-size* command.
(Optional) Disable the function of sending a trap message after authentication fails	1. Access the global configuration view. 2. Run the **snmp auth-trap disable** command.
(Optional) Disable the SNMP rich alarm function	1. Access the global configuration view. 2. Run the **snmp rich-trap disable** command.
(Optional) Disable the function of designating the alarm source IP address	1. Access the global configuration view. 2. Run the **snmp source-input disable** command.
Delete the release address of SNMP trap messages	1. Access the global configuration view. 2. Run the **no snmp trap-source** command.
Delete the destination host for receiving SNMP trap messages	1. Access the global configuration view. 2. (IPv4) Run the following commands: ● **no snmp trap-server** *ipv4-address* ● **no snmp trap-server** *ipv4-address security-name*

13.3.5 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the SNMP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View the SNMP agent information of the device	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp agent** command.
View the SNMP community configuration	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp community** command.
View the SNMP configuration	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp config** command.
View the SNMP group information	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp group** command.
View statistics on SNMP packet processing	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp statistic** command.
View the SNMP alarm description	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp trap-description** command.
View the SNMP alarm history	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp trap-history** command.
View the host that receives the trap message and the host version and type	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp trap-server** command.
View the SNMP user information	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp user** command.

Purpose	Procedure
View the SNMP view information	1. Access the common user view, privileged user view, or global configuration view. 2. Run the **show snmp view** command.
View the alarm information state of the network management protocol	1. Access the common user view. 2. Run the **show snmp trap state** command.

13.4 Configuring LLDP

13.4.1 LLDP Overview

Background

As Ethernet technology is increasingly adopted, large-scale networking application requirements are surging, and more network equipment with complex configurations is emerging. As a result, higher demands are being placed on network management capabilities. To enable automatic discovery and exchange of system and configuration information between devices from different manufacturers, a standard information exchange platform is required. However, many network management solutions currently support only Layer 3 (L3) network topology analysis and cannot provide information such as equipment location or operational details. Link Layer Discovery Protocol (LLDP) was introduced to address this need.

LLDP Overview

LLDP is a Layer 2 discovery protocol defined in the IEEE 802.1ab standard. It provides a standardized method for link layer discovery, organizing key capabilities, management addresses, device IDs, and interface IDs into different types/length/values (TLVs), encapsulating them into Link Layer Discovery Protocol Data Units (LLDPDUs), and broadcasting the information to directly connected neighbors. A neighbor device receives and stores this information in Management Information Base (MIB) format, making it available for query and link status evaluation.

By running LLDP, the network can gain a clear understanding of all Layer 2 information for directly connected devices. This mechanism supports quick scaling of network management and enables more detailed tracking of network topology and configuration changes. LLDP also detects improper configurations on the network and helps in eliminating them promptly.

LLDP Terms

- LLDP: Link Layer Discovery Protocol
- LLDPDU: Link Layer Discovery Protocol Data Unit
- MIB: Management Information Base
- SNAP: Subnetwork Access Protocol
- TTL: time to live (value)

13.4.2 LLDP Working Principle

LLDP Port Working Mode

An LLDP port supports the following four working modes:

- TxRx: sending and receiving LLDP packets
- Tx: sending LLDP packets only
- Rx: receiving LLDP packets only
- Disable: neither sending nor receiving LLDP packets

Note:

When the LLDP working mode changes on a port, the port initializes the protocol status machine. To avoid repeated port initialization caused by frequent changes of port working mode, you can configure a port initialization delay period, so that the port can wait for a specified period before initialization after the port working mode changes.

13.4.3 Configuring LLDP Basic Functions

Purpose

This section describes how to configure the LLDP so as to discover the network topology, obtain device capability and configuration information from remote devices, detect inconsistent or incorrect configurations that may affect upper-layer application interworking, and help locate inconsistencies or errors on a network consisting of devices provided by different manufacturers.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
Enable LLDP and set its administrative status or disable LLDP on an interface	1. Access the global configuration view. 2. Access the interface group configuration view. 3. Run the **lldp admin-status { tx-only | rx-only | rx-tx | disable }** command.
Configure the LLDP management address	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **lldp management-address** *ip-address* **{ enable | disable } or lldp management-address** *mac-address* **{ enable | disable }** command.

13.4.4 Configuring LLDP Parameters

Purpose

This section introduces the operations for configuring the LLDP parameters, including adjusting LLDP packet sending intervals based on the network load and setting the delay period.
Operations described in this section are optional.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
(Optional) Configure the LLDP frame transmission interval	1. Access the global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **lldp tx-interval** { *tx-interval* | **default** } command.
(Optional) Configure the multiplier of the LLDP frame transmission interval	1. Access the global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **lldp tx-hold** { *tx-hold* | **default** } command.
(Optional) Configure a delay in re-initiating LLDP interface status	1. Access the global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **lldp reinit-delay** { *reinit-delay* | **default** } command.
(Optional) Configure a delay in sending LLDP packets	1. Access the global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **lldp tx-delay** { *tx-delay* | **default** } command.
(Optional) Configure the global alarm transmission interval	1. Access the global configuration view, interface configuration view (Ethernet), or interface group configuration view. 2. Run the **lldp notification-interval** { *notification-interval* | **default** } command.
(Optional) Configure the number of fast transmitted LLDP MED packets	1. Access the global configuration view. 2. Run the **lldp faststart-count** { *faststart-count* | **default** } command.
(Optional) Enable or disable the LLDP MED alarm function of an interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **lldp med-notification { enable | disable }** command.
(Optional) Configure MED attributes on an interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **lldp med-tlv-tx { capabilities | network-policy | location | extended-pse | extended-pd | inventory | all } { enable | disable }** command.
(Optional) Configure the basic	1. Access the global configuration view.

Purpose	Procedure
LLDP TLV on an interface	2. Access the interface configuration view or interface group configuration view. 3. Run the command **lldp basic-tlv-tx { port-description | system-name | system-description | system-capability | all } { enable | disable }**.
(Optional) Enable or disable the port VLAN ID (VID) field in optional IEEE802.1 TLVs	1. Access the global configuration view. 2. Run the corresponding command to access the interface configuration view or interface group configuration view. 3. Run the **lldp dot1-tlv-tx port-vid { enable | disable }** command.
(Optional) Enable or disable the VLAN name field in optional IEEE 802.1 TLVs	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **lldp dot1-tlv-tx vlan-name** *vlanlist* **{ enable | disable }** command.
(Optional) Configure the protocol VLAN ID function of the optional TLV for IEEE802.1	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **lldp dot1-tlv-tx protocol-id { enable | disable } or lldp dot1-tlv-tx protocol-vid** *vlanlist* **{ enable | disable }** command.
(Optional) Configure TLV information defined in IEEE802.3	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the command **lldp dot3-tlv-tx { mac-phy | power | link-aggregation | max-frame-size | all } { enable | disable }**.
Configure the position information of a device	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the following commands to configure TLV information defined in IEEE802.3. ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value*

Purpose	Procedure
	● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id elin-address** *number*

13.4.5 Maintenance and Debugging

Purpose

This section describes how to check or locate the fault when the LLDP function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**

Purpose	Procedure
View information about an LLDP interface	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the following commands: ● **show lldp interface** ● **show lldp interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show lldp interface verbose**
View the LLDP statistics information	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the following commands: ● **show lldp statistic** ● **show lldp statistic interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*
View the device information of all neighbors or a specified neighbor	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the following commands: ● **show lldp remote** ● **show lldp remote verbose** ● **show lldp remote** *remote-number*
View local LLDP device information	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the **show lldp local** command.
View the LLDP configuration information	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the **show lldp config** command.
View the neighbor information on a specified interface	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the command **show lldp remote interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
View the configuration information of a specified interface	1. Access the common user view, privileged user view, global configuration view, or interface configuration view. 2. Run the command **show lldp config interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
View the local device information	1. Access the common user view, privileged user view, global configuration view, or interface configuration view.

Purpose	Procedure
of a specified interface	2. Run the command **show lldp local interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*.
Clear the counter of an LLDP interface	1. Access the global configuration view. 2. Access the interface configuration view or interface group configuration view. 3. Run the **reset lldp counter** command.
Enable or disable LLDP debugging	1. Access the privileged user view. 2. Run the **debug lldp { config | rxstate | txstate | rxpkt | event | sync | all } or no debug lldp { config | rxstate | txstate | rxpkt | event | sync | all }** command.

13.4.6 Configuration Example

Network Requirements

1) Switch_1, Switch_2, Switch_3, Switch_4, and Switch_5 broadcast their Chassis IDs, port IDs, TTLs, management addresses, and other configuration information to other devices respectively.

2) Each of them can save the obtained information to its local MIB database and can access the database through SNMP.

3) The PC accesses Switch_1 through SNMP and it is found that Switch_2 and Switch_3 are directly connected to Switch_1. Therefore, the topology of direct connections with Switch_1 is obtained. According to the broadcast messages of Switch_2 and Switch_3, their management addresses are 10.1.1.2 and 10.1.1.3 respectively, so others can access Switch_2 and Switch_3 using these addresses.

4) By accessing Switch_2, Switch_4 is found to have direction connection with Switch_2. Thereby, the topology of direct connections with Switch_2 is obtained. According to the broadcast messages of Switch_4, its management address is 10.1.1.4, so others can access Switch_4 using the address.

5) By accessing Switch_3, Switch_5 is found to have direction connection with Switch_3. Thereby, the topology of direct connections with Switch_3 is obtained. According to the broadcast messages of Switch_5, its management address is 10.1.1.5, so others can access Switch_5 using the address.

6) Following the above-mentioned steps, a full topology and configuration information of each device are obtained, as shown in Figure 13-3.

Network Diagram

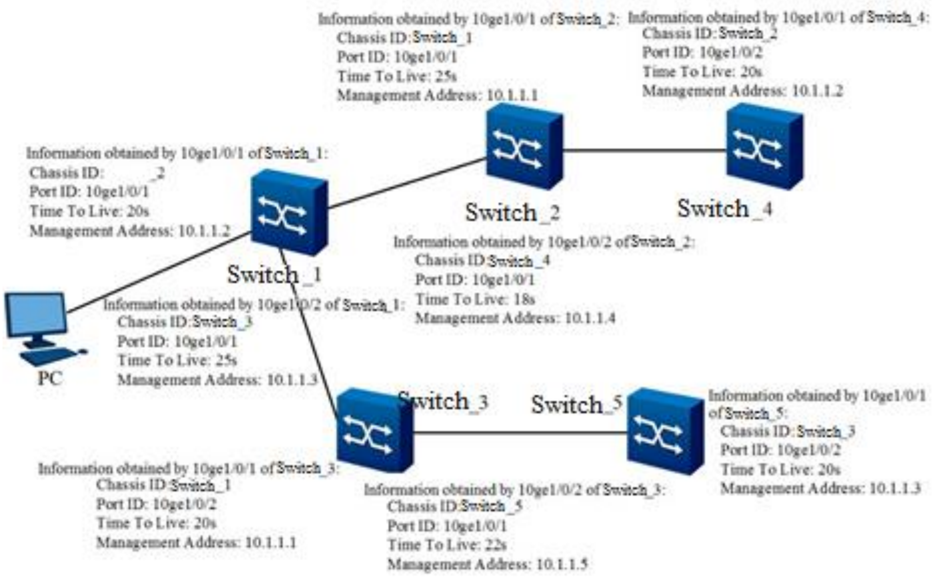


Figure 13-3 LLDP configuration network diagram

Configuration Suggestion

On Switch_1, set the LLDP working mode to Rx-Tx and the management address to 10.1.1.1.

On Switch_2, set the LLDP working mode to Rx-Tx and the management address to 10.1.1.2.

On Switch_3, set the LLDP working mode to Rx-Tx and the management address to 10.1.1.3.

On Switch_4, set the LLDP working mode to Rx-Tx and the management address to 10.1.1.4.

On Switch_5, set the LLDP working mode to Rx-Tx and the management address to 10.1.1.5.

Configuration

1. Configure Switch_1.

```
Switch_1(config)#interface 10gigaethernet 1/0/1
Switch_1(config-10ge1/0/1)#no shutdown
Switch_1(config-10ge1/0/1)#lldp admin-status rx-tx
Switch_1(config-10ge1/0/1)#lldp management-address 10.1.1.1 enable
```

2. Configure Switch_2.
Switch_2(config)#interface 10gigaethernet 1/0/1
Switch_2(config-10ge1/0/1)#no shutdown
Switch_2(config-10ge1/0/1)#lldp admin-status rx-tx
Switch_2(config-10ge1/0/1)#lldp management-address 10.1.1.2 enable

3. Configure Switch_3.
Switch_3(config)#interface 10gigaethernet 1/0/1
Switch_3(config-10ge1/0/1)#no shutdown
Switch_3(config-10ge1/0/1)#lldp admin-status rx-tx
Switch_3(config-10ge1/0/1)#lldp management-address 10.1.1.3 enable

4. Configure Switch_4.
Switch_4(config)#interface 10gigaethernet 1/0/1
Switch_4(config-10ge1/0/1)#no shutdown
Switch_4(config-10ge1/0/1)#lldp admin-status rx-tx
Switch_4(config-10ge1/0/1)#lldp management-address 10.1.1.4 enable

5. Configure Switch_5.
Switch_5(config)#interface 10gigaethernet 1/0/1
Switch_5(config-10ge1/0/1)#no shutdown
Switch_5(config-10ge1/0/1)#lldp admin-status rx-tx
Switch_5(config-10ge1/0/1)#lldp management-address 10.1.1.5 enable

13.5 Configuring Packet Capturing

13.5.1 Overview of CPU Packet Capturing

When CPU debugging is enabled, you can view details of CPU transmission and receiving. This function can be used to debug the device when a device fault occurs.

13.5.2 Maintenance and Debugging

Purpose

This section describes how to view data packets sent by the device to the CPU when a device fault occurs.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the continuous duration for capturing the packets sent and received by the CPU in the current interface	1. Remain in the current privileged user view. 2. Run the following commands: ● **capture cpupkt interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } { **enable** | **disable** } ● **capture cpupkt interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* **time** *time-value* ● **capture cpupkt interface eth-trunk** *trunk-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } { **enable** | **disable** } ● **capture cpupkt interface eth-trunk** *trunk-number* **time** *time-value*

Purpose	Procedure
	• **capture cpupkt interface mgt-eth** *mgt-eth-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } { **enable** | **disable** } • **capture cpupkt interface mgt-eth** *mgt-eth-number* **time** *time-value* • **capture cpupkt interface stack-port** *iss-group-id* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } { **enable** | **disable** } • **capture cpupkt interface stack-port** *iss-group-id* **time** *time-value* • **no capture cpupkt interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* • **no capture cpupkt interface eth-trunk** *trunk-number* • **no capture cpupkt interface mgt-eth** *mgt-eth-number* • **no capture cpupkt interface stack-port** *iss-group-id*
Display the statistics of packets sent and received by the CPU in an interface	1. Run the **disable** command to return to the common user view. 2. Run the following commands: • **show cpupkt interface** { **ethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } **statistic** • **show cpupkt interface eth-trunk** *trunk-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-**

Purpose	Procedure
	reply | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } **statistic** ● **show cpupkt interface mgt-eth** *mgt-eth-number* { **arp** | **lldp** | **loopback** | **dot3ah** | **lacp** | **dot1x** | **cfm** | **y1731** | **g8032** | **g8031** | **eaps** | **dlip** | **mlag** | **mpls** | **stp** | **isis** | **iss** | **bfd** | **sync** | **arp** | **ip** | **ospf** | **igmp** | **icmp** | **udp** | **dhcp** | **ldp-hello** | **bfd-udp** | **tcp** | **bgp** | **ldp-tcp** | **ipv6** | **icmpv6** | **icmpv6-echo-request** | **icmpv6-echo-reply** | **icmpv6-rs** | **icmpv6-ra** | **icmpv6-ns** | **icmpv6-na** | **icmpv6-redirect** | **ospfv3** | **all** | **other** } **statistic**

13.6 Configuring Telemetry

13.6.1 Telemetry Overview

Telemetry is a technology that remotely collects data at a high speed from physical devices or virtual devices. Devices periodically send information such as interface traffic statistics and CPU or memory data to the collector in push mode. Compared with the question-and-answer interaction provided by the traditional pull mode, the push mode provides a more real-time and high-speed data collection function.

13.6.2 Configuring a Destination Collector

Purpose

Before configuring Telemetry static subscription sampling data, you must create a destination group and specify a destination collector to which the sampled data is sent.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**.

Purpose	Procedure
Enable or disable the data collection function	1. Access the global configuration view. 2. Run the **telemetry** { **enable** | **disable** } command.
Configure an upstream destination group of sampled data and access the Destination-group view	1. Access the global configuration view. 2. Run the **telemetry destination-group** *name* command.
Create subscription to associate an upstream destination group and a sampling sensor group and access the Subscription view	1. Access the global configuration view. 2. Run the **telemetry subscription** *name* command.
Associate an upstream destination group	1. Access the global configuration view. 2. Run the **telemetry subscription** *name* command to access the Subscription view. 3. Run the **destination-group** *name* command.
Configure the IP address, port number, protocol, and encryption mode of an upstream destination collector	1. Access the global configuration view. 2. Run the **telemetry destination-group** *name* command to access the Destination-group view. 3. Run the **ip address** *ipv4-address* **port** *port-number* **protocol grpc** or **ip address** *ipv4-address* **port** *port-number* **vpn-instance** *name* **protocol grpc** command.

13.6.3 Configuring Sampling Data

Purpose

Before configuring Telemetry static subscription sampling data, you must create a sampling sensor group and specify the sampling path and filter conditions.

Procedure

Perform the corresponding steps according to different purposes, as shown below. For parameter description, see **Switch Command Reference Manual**.

Purpose	Procedure
Enable or disable the data collection function	1. Access the global configuration view. 2. Run the **telemetry** { **enable** | **disable** } command.
Create a sampling sensor group and access the Sensor-group view	1. Access the global configuration view. 2. Run the **telemetry sensor-group** *name* command.
Associate a sampling sensor group and configure the sampling period of the group	1. Access the global configuration view. 2. Run the **telemetry subscription** *name* command to access the Subscription view. 3. Run the **sensor-group** *name* **sample-interval** *interval-value* command.
Configure the path for a Telemetry sampling sensor	1. Access the global configuration view. 2. Run the **telemetry sensor-group** *name* command to access the Sensor-group view. 3. Run the **sensor-path** *name* command.

13.6.4 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the Telemetry function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
View the configuration information of a Telemetry sensor	1. Run the **disable** command to return to the common user view. 2. Run the **show telemetry config** command.
View information about an upstream destination group	1. Run the **disable** command to return to the common user view. 2. Run the **show telemetry destination config** command.
View information about a sampling sensor group	1. Run the **disable** command to return to the common user view. 2. Run the **show telemetry sensor config** command.
View the subscription information of a Telemetry sensor	1. Run the **disable** command to return to the common user view. 2. Run the **show telemetry subscription config** command.

13.7 Configuring NQA

13.7.1 Overview of NQA

Features of the quality analysis (NQA):

- Test type: ICMP-Echo
- NQA association
- Threshold alarms

13.7.2 NQA Test Mechanism

ICMP-Echo test mechanism

Compliant with RFC-2925, the ICMP-echo test is run by sending ICMP packets to calculate the network response time and packet loss rate.

To ensure success of the ICMP-echo test, the destination device should be able to correctly respond to the ICMP echo request packets.

The ICMP-echo test works as follows:

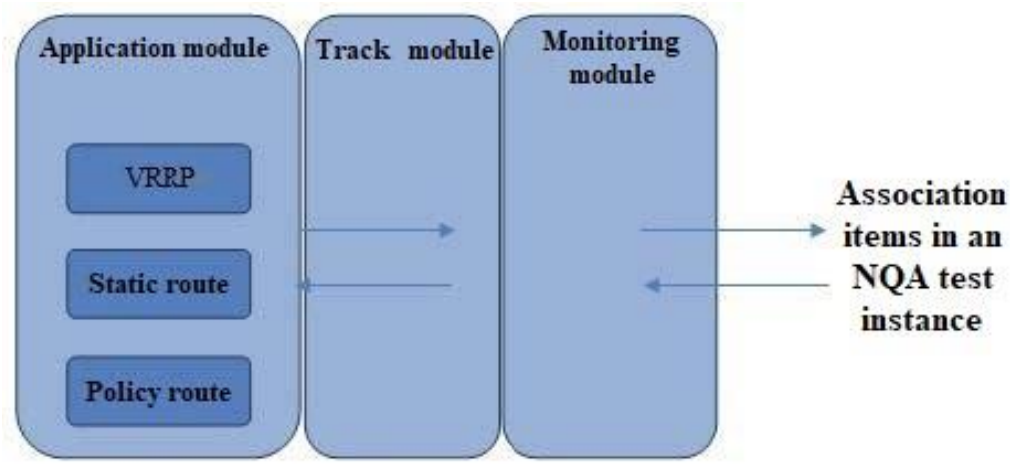
(1) The NQA client sends ICMP echo request packets to the destination IP address according to the set probe time and frequency.

(2) The switch at the destination IP address receives the ICMP echo request packets and replies with ICMP echo reply packets.

(3) The NQA client calculates the response time and packet loss rate of the destination IP address based on reception parameters of the ICMP echo reply packets, such as the reception timestamp and the number of packets, so as to reflect the current network performance and network conditions.

13.7.3 NQA Association Mechanism

Association means probing the results in the current test instance by creating association items. When the number of consecutive failed probes reaches a certain number, the application module will act accordingly through the track module.



NQA association comprises three modules:

1. Monitoring module: Monitors link states, network performance, and the like, and notifies the track module of the detection results.
2. Track module: After receiving detection results from the monitoring module, the track module changes the track item status in time and notifies the application module.
   Note that the track module resides between the application module and monitoring module, which can block differences of different monitoring modules and provide a unified interface for different application modules.
3. Application module: Process the change accordingly based on status of the track item.
   This process achieves the association.

13.7.4 Configuring an ICMP-Echo Test

Purpose

An ICMP-echo NQA test can be used to check whether a packet sent from the local end (DUT2) can reach a specified destination (DUT1) and show the round-trip time of the packet.

Procedure

Perform corresponding steps for your purposes by referring to the table below.

Purpose	Procedure
Creating an ICMP-echo NQA test instance and configuring	1. Enter global configuration view. 2. Run the following commands: ● DUT2# configure ● DUT2 (config)#nqa start ● DUT2 (config)# nqa test-instance 123 456

Purpose	Procedure
relevant test parameters.	● DUT2 (config-nqa-123-456)#type icmp-echo ● DUT2 (nqa-123-456-icmp-echo)#destination ip 3.3.3.1
Configuring optional parameters	1. Enter global configuration view. 2. Run the following commands: ● DUT2 (nqa-123-456-icmp-echo)#probe count 10 ● DUT2 (nqa-123-456-icmp-echo)#probe timeout 500 ● DUT2 (nqa-123-456-icmp-echo)# frequency 5000
Configuring the NQA history records	1. Enter global configuration view. 2. Run the following commands: ● DUT2 (nqa-123-456-icmp-echo)#history-record enable ● DUT2 (nqa-123-456-icmp-echo)# history-record number 10 ● DUT2 (nqa-123-456-icmp-echo)# quit ● DUT2 (config-nqa-123-456)#quit
Starting the ICMP-echo test	1. Enter the global configuration view. 2. Run the command nqa schedule 123 456 start-time now life-time forever to start the test.

13.8 Configuring JSON-RPC

13.8.1 JSON-RPC Overview

Introduction to JSON-RPC

JSON-RPC interface services allow users to remotely control switches through software.
The data format for JSON-RPC interface service requests complies with JSON-RPC protocols while RPC services use HTTP RESTFul APIs. The API client supports basic HTTP authentication and allows controlling the IP address whitelist.

JSON-RPC Principles

JSON-RPC is a stateless, light-weight remote procedure call (RPC) control. It is transport agnostic in that the concepts can be used within the same process, over sockets, over HTTP, or in many various message passing environment. It uses JSON (RFC 4627) as data format.
In JSON-RPC interface services, the switch command lines are executed through "JSON-RPC method：executeCmds". This interface service uses the same account system with the network management system of the switches. The command execution privileges should be set according to the account information set by the interface request.

The format of JSON-RPC protocol compliant data sent or received by the user is as follows:

- The user request URL is

```
http://{api_ip}:{api_port}/command-api
```

The parameter api_ip is the network IP address of the interface service, which can be configured through the out-of-band management port or the service port, and api_port is the request port, which is 8080 by default.

- The HTTP request and response data complies with the JSON-RPC 2.0 specifications.

The format of a JSON-RPC request is

```
{
   "jsonrpc": "2.0",                                    // JSON-RPC version
   "method": "executeCmds",                             // RPC method for executing switch
commands
   "params": [
      {
         "format": "text",                              // Return format of commands
         "version": 1,                           // Command version
         "cmds": [                               // List of command lines
            "show run",                          // Command line 1
            "configure",                         // Command line 2
            "interface vlan 300",                // Command line 3
            "ip address 10.103.107.254/23",      // Command line 4
            "ip dhcp relay",                     // Command line 5
            "dhcp relay server-ip 10.10.11.201", // Command line 6
            "end",
            "write file"
         ]
      }
   ],
   "id": "c5faf42b-d18f-405b-b1e0-f6d3383d8e2c"     // JSON-RPC protocol UID
}
```

The format of a JSON-RPC response is

```
{
   "jsonrpc": "2.0",
   "result": [
      {                                                          // Return of command line 1
         "sourceDetails": "!Device running configuration:\n!version V410R240......"
      },
      {                                                          // Return of command line 2
         "sourceDetails": " %Enter configuration commands.End with Ctrl+Z or command 'quit' &
'end'\n"
      },
      {       // Return of command line 3
         "errorCode": -3001,                              // Error code
         "sourceDetails": "",                             // Command screen output, if any
         "errorDesc": "command excute timeout",                // Error description
         "warnings": ""                                   // Warning message, if any
      },
      {},                                                 // If there is no output but the command
execution is correct, return NULL.
      …
   ],
   "id": "c5faf42b-d18f-405b-b1e0-f6d3383d8e2c"
}
```

Note

The returned results have a one-to-one correspondence with requests

Definition of Error Codes

- JSON-RPC error codes

Error Code	Meaning
-32700	JSON parsing error
-32600	Invalid request
-32601	Invalid method
-32602	Invalid parameter
-32603	Internal error

- API error codes

Error Code	Meaning
-1000	Common error
-2000	Internal error
-2001	JSON-RPC API version not supported
-2002	paramas and cmds attributes for JSON-RPC not specified
-2003	Return method not support. Data must be in json or text format.
-2004	Invalid parameter format
-3001	Command execution error: timeout
-3002	Command execution error: command not supported
-3003	Command execution error: command not authorized
-3004	Command execution error: command not found
-3005	Command execution error: unable to convert to JSON format
-3006	Command execution error: insufficient command lines
-3007	Command execution error: too many command lines
-3008	Command return error: total length of the string returned by the commands exceeding the limit
-3009	Command return error: the length of the string returned by a single command exceeding the limit

13.8.2 Configuring Basic JSON-RPC Functions

Purpose

This section introduces how to enable or disable JSON-RPC interface services and modify configuration parameters.

Preparation

The device link-layer protocols, network-layer IP addresses or routing protocols in the network have been configured, ensuring that the IP messages are reachable.

Procedure

Perform corresponding steps for your purposes by referring to the table below.

Purpose	Procedure
Starting / stopping services	1. Access the global configuration view. 2. Run the **batch-cmd jsonrpc enable** command to start services. 3. Run the **batch-cmd jsonrpc disable** command to stop services.
Setting an IP address and port for the JSON-RPC interface connecting to the external	1. Access the global view. 2. Run the **batch-cmd jsonrpc bind-ip** *ip-address* command to set an IP address for interface services. 3. Run the **batch-cmd jsonrpc bind-ip default** command to restore the default IP address 0.0.0.0. 4. Run the **batch-cmd jsonrpc bind-port** *port-value* command to set a port for interface services. 5. Run the **batch-cmd jsonrpc bind-port default** command to restore the default port numbered 8080.
Setting authentication mode of the interface	1. Access the global view. 2. Run the **batch-cmd jsonrpc auth-mode { none | basic | strict | default }** command to set the authentication mode of the interface.
Setting the whitelist for client access	1. Access the global view. 2. Run the **batch-cmd jsonrpc whitelist** *ip-address* command to add an IP address into the whitelist. 3. Run the **no batch-cmd jsonrpc whitelist** *ip-address* command to remove an IP address from the whitelist. 4. Run the **batch-cmd jsonrpc whitelist default** command to restore the default setting, which allows access from all clients.
Setting timeout period of client requests	1. Access the global view. 2. Run the **batch-cmd jsonrpc timeout** *time-value* command to set the request timeout period. 3. Run the **batch-cmd jsonrpc timeout default** command to restore the default timeout period.
Setting the maximum number of command lines allowed for a single batch request	1. Access the global view. 2. Run the **batch-cmd jsonrpc max-cmds** *value* command to set the maximum number of command lines allowed for a single batch request. 3. Run the **batch-cmd jsonrpc max-cmds default** command to restore the default maximum number 10.
Querying configuration parameters	1. Access the global view. 2. Run the **show batch-cmd jsonrpc** command to query service running parameters.

13.8.3 Configuring User Authentication

Purpose

This section introduces how to authenticate accounts for JSON-RPC interface services and set users' privileges.

Procedure

The JSON-RPC interface services use the same account system with the network management system of the switches. The account setting procedures are the same as those for the network management system. Procedures are as follows:

Purpose	Procedure
Creating interface accounts and setting users' privileges	1. Access the global configuration view. 2. Run the **username** *username* **group { administrators | operators | guests | users } password** *password* **simple** command to create user accounts, set passwords and grant privileges to users. 3. Run the following command to set JSON-RPC interface privileges. − **no username** *username* **domain all** − **username** *username* **domain jsonrpc**

13.9 Locally Upgrading a Device

The switch can be upgraded using command lines. Upgrade through the command line is simple, safe, and reliable. This mode is frequently used by network administrators.

13.9.1 Upgrading the OS Through Command Lines

Upgrading Network Diagram

Use a network cable to connect the PC network card with the Ethernet port of the switch. Use a serial port cable to connect the serial port of PC and the serial port of switch.

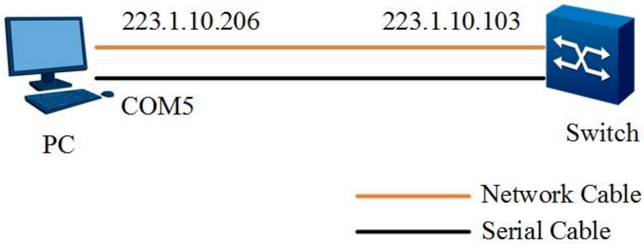
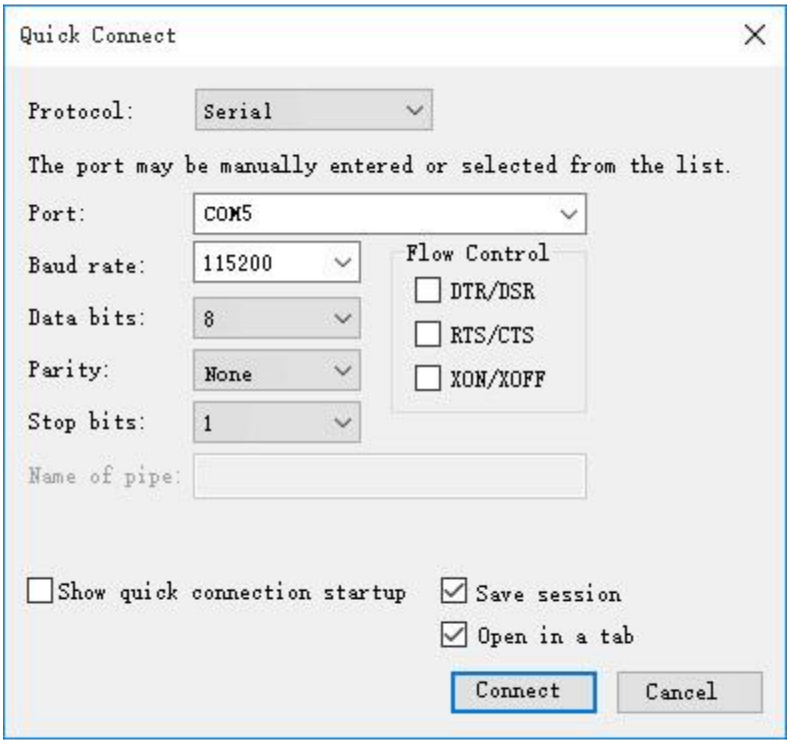


Figure 13-4 Network diagram of upgrading the switch locally

Preparations

1. Before using SecureCRT to log in to the switch via serial port, configure the baud rate on SecureCRT to 115200, and select the number of the PC serial port connected to the switch, as shown in the following figure.



Upgrading Steps

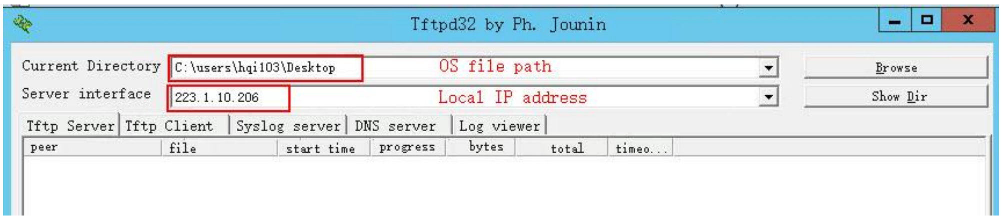
Caution

Disable the firewall for the PC during the upgrade process.

1. Log in to the switch through the serial port and enter the username and password.
2. Run the **configure** command to access the global configuration view.
3. Run the **interface mgt-eth 0/0/0** command to access the out-of-bound interface configuration view. Run the **ip address 223.1.10.103/24**command to configure an IP address for the switch (in the same network segment of the IP address of the PC network card).
4. Run the **exit** command to exit the out-of-bound interface configuration view.
5. Run the **ping 223.1.10.206** command to check whether the switch and PC can ping each other.

```
Switch#config
Switch(config)#interface mgt-eth 0/0/0
Switch(config-mgt-eth-0/0/0)#ip address 223.1.10.103/24
Switch(config-mgt-eth-0/0/0)#exit
Switch(config)#
Switch(config)#ping 223.1.10.206
 PING 223.1.10.206: 64 data bytes
 Reply from 223.1.10.206: bytes=64 time<1ms TTL=64 icmp_seq=1
 Reply from 223.1.10.206: bytes=64 time<1ms TTL=64 icmp_seq=2
 Reply from 223.1.10.206: bytes=64 time<1ms TTL=64 icmp_seq=3
 Reply from 223.1.10.206: bytes=64 time<1ms TTL=64 icmp_seq=4
 Reply from 223.1.10.206: bytes=64 time<1ms TTL=64 icmp_seq=5
 PING Statistics for 223.1.10.206
 5 packets transmitted, 5 packets received, 0% packet loss
 round-trip (ms)  min/avg/max = 0/0/0
Switch(config)#
```

6. Start the TFTP software. Configure an upgrade file path (the path to save the upgrade file on the PC), and enter the IP address configured for the PC network card in the **Server interfaces** field.



7. Run the **tftp get 223.1.10.206 Switch_OS_V410R240.bin** command to download the upgrade file.

```
Switch(config)#tftp get 223.1.10.206 Switch_OS_V410R240.bin
 Local path is "/tmp/ram/download".
 Getting data...
 303407177 bytes downloaded %Transmission success.

Switch(config)#
```

8. After the upgrade file is downloaded, run the **upgrade os system all** command to upgrade the switch version.

```
Switch(config)#upgrade os system all
  This operation will upgrade system file.Are you sure?(y/n) [y]y
  System now is upgrading,please wait...
Upgrade subsys:1 OS:
Step 1,times 1,Initializing SUCCESS...
Step 2,times 1,Transfer file SUCCESS...
Step 3,times 1,Upgrade SUCCESS...
Step 4,times 1,Finish SUCCESS...
```

9. After the switch is upgraded, run the **reboot** command to restart the switch.

```
Switch#reboot
  WARNING:System will reboot! Continue?(y/n) [y]y
  System now is rebooting,please wait.
Switch#
```

Check after Upgrading

1. After the switch is restarted, log in to the switch through the serial port and enter the default username and password.
2. Run the **show system** command to view the system device code, default MAC address, and current MAC address.
3. Run the **show version** command to view the device model, BIOS version, and hardware version.
4. Run the **show os** command to view the OS version.

```
Switch(config)#show system
  System device code   : G7FE200T00B220527
  Default mac-address  : 34:61:31:35:33:36
  Current mac-address  : 34:61:31:35:33:36
Switch(config)#show version
  Universal Software Platform
  Copyright (c) 2000-2022,
  USP (R) Software Version V370R240
  Compiled May 27 2022 06:23:53
  Routing Switch
  System Uptime is 4 days 0 hours 43 minutes 8 seconds

  Hardware Version   : 1.01
  BIOS Version       : N/A
  FPGA Version       : 1.01
  Serial Number      :
  System Memory      : 3784760K

Switch(config)#show os
attr        link  uid   gid   size        date    time   name
----------  ----  ----  ----  ----------  ------  -----  -----
total:297644
-rw-r--r--  1     root  root  304782261   Apr 12  10:24  Switch_OS_V410R240.bin
```

Configuring VPN

This chapter describes the basic content, configuration process, and configuration example of VPN tunnel management of the Switch.

13.10 Configuring L3VPN

13.10.1 Overview of L3VPN

Introduction

Multiprotocol Label Switching (MPLS) L3VPN is a type of provider edge (PE)-based L3VPN technology in the VPN solution designed for service providers (SPs). It uses BGP to distribute VPN routes and uses MPLS to forward VPN packets in the SP backbone network. MPLS L3VPN provides flexible network modes and high scalability, and can easily support MPLS QoS and MPLS TE.

The latest version of the MPLS L3VPN module is 1.0.

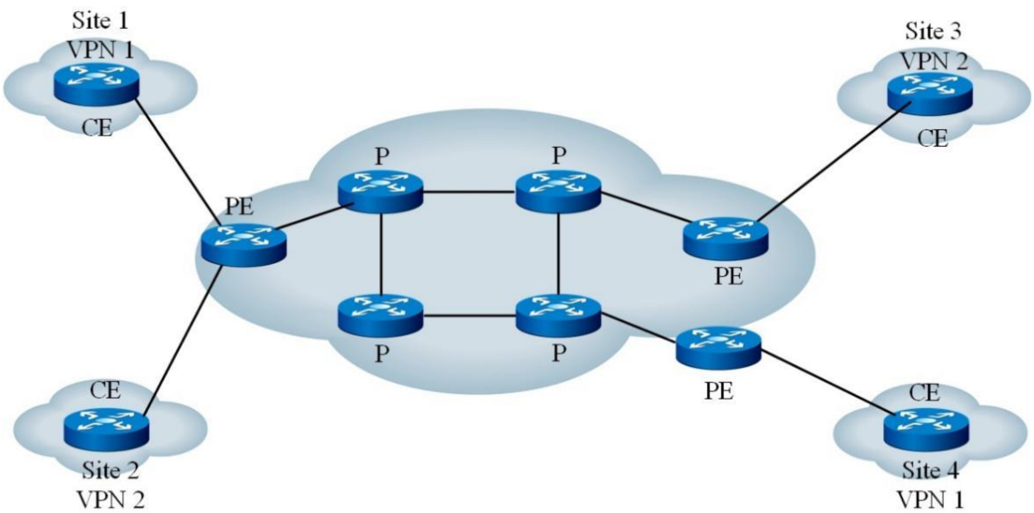


Figure 13-5 MPLS L3VPN network diagram

Figure 13-5 shows the MPLS L3VPN network diagram. The MPLS L3VPN model is composed of three parts: customer edge (CE), provider edge (PE), and provider (P).

- CE provides an interface to connect to the SP directly. CE can be a router, a switch, or a host. CE cannot perceive the existence of VPN and does not need to support MPLS.

- A PE router is located at the edge of the SP network and is directly connected to the user CE. In an MPLS network, all processing on VPN occurs on PE.
- A P router is the backbone router in the SP network. It is not directly connected to CE and only requires the basic MPLS forwarding capability.

The classification of CE and PE is mainly based on the management range of SP and user. CE and PE are boundaries of the management ranges of SP and user.

CE is generally a router. When establishing an adjacency relationship with the directly connected PE, CE distributes the VPN route of the local site to PE, and learns the route of remote VPN from PE. CE and PE use BGP/IGP to exchange routing information, and static routing can also be used.

After learning the local VPN routing information from CE, PE exchanges the VPN routing information with other PEs over BGP. A PE router only maintains the routing information of the VPN that is connected to it directly.

A P router only maintains the route destined for PE and does not need to know any VPN routing information.

When VPN traffic is transmitted in an MPLS backbone network, the ingress PE acts as an ingress label switch router (LSR), the egress PE acts as an egress LSR, and the P router acts as a transit LSR.

Packet Forwarding

In the basic MPLS L3VPN application (excluding cross-domain case), the double-tag mode is used for forwarding VPN packets.

- The first (outer layer) tag is exchanged within the backbone network and indicates an LSP from local PE to peer PE. VPN packets are forwarded using this tag to the peer PE along the LSP.
- The second (inner layer) tag is used when VPN packets are forwarded from the peer PE to CE. The tag indicates the site or the specific CE to which the packets must be sent. Therefore, the peer PE can find the interface that forwards the packet based on the inner layer tag.

Under special circumstances, two sites that belong to the same VPN are connected to the same PE. In this case, you only need to know how to reach the peer CE.

Figure 13-6 shows an example to illustrate the forwarding of VPN packets.

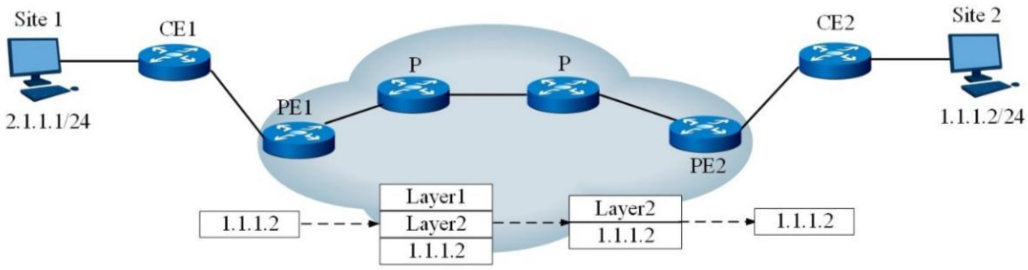


Figure 13-6 VPN packet forwarding diagram

1) Site 1 sends an IP packet whose destination address is 1.1.1.2, and the packet is transmitted by CE 1 to PE 1.

2) PE 1 searches for the VPN instance table entry according to the interface and destination address to be reached by the packet, forwards the packet after matching, and adds double tags (inner layer and outer layer tags) to the packet.

3) The MPLS network uses the outer layer tag of the packet to transmit the packet to PE 2 (the outer layer tag has been stripped before the packet reaches the previous hop of PE 2 and only the inner layer tag is retained).

4) PE 2 searches for the VPN instance table entry according to the inner layer tag and destination address, determines the outbound interface for the packet, and forwards the packet to CE 2.

5) CE 2 transmits the packet to the destination according to the normal IP forwarding process.

Routing Information Distribution

In the basic MPLS L3VPN network, the distribution of VPN routing information involves CE and PE. The P router only maintains the routing information of the backbone network and does not need to know any VPN routing information. A PE router only maintains the routing information of the VPN that is connected to it directly, but does not maintain all VPN routing information. Therefore, MPLS L3VPN is highly scalable.

The distribution process of VPN routing information includes three steps: from local CE to ingress PE, from ingress PE to egress PE, and from egress PE to remote CE. After these three steps are complete, a reachable route is established between local CE and remote CE, and VPN routing information can be distributed in the backbone network.

The three steps are described as follows.

1) Routing information exchange from local CE to ingress PE:

After establishing an adjacency relationship with the directly connected PE, CE distributes the VPN route of the local site to PE.
Routing protocols such as static routing, RIP, OSPF, IS-IS, or EBGP can be used between CE and PE. No matter which type of routing protocol is used, CE always distributes standard IPv4 routes to PE.

2) Routing information exchange from ingress PE to egress PE:

After learning the VPN routing information from CE, PE adds the route distinguisher (RD) and VPN target attributes to these standard IPv4 routes to form VPN-IPv4 routes to be saved in the VPN instance created for CE.

3) Routing information exchange from egress PE to remote CE:

There are multiple modes for the remote CE to learn VPN routing information from the egress PE, such as static routing, RIP, OSPF, IS-IS, and EBGP. The routing information exchange from egress PE to remote CE is the same as that from local CE to ingress PE.

13.10.2 Configuring L3VPN

In MPLS L3VPN, the carrier runs the MPLS VPN backbone network and provides VPN services by means of PE. VPN users are connected to the carrier's PE device over the CE device and access the MPLS VPN network to implement communication among different sites that belong to the user VPN. The basic configuration procedures of MPLS L3VPN are as follows:

1. Configure IGP in the P network and deploy MPLS LDP.
2. On PE, create VPN routing and forwarding (VRF) and designate the import/export policy of RD and route target (RT) for VPN customers.
3. Enable MP-BGP on PE and establish the VPNv4 neighbor relationship.
4. Run the PE-CE routing protocol.
5. Redistribute the PE-CE protocol to each other.

The MPLS L3VPN module performs the second step as mentioned above, namely the VPN instance configuration of MPLS L3VPN.

13.10.2.1 Creating a VPN Instance

Purpose

This section describes how to create a VPN instance and access the VPN instance view.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command.
Delete a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **no ip vpn-instance** *name* command.

13.10.2.2 Configuring an RD

Purpose

This section describes how to configure an RD.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the route distinguisher (RD) of a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **ipv4-family** or **ipv6-family** command to access the vpn-instance-af-ipv4 or vpn-instance-af-ipv6 configuration view. 4. Run the **route-distinguisher** *rd-string* command.

Caution

There is no default value for RD, which must be configured when you create the VPN instance.

13.10.2.3 Configuring a VPN Target

Purpose

This section describes how to configure a VPN target.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure a VPN target	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **ipv4-family** or **ipv6-family** command to access the vpn-instance-af-ipv4 or vpn-instance-af-ipv6 configuration view. 4. Run the **vpn-target** *target* **{ both | export-extcommunity | import-extcommunity }** command.
Delete all VPN targets associated with the current VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **ipv4-family** or **ipv6-family** command to access the vpn-instance-af-ipv4 or vpn-instance-af-ipv6 configuration view. 4. Run the **no vpn-target** command.
Delete a designated VPN target	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **ipv4-family** or **ipv6-family** command to access the vpn-instance-af-ipv4 or vpn-instance-af-ipv6 configuration view. 4. Run the **no vpn-target** *target* **{ both | export-extcommunity | import-extcommunity }** command.

Caution

There is no default value for VPN target, which must be configured when you create the VPN instance.

13.10.2.4 Configuring the Descriptive Information of a VPN Instance

Purpose

This section describes how to configure the descriptive information of a VPN instance.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Configure the descriptive information of a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **description** *description* command.
Delete the descriptive information of a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **no description** command.

13.10.2.5 Binding an Interface to a Designated VPN Instance

Purpose

This section describes how to bind an interface to a designated VPN instance.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Bind an interface to a designated VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, loopback interface configuration view, or BD configuration view. 3. Run the **ip binding vpn-instance** *name* command.
Unbind an interface from a VPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the corresponding command to access the VLANIF configuration view, Tunnel interface configuration view, loopback interface configuration view, or BD configuration view. 3. Run the **no ip binding vpn-instance** *name* command.

Caution

1. Running the **ip binding vpn-instance** command will delete the L3 attributes (such as IP address and routing protocol) configured on the interface. Reconfiguration is required if necessary.

2. The same interface cannot be used as the AC interface of both L2VPN and L3VPN. After an interface is bound to L2VPN, the L3 attributes (such as IP address and routing protocol) configured on the interface become invalid.

3. After configuring a VPN instance, you need to associate the interface belonging to this VPN on the device with this VPN instance; otherwise, this interface belongs to the public network.

4. Configuring association with a VPN instance on an interface or canceling the established association will clear the L3 attributes (such as IP address and routing protocol) of the interface. Reconfiguration is required if necessary.

5. Canceling the established association on the interface will clear the L3 attributes (such as IP address and routing protocol) of the interface. Reconfiguration is required if necessary.

13.10.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the MPLS L3VPN function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Display the configuration of a VPN instance	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-instance** *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the **show ip vpn-instance** command.
Display the details of a VPN instance	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-**

Purpose	Procedure
	instance *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the following commands: ● **show ip vpn-instance verbose;** ● **show ip vpn-instance** *vpn-instance-name* **verbose**
Display the configuration of a VPN instance	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-instance** *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the **show ip vpn-instance config** command.
Display all VPN instances with the specified egress VPN-target attribute	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-instance** *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the **show ip vpn-instance import-v**t *target* command.
Display information of introduced routes	1. Run the corresponding command to access the common user view. 2. Run the following commands: ● s**how import-route { all | imported };** ● **show import-route vpn-instance** *name* **{ all | imported }**
Enable L3VPN debugging	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-instance** *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the **debug l3vpn** { **io** | **event** | **all** } command.
Disable L3VPN debugging	1. Remain in the current privileged user view, or run the **configure** command to access the global configuration view, or run the **ip vpn-instance** *name* command in the global configuration view to access the VPN instance configuration view. 2. Run the **no debug l3vpn** { **io** | **event** | **all** } command.
Import the static route protocol over the public network	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance** *name* command to create a VPN instance and access the VPN instance configuration view. 3. Run the **ipv4-family** or **ipv6-family** command to access the vpn-instance-af-ipv4 or vpn-instance-af-ipv6 configuration view. 4. Run the following commands: ● **import-rib public protocol static;**

Purpose	Procedure
	● **import-rib public protocol static route-policy** *policy-name;* ● **import-rib vpn-instance** *vpn-instance-name* **protocol static;** ● **import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*; ● **no import-rib public protocol static;** ● **no import-rib vpn-instance** *vpn-instance-name* **protocol static.**
Import a VPN instance of the static route protocol	1. Run the **configure** command to access the global configuration view. 2. Run the following commands: ● **ip import-rib vpn-instance** *vpn-instance-name* **protocol static;** ● **ip import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*; ● **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static;** ● **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static route-policy** *policy-name*; ● **no ip import-rib vpn-instance** *vpn-instance-name* **protocol static;** ● **no ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol static.**
Enable or disable the L3VPN alarm function	1. Run the **configure** command to access the global configuration view. 2. Run the **ip vpn-instance snmp-trap { enable | disable }** command.

Chapter 14 Configuring Data Center Features

This chapter describes the basic content, configuration procedure, and configuration examples of VXLAN.

14.1 Configuring VXLAN

14.1.1 VXLAN Overview

Restrictions of traditional data center networks have facilitated emergence of new technologies. Virtual Extensible Local Area Network (VXLAN) is a result of joint efforts of global renowned vendors such as VMware and Cisco.

VXLAN is one of the Network Virtualization over Layer 3 (NVO3) technologies defined by IETF. VXLAN encapsulated L2 packets into L3 packets through L2 over L4 (MAC-in-UDP) to extend L2 packets to L3 packets and meet the requirements of great L2 virtual migration and multi-tenant requirements of data centers.

14.1.1.1 VXLAN Model

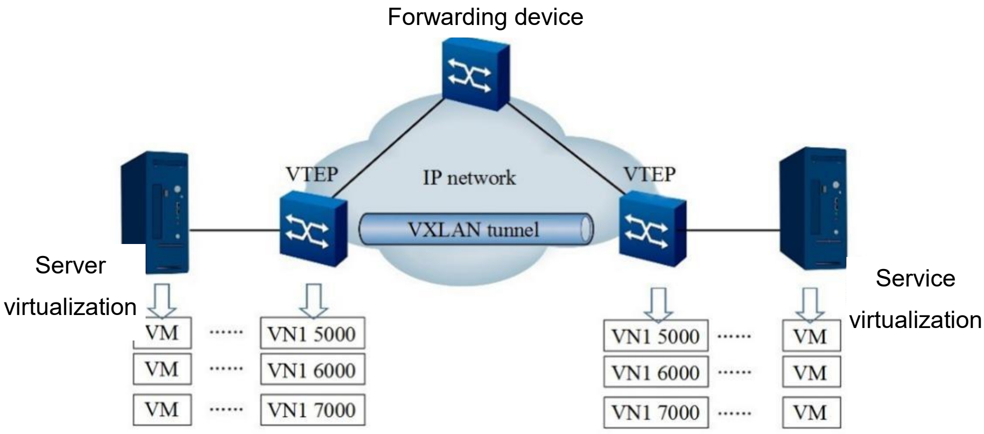


Figure 14-1 VXLAN model

As shown in Figure 14-1, VXLAN is added with the following new elements:

- VXLAN Tunnel Endpoints (VTEPs)

VTEPs are edge devices in VXLAN and the start and end points of a VXLAN tunnel. All VXLAN packets are processed on VTEP. A VTEP can be either an independent network device or a server where a virtual machine is located.

- VXLAN Network Identifier (VNI)

In an Ethernet data frame, VLAN only occupies 12 bits, which makes the isolation ability of VLAN in a data center network inadequate. VNI is designed to solve this problem. VNI is a kind of user identifier similar to VLAN ID. A VNI represents a tenant, and virtual machines with different VNIs cannot communicate directly at L2. When a VXLAN packet is encapsulated, enough space is allocated to VNI to support isolating a large number of tenants. The details will be introduced below.

- VXLAN tunnel

Tunnel is a logical concept. It is not new, such as GRE, which is familiar to everyone. It is used to package an original packet to facilitate transmission on a carrier network, such as an IP network. For hosts, there is a direct link between the start and end points of the original packet. This direct link is a tunnel. A VXLAN tunnel is used to transmit packets encapsulated by VXLAN and is a virtual tunnel between two VTEPs.

14.1.1.2 VXLAN Data Encapsulation Format

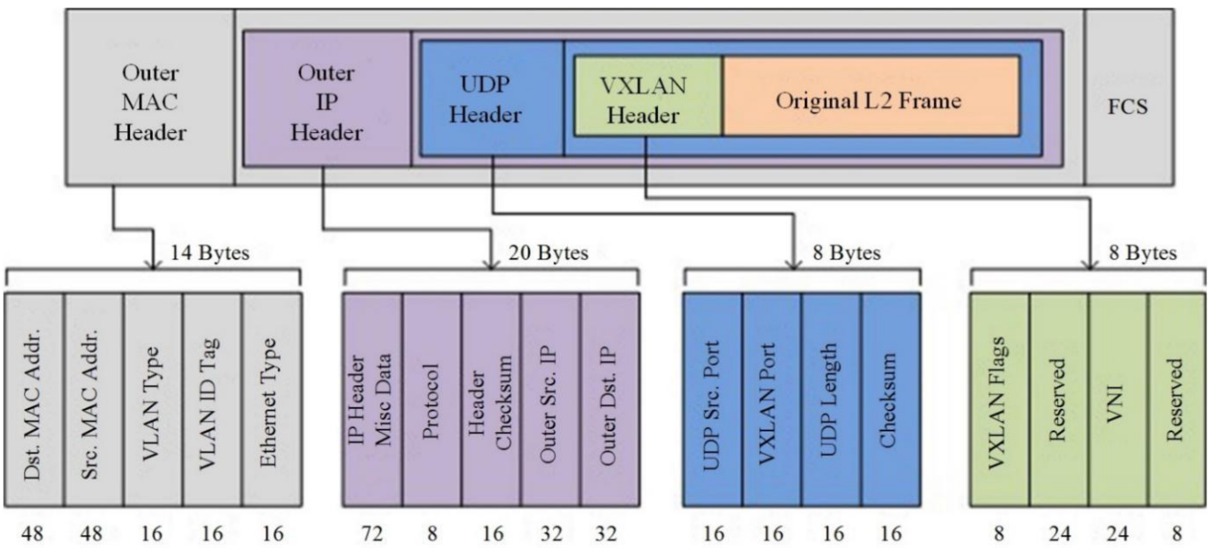


Figure 14-2 VXLAN data encapsulation format

As shown in Figure 14-2, VXLAN adopts the MAC-in-UDP encapsulation mode. It encapsulates the original data packet with a specific VXLAN header at the VTEP entrance and transmits the packet to the peer VTEP through a VXLAN tunnel, at which the packet is decapsulated (removing the header) and sent to the destination machine.

- VXLAN Header

A VXLAN header consists of 8 bytes, including a 24-bit VNI field, which is used to define different tenants in a VXLAN. The VXLAN header also contains an 8-bit VXLAN Flags field (value: 00001000), a 24-bit reserved field, and an 8-bit reserved field.

- UDP Header

The VXLAN header and the original Ethernet frame are used as UDP data. In the UDP header, the destination port number (VXLAN Port) is fixed at 4789, and the source port number (UDP Src. Port) is the value of the original Ethernet frame calculated by Hash algorithm.

- Outer IP Header

The outer IP header is encapsulated. In the outer IP header, the source IP address (Outer Src. IP) is the IP address of the VTEP to which the source VM belongs, and the destination IP address (Outer Dst. IP) is the IP address of the VTEP to which the destination VM belongs.

- Outer MAC Header

The outer Ethernet header is encapsulated. In the outer MAC header, the source MAC address (Src. MAC Addr.) is the MAC address of the VTEP to which the source VM belongs, and the destination MAC address (Dst. MAC Addr.) is the MAC address of the next hop device on the path to the destination VTEP.

14.1.1.3 VXLAN Packet Forwarding Mechanism

Establish a VXLAN Tunnel

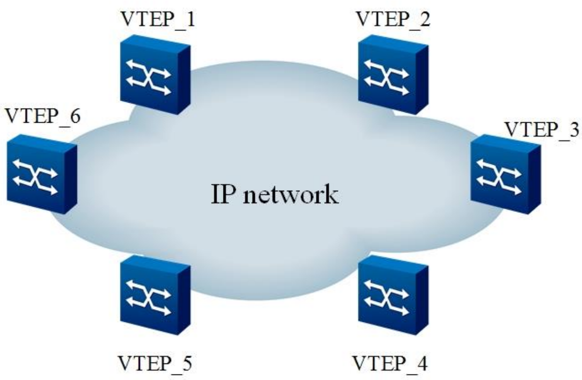


Figure 14-3 Network diagram of establishing a VXLAN Tunnel

As shown in Figure 14-3, the network has multiple VTEPs. Then, between which VTEPs do we need to establish a VXLAN tunnel? As we know, through the VXLAN tunnel, the L2 domains can break through the physical boundaries and realize the communication between VMs in L2 network. Therefore, if there is a need for great L2 intercommunication between VMs connected on different VTEPs, a VXLAN tunnel needs to be established between these two VTEPs. In other words, VXLAN tunnels need to be established between VTEPs in the same L2 domain.

For example, assume that, the VMs connected with VTEP_1, VTEP_2, and VTEP_3 in Figure 14-3 need great L2 intercommunication. You must establish VXLAN tunnels between every two of VTEP_1, VTEP_2, and VTEP_3, as shown in Figure 14-4.

Same great L2 domain is similar to a VLAN in a traditional network, but is called as bridge domain (BD) in a VXLAN.

As we know, VLANs are distinguished by VLAN ID, so how do distinguish BDs. As mentioned above, BDs are distinguished by VNI. For data center switches, there is a 1:1 mapping relationship between BDs VNIs, which is established by configuring the command line on VTEP. VTEP will generate the mapping table between BDs and VNIs according to the above configuration.

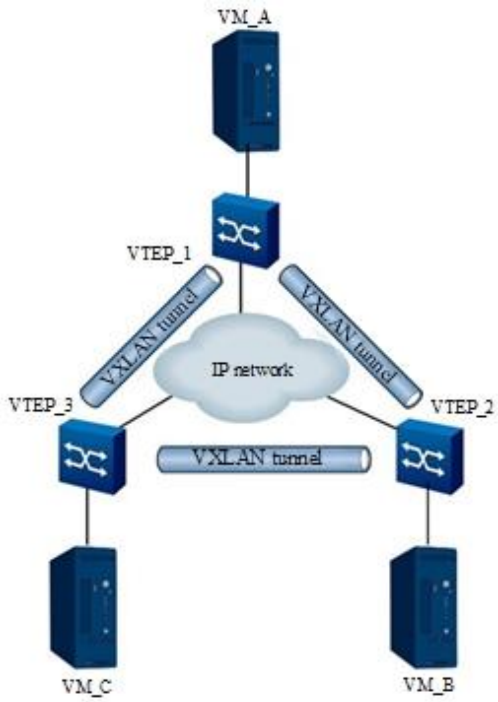


Figure 14-4 Network diagram of establishing a VXLAN tunnel

Packets Entering a VXLAN Tunnel

Not all packets entering the switch will pass through the VXLAN tunnel (or the packets may just undergo the ordinary L2 or L3 forwarding process). Three types of interfaces are defined in traditional networks: Access, Trunk, and Hybrid. These three types of interfaces have different application scenarios but the ultimate purpose: check which packets are allowed to pass according to the configuration, and judge how to handle the packets that passed the check.

In a VXLAN, VTEP interfaces undertake similar tasks. However, in data center switches, these interfaces are not physical interfaces. They are logic interfaces called L2 sub-interfaces. L2 sub-interfaces check which packets need to enter the VXLAN tunnel based on the configuration, and determine the action for the packets that passed the check.

Stream encapsulation type	Types of Packets Allowed to Enter a VXLAN Tunnel	Processing before encapsulating packets	Processing after receiving and decapsulating VXLAN packets
dot1q	Only packets with the specified VLAN tag are allowed to enter the VXLAN tunnel. (you can run the corresponding command to specify the VLAN tag)	Before VXLAN encapsulation, the outer VLAN tag of the original packet is removed.	After VXLAN decapsulation: If the inner original packet carries a VLAN tag, replace this VLAN tag with the specified VLAN tag and then forward the packet. If the inner original packet carries no VLAN tag, add the specified VLAN tag to the packet and then forward the packet.
untag	Only packets without VLAN tag are allowed to enter the VXLAN tunnel.	Before VXLAN encapsulation, no VLAN tag is added to the original packet.	After VXLAN decapsulation, no VLAN tag is added to, replaced, or removed from the original packet.
default	All packets, with or without VLAN tag, are allowed to enter the VXLAN tunnel.	Before VXLAN encapsulation, no VLAN tag is added to, replaced, or removed from the original packet.	After VXLAN decapsulation, no VLAN tag is added to, replaced, or removed from the original packet.

Only the L2 sub-interface is added to the specified BD. Then, the BD to which the packet can be determined based on configuration of the L2 sub-interface. Sub-interfaces of the default type are generally used in scenarios where packets passing through such interfaces must be transmitted in the same VXLAN tunnel. In other words, all VMs of such interfaces must belong to the same BD. When part of packets passing through a physical interface have a VLAN tag while others passing through the same physical interface do not have a VLAN tag and these packets need to enter different VXLAN tunnels, you can create both dot1q and untag L2 sub-interfaces on this physical interfaces.

14.1.2 Configuring a VXLAN

Purpose

This section describes how to configure a VXLAN.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create a BD and access the BD configuration view	1. Run the **configure** command. 2. Run the **bridge-domain** *bd-id* command.
Delete a BD	1. Run the **configure** command. 2. Run the **no bridge-domain** *bd-id* command.
Create an L3 BD and access its view	1. Run the corresponding command to access the global configuration view, interface configuration view (Ethernet or Trunk), VLAN configuration view, interface group configuration view, or VLANIF interface configuration view. 2. Run the **interface bridge-domain** *bd-id* command.
Bind a VNI to a BD	1. Run the **configure** command. 2. Run the **bridge-domain** *bd-id* command. 3. Run the **vxlan vni** *vni-id* command.
Delete a VNI bound to a BD	1. Run the **configure** command. 2. Run the **bridge-domain** *bd-id* command. 3. Run the **no vxlan vni** *vni-id* command.
Bind a BD to a sub-interface	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **bridge-domain bind** *bd-id* command.
Delete a BD bound to a sub-interface	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **no bridge-domain bind** command.
Configure the encapsulation mode for a sub-interface	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the e**ncapsulation { dot1q | untag | qinq |default }** command.

Purpose	Procedure
Configure a VLAN for a sub-interface with the encapsulation mode dot1q	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **encapsulation dot1q** *vlan-id* command
Delete the VLAN configured for a sub-interface with the encapsulation mode dot1q	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **no encapsulation dot1q** *vlan-id* command.
Configure two VLANs for a sub-interface with the encapsulation mode dot1q	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **encapsulation qinq** *vlan1-id* **ce-vid** *vlan2-id* command.
Delete the two VLANs configured for an interface with the encapsulation mode dot1q	1. Run the **configure** command. 2. Run the command **interface { ethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*. 3. Run the **no encapsulation qinq** *vlan1-id* **ce-vid** *vlan2-id* command.
Create an NVE and access its view	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command.
Delete an NVE view	1. Run the **configure** command. 2. Run the **no interface nve** *nve-id* command.
Configure a VNI for a tunnel and the IP address of the peer	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command. 3. Run the **vni** *id* **ucast-peer** *peer-ip-address* command.
Delete all peers with different VNIs under an NVE interface	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command. 3. Run the **no vni** *id* **peer** command.
Delete the tunnel with the specified VNI and IP address	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command. 3. Run the **no vni** *id* **ucast-peer** *peer-ip-address* command.
Configure the source IP address of a tunnel	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command. 3. Run the **tunnel source** *ip-address* command.

Purpose	Procedure
Delete the source IP address of a tunnel	1. Run the **configure** command. 2. Run the **interface nve** *nve-id* command. 3. Run the **no tunnel source** command.
Enable the switch to forward or drop unknown unicast packets on a BD interface or disable the function	1. Run the **configure** command. 2. Run the **bridge-domain** *bd-id* command. 3. Run the **unknown-ucast { forward | drop }** command.

14.1.3 Configuring GRPC Logs

Purpose

This section describes how to configure GRPC logs.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the GRPC log	1. Run the **configure** command. 2. Run the command **debug grpc { api | cares_address_sorting | cares_resolver | client_channel_call | client_channel_routing | http | http_keepalive | chttp2_refcount | channel | combiner | tcp | polling | fd_trace | fd_refcount | polling_api | executor | timer | timer_check|op_failure | pending_tags | cq_refcount | queue_pluck | connectivity_state | resource_quota | all } { on | off }**.
Set a GRPC debugging level	1. Run the **configure** command. 2. Run the **grpc debug-level { debug | info | error | none }** command.

14.1.4 Configuring DID

Purpose

This section describes how to configure the destination IP detect (DID) function.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Debug DID	1. Remain in the privileged user view. 2. Run the **debug did** { **event** | **detect** | **cmd** | **off** | **all** } command.
View the DID peer information	1. Access the common user view. 2. Run the **show did peer** command.
View the DID resource information	1. Access the common user view. 2. Run the **show did resource** command.

14.1.5 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the VXLAN function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable VXLAN debugging	1. Remain in the current privileged user view. 2. Run the **debug vxlan { event | detect | did | hw | off | all }** command.
Display BD information	1. Run the corresponding command to access the common user view, privileged user view, or global configuration view. 2. Run the following commands: ● The **show bridge-domain** command displays all the configured L2 BD interface information, including the BD interface number, bound VNI, unknown unicast configuration, statistics collection on enabling or disabling, and bound sub-interface. ● The **show bridge-domain** *domain-id* command displays the configuration of a specified L2 BD interface.

Purpose	Procedure
Display VNI information	1. Run the corresponding command to access the privileged user view or global configuration view. 2. Run the **show vxlan vni** command.
Display information about VXLAN resources	1. Run the corresponding command to access the privileged user view or global configuration view. 2. Run the **show vxlan resourse** command.
Display information about all NVE peers or filtered information	1. Run the corresponding command to access the common user view, privileged user view, or global configuration view. 2. Run the **show nve peer or show nve peer verbose** command.
Display NVE information on interfaces	1. Run the corresponding command to access the common user view, privileged user view, or global configuration view. 2. Run the **show interface nve** command.
Display the reference count of a BD interface	1. Run the corresponding command to access the common user view. 2. Run the **show l3int bridge-domain** *domain-id* command.

14.1.6 Configuration Example

14.1.6.1 Typical Scenario (Static Tunnel) in Which Users in the Same Network Segment Interconnect with Each Other Through a VXLAN Tunnel

Network Requirements

As shown in Figure 14-5, PC1 and PC3 are in the same network segment and interconnect with each other through the VXLAN tunnel between VTEP1 and VTEP2.

VTEP1 connects to PC1 through GE1/0/1 and connects to VTEP2 through GE1/0/2. VTEP2 connects to PCS through GE1/01 and connects to VTEP1 through GE1/0/2. VTEP1 and VTEP2 interconnect with each other through VLAN 10 at L3.

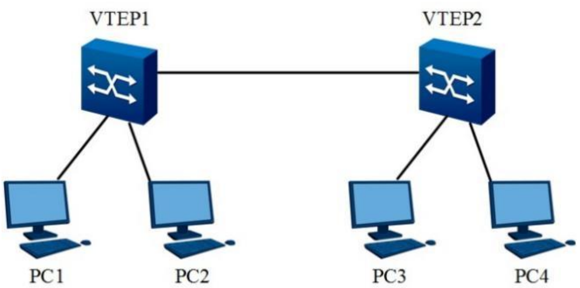


Figure 14-5 Network diagram of basic VXLAN L2 interconnection

Configuration Suggestion

Configure basic VXLAN L2 interconnection functions as follows:

1. Create an L3 connection between VTEP1 and VTEP2.
2. Bind sub-interfaces to BDs at the access side of VTEP1 and VTEP2.
3. Configure an NVE interface and tunnel for VTEP1 and VTEP2.

Data Preparation

Prepare the following data to complete the configuration in this example:

Network interface through which network members can interconnect with each other.

The interconnected IP addresses of L3 VLAN 10 through which VTEP1 and VTEP2 are connected are 10.18.1.1/24 and 10.18.1.2/24.

Bind BD interface 1 at the access side of VTEP1 to VNI 100. Bind BD interface 5 at the access side of VTEP2 to VNI 100.

Set the access mode for the sub-interface through which VTEP1 connects to PC1 to VLAN 5 untag and bind it to BD 1. Set the access mode for the sub-interface through which VTEP2 connects to PC3 to VLAN 5 untag and bind it to BD 5.

Configure a network-side NVE interface, tunnel VNI 100, and source and destination IP addresses for VTEP1 and VTEP2, respectively.

Test Procedure

Step 1 Configure VTEP1.

Configure a BD interface.

VTEP1(config)#bridge-domain 1

VTEP1(config-bridge-domain-1)#vxlan vni 100

VTEP1(config-bridge-domain-1)#exit

Configure the access mode for a sub-interface to tag, untag, or qinq as needed.

VTEP1(config)#interface 10gigaethernet 1/0/1.1

VTEP1(config-10ge1/0/1.1)#no shutdown

VTEP1(config-10ge1/0/1.1)#encapsulation untag 5

VTEP1(config-10ge1/0/1.1)#bridge-domain bind 1

VTEP1(config-10ge1/0/1.1)#exit

Configure a network interface connecting with VTEP2.

VTEP1(config)#interface vlan 20

VTEP1(config-vlan-20)#ip address 10.18.1.1 255.255.255.0

VTEP1(config-vlan-20)#exit

VTEP1(config)#interface 10gigaethernet 1/0/2

VTEP1(config-10ge1/0/2)#no shutdown

VTEP1(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP1(config-10ge1/0/2)#port hybrid pvid 20

VTEP1(config-10ge1/0/2)#exit

Configure a VXLAN tunnel for the NVE interface.

VTEP1(config)#interface nve 1

VTEP1(config-nve-1)#tunnel source 10.18.1.1

VTEP1(config-nve-1)#vni 100 ucast-peer 10.18.1.2

VTEP1(config-nve-1)#exit

Step 2 Configure VTEP2 in the same way as VTEP1 with reversed source and destination tunnel addresses.

Configure a BD interface.

VTEP2(config)#bridge-domain 5

VTEP2(config-bridge-domain-5)#vxlan vni 100

VTEP2(config-bridge-domain-5)#exit

Configure the access mode for a sub-interface.

VTEP2(config)#interface 10gigaethernet 1/0/1.1

VTEP2(config-10ge1/0/1.1)#no shutdown

VTEP2(config-10ge1/0/1.1)#encapsulation untag 5

VTEP2(config-10ge1/0/1.1)#bridge-domain bind 5

VTEP2(config-10ge1/0/1.1)#exit

Configure a network interface connecting with VTEP1.

VTEP2(config)#interface vlan 20

VTEP2(config-vlan-20)#ip address 10.18.1.2 255.255.255.0

VTEP2(config-vlan-20)#exit

VTEP2(config)#interface 10gigaethernet 1/0/2

VTEP2(config-10ge1/0/2)#no shutdown

VTEP2(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP2(config-10ge1/0/2)#port hybrid pvid 20

VTEP2(config-10ge1/0/2)#exit

Configure a VXLAN tunnel for the NVE interface.

VTEP2(config)#interface nve 1

VTEP2(config-nve-1)#tunnel source 10.18.1.2

VTEP2(config-nve-1)#vni 100 ucast-peer 10.18.1.1

VTEP2(config-nve-1)#exit

Step 3 Debug VXLAN.

After configuring VTEP1 and VTEP2, ping PC3 from PC1. If PC3 cannot be pinged, view the MAC address tables on VTEP1 and VTEP2 and check whether the MAC address of the PC3 VXLAN tunnel is displayed on VTEP1 and whether the MAC address of the PC1 on VTEP2. If not, check whether the two ends of the tunnel can be pinged.

14.1.6.2 Typical Scenario (Static Tunnel) in Which Users in Different Network Segments Interconnect with Each Other Through a VXLAN Tunnel

Network Requirements

As shown in Figure 14-6, PC1 and PC3 are in different network segments and interconnect with each other through the VXLAN tunnel among VTEP1, L3GW, and VTEP2.

VTEP1 connects to PC1 through GE 1/0/1 and connects to L3GW through GE 1/0/2. VTEP2 connects to PC3 through GE 1/0/1 and connects to L3GW through GE 1/0/2. L3GW connects to VTEP1 through GE1/0/2 and connects to VTEP2 through GE1/0/3.

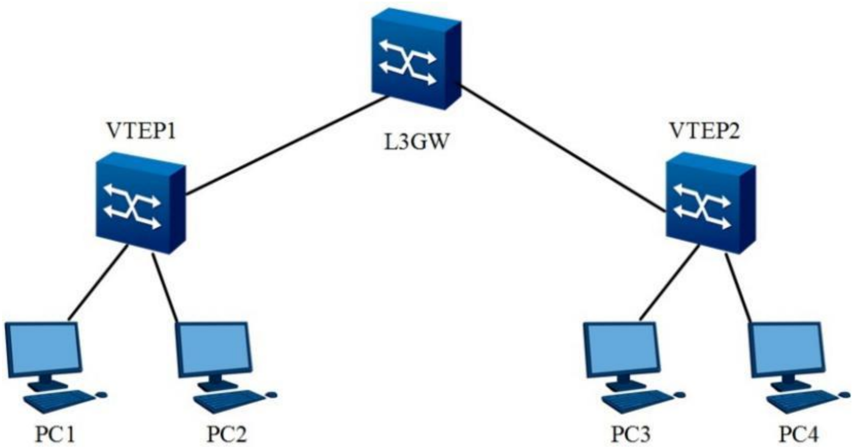


Figure 14-6 Network diagram of basic VXLAN L3 interconnection

Configuration Suggestion

Configure basic VXLAN L3 interconnection functions as follows:

1. Create an L3 connection among VTEP1, L3GW, and VTEP2. Established a VXLAN tunnel between VTEP1 and L3 gateway, and between VTEP2 and L3 gateway.
2. Bind sub-interfaces to BDs at the access side of VTEP1 and VTEP2. Configure an NVE interface and tunnel at the network side of VTEP1 and VTEP2.

Configure an NVE interface and tunnel at two sides of the L3GW device and configure the L3 BD interface as the gateway of PCs at two sides.

Data Preparation

Prepare the following data to complete the configuration in this example:

Network interface through which network members can interconnect with each other.

The interconnected IP addresses of L3 VLAN 10 to which VTEP1 and L3GW are connected are 10.18.1.1/24 and 10.18.1.2/24. The interconnected IP addresses of L3 VLAN 20 to which VTEP2 and L3GW are connected are 10.18.2.1/24 and 10.18.2.2/24.

Bind BD interface 1 at the access side of VTEP1 to VNI 100. Bind BD interface 5 at the access side of VTEP2 to VNI 200.

Set the access mode for the sub-interface through which VTEP1 connects to PC1 to VLAN 5 untag and bind it to BD 1. Set the access mode for the sub-interface through which VTEP2 connects to PC3 to VLAN 50 untag and bind it to BD 5.

Configure a network-side NVE interface, tunnel VNI 100, and source and destination IP addresses for VTEP1 and VTEP2, respectively.

Configure an NVE interface, and a tunnel through which L3GW connects to VTEP1 and VTEP2.

Configure L3 BD interface 100 as the PC1 gateway and BD interface 200 as the PC3 gateway.

Test Procedure

Step 1 Configure VTEP1.

Configure a BD interface.

VTEP1(config)#bridge-domain 1

VTEP1(config-bridge-domain-1)#vxlan vni 100

VTEP1(config-bridge-domain-1)#exit

Configure the access mode for a sub-interface.

VTEP1(config)#interface 10gigaethernet 1/0/1.1

VTEP1(config-10ge1/0/1.1)#no shutdown

VTEP1(config-10ge1/0/1.1)#encapsulation untag 5

VTEP1(config-10ge1/0/1.1)#bridge-domain bind 1

VTEP1(config-10ge1/0/1.1)#exit

Configure a network interface connecting with L3GW.

VTEP1(config)#interface vlan 10

VTEP1(config-vlan-10)#ip address 10.18.1.1 255.255.255.0

VTEP1(config-vlan-10)#exit

VTEP1(config)#interface 10gigaethernet 1/0/2

VTEP1(config-10ge1/0/2)#no shutdown

VTEP1(config-10ge1/0/2)#port hybrid vlan 10 untagged

VTEP1(config-10ge1/0/2)#port hybrid pvid 10

VTEP1(config-10ge1/0/2)#exit

Configure a VXLAN tunnel for the NVE interface.

VTEP1(config)#interface nve 1

VTEP1(config-nve-1)#tunnel source 10.18.1.1

VTEP1(config-nve-1)#vni 100 ucast-peer 10.18.1.2

VTEP1(config-nve-1)#exit

Step 2 Configure VTEP2 in the same way as VTEP1.

Configure a BD interface.

VTEP2(config)#bridge-domain 5

VTEP2(config-bridge-domain-5)#vxlan vni 200

VTEP2(config-bridge-domain-5)#exit

Configure the access mode for a sub-interface.

VTEP2(config)#interface 10gigaethernet 1/0/1.1

VTEP2(config-10ge1/0/1.1)#no shutdown

VTEP2(config-10ge1/0/1.1)#encapsulation untag 50

VTEP2(config-10ge1/0/1.1)#bridge-domain bind 5

VTEP2(config-10ge1/0/1.1)#exit

Configure a network interface connecting with VTEP1.

VTEP2(config)#interface vlan 20

VTEP2(config-vlan-20)#ip address 10.18.2.1 255.255.255.0

VTEP2(config-vlan-20)#exit

VTEP2(config)#interface 10gigaethernet 1/0/2

VTEP2(config-10ge1/0/2)#no shutdown

VTEP2(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP2(config-10ge1/0/2)#port hybrid pvid 20

VTEP2(config-10ge1/0/2)#exit

Configure a VXLAN tunnel for the NVE interface.

VTEP2(config)#interface nve 1

VTEP2(config-nve-1)#tunnel source 10.18.2.1

VTEP2(config-nve-1)#vni 200 ucast-peer 10.18.2.2

VTEP2(config-nve-1)#exit

Step 3 Configure L3GW.

Configure an L3 interface for interconnecting with VTEP1 and VTEP2.

L3GW(config)#interface vlan 10

L3GW(config-vlan-10)#ip address 10.18.1.2 255.255.255.0

L3GW(config-vlan-10)#exit

L3GW(config)#interface vlan 20

L3GW(config-vlan-20)#ip address 10.18.2.2 255.255.255.0

L3GW(config-vlan-20)#exit

L3GW(config)#interface 10gigaethernet 1/0/2

L3GW(config-10ge1/0/2)#no shutdown

L3GW(config-10ge1/0/2)#port hybrid vlan 10 untagged

L3GW(config-10ge1/0/2)#port hybrid pvid 10

L3GW(config-10ge1/0/2)#exit

L3GW(config)#interface 10gigaethernet 1/0/3

L3GW(config-10ge1/0/2)#no shutdown

L3GW(config-10ge1/0/2)#port hybrid vlan 20 untagged

L3GW(config-10ge1/0/2)#port hybrid pvid 20

L3GW(config-10ge1/0/2)#exit

Configure a VXLAN tunnel for the NVE interface.

L3GW(config)#interface nve 1

L3GW(config-nve-1)#tunnel source 10.18.1.2

L3GW(config-nve-1)#vni 100 ucast-peer 10.18.1.1

L3GW(config-nve-1)#exit

L3GW(config)#interface nve 2

L3GW(config-nve-2)#tunnel source 10.18.2.2

L3GW(config-nve-2)#vni 200 ucast-peer 10.18.2.1

L3GW(config-nve-2)#exit

Configure an L3 BD interface.

L3GW(config)#bridge-domain 1

L3GW(config-bridge-domain -1)#vxlan vni 100

L3GW(config-bridge-domain-1)#exit

L3GW(config)#interface bridge-domain 1

L3GW(config-if-bridge-domain1)#ip address 10.18.3.254 255.255.255.0

L3GW(config-if-bridge-domain1)# exit

L3GW(config)#bridge-domain 2

L3GW(config-bridge-domain-2)#vxlan vni 200

L3GW(config-bridge-domain-2)#exit

L3GW(config)#interface bridge-domain 2

L3GW(config-if-bridge-domain2)#ip address 10.18.4.254 255.255.255.0

L3GW(config-if-bridge-domain2)#exit

Step 4 Debug VXLAN.

After configuring VTEP1, VTEP2, and L3GW, ping PC3 from PC1. If PC3 cannot be pinged, view the ARP address table on L3GW and check whether ARPs of PC1 and PC3 VXLAN tunnel are displayed. If not, check whether L3GW can ping the two ends of the VTEP1 and VTEP2 tunnel.

14.2 Configuring EVPN

14.2.1 EVPN Overview

Ethernet Virtual Private Network (EVPN) is an L2 VPN technology. The control plane uses MP-BGP to advertise EVPN routing information, and the data plane uses VXLAN encapsulation to forward packets. EVPN has the following features except for the advantages of MP-BGP and VXLAN:

- Simple configuration: It realizes automatic discovery of VTEPs, automatic establishment of VXLAN tunnels and automatic association between VXLAN tunnels and VXLANs through MP-BGP, which reduces the difficulty of network deployment.
- Isolation between control plane and data plane: The control plane is responsible for issuing routing information, and the data plane is responsible for forwarding packets, which is easy to manage.
- Support to Integrated Bridging and Routing (IRB): MP-BGP issues both L2 MAC addresses and L3 routing information, and VTEPs can perform L2 forwarding and L3 routing. The optimal path forwarding of traffic is adopted, which reduces the broadcast traffic.

14.2.2 Configuring EVPN

Purpose

This section describes how to configure EVPN.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Create an EVPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **bridge-domain** *bd-id* command to access the BD configuration view. 3. Run the **evpn** command.
Delete an EVPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **bridge-domain** *bd-id* command to access the BD configuration view.

Purpose	Procedure
	3. Run the **no evpn** command.
Configure an RD for an EVPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **bridge-domain** *bd-id* command to access the BD configuration view. 3. Run the **evpn** command to access the EVPN instance. 4. Run the **evpn route-distinguisher** *rdstring* command.
Configure a target for an EVPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **bridge-domain** *bd-id* command to access the BD configuration view. 3. Run the **evpn** command to access the EVPN instance. 4. Run the **evpn vpn-target target { both | export-extcommunity | import-extcommunity }** command.
Delete a target for an EVPN instance	1. Run the **configure** command to access the global configuration view. 2. Run the **bridge-domain** *bd-id* command to access the BD configuration view. 3. Run the **evpn** command to access the EVPN instance. 4. Run the following commands: ● **no evpn vpn-target** ● **no evpn vpn-target target { both | export-extcommunity | import-extcommunity }**

14.2.3 Maintenance and Debugging

Purpose

This section describes how to check, debug or locate the fault when the EVPN function fails to work.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable EVPN debugging	1. Run the **configure** command to access the global configuration view or remain in the privileged user view. 2. Run the **debug evpn** { **error** | **nm** | **event** | **all** } command.
Disable EVPN debugging	1. Run the **configure** command to access the global configuration view or remain in the privileged user view.

Purpose	Procedure
	2. Run the **no debug evpn** { **error** | **nm** | **event** | **all** } command.
View information about an EVPN instance	1. Run the **configure** command to access the global configuration view or remain in the privileged user view. 2. Run the **show evpn or show evpn vpn-target** command.
View the BGP EVPN route information	1. Run the corresponding command to access the privileged user view. 2. Run the following commands: ● **show ip bgp evpn route;** ● **show ip bgp evpn route { mac-ip | prefix | tunnel };** ● **show ip bgp evpn route arp** *ip-address*; ● **show ip bgp evpn route count;** ● **show ip bgp evpn route mac** *mac-address*; ● **show ip bgp evpn route nd** *ipv6-address*; ● **show ip bgp evpn route prefix** *ip-address*; ● **show ip bgp evpn route prefix** *ipv6-address*; ● **show ip bgp evpn route tunnel** *tunnel-source-ip-address tunnel-vni;* ● **show ip bgp evpn route tunnel** *tunnel-source-ipv6-address tunnel-vni;* ● **show ip bgp evpn route { arp | nd } peer** *peer-ipv4-address* **l2vni** *vni-id* **l3vni** *vni-id*; ● **show ip bgp evpn route { arp | nd }** *peer peer-ipv6-address* **l2vni** *vni-id* **l3vni** *vni-id*; ● **show ip bgp evpn route { arp | nd | prefix } peer** *peer-ipv4-address* **l3vni** *vni-id*; ● **show ip bgp evpn route { arp | nd | prefix } peer** *peer-ipv6-address* **l3vni** *vni-id*; ● **show ip bgp evpn route { mac | arp | nd } peer** *peer-ipv4-address* **l2vni** *vni-id*; ● **show ip bgp evpn route { mac | arp | nd } peer** *peer-ipv6-address* **l2vni** *vni-id*; ● **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer** *peer-ipv4-address*; ● **show ip bgp evpn route { mac | arp | nd | prefix | tunnel } peer** *peer-ipv6-address*

14.2.4 Configuration Example

Network Requirements

In an EVPN-based data center L2 application scenario, it is required that S2 and S3 can interconnect with each other at L2 and VMA and VMG can access each other.

Network Diagram

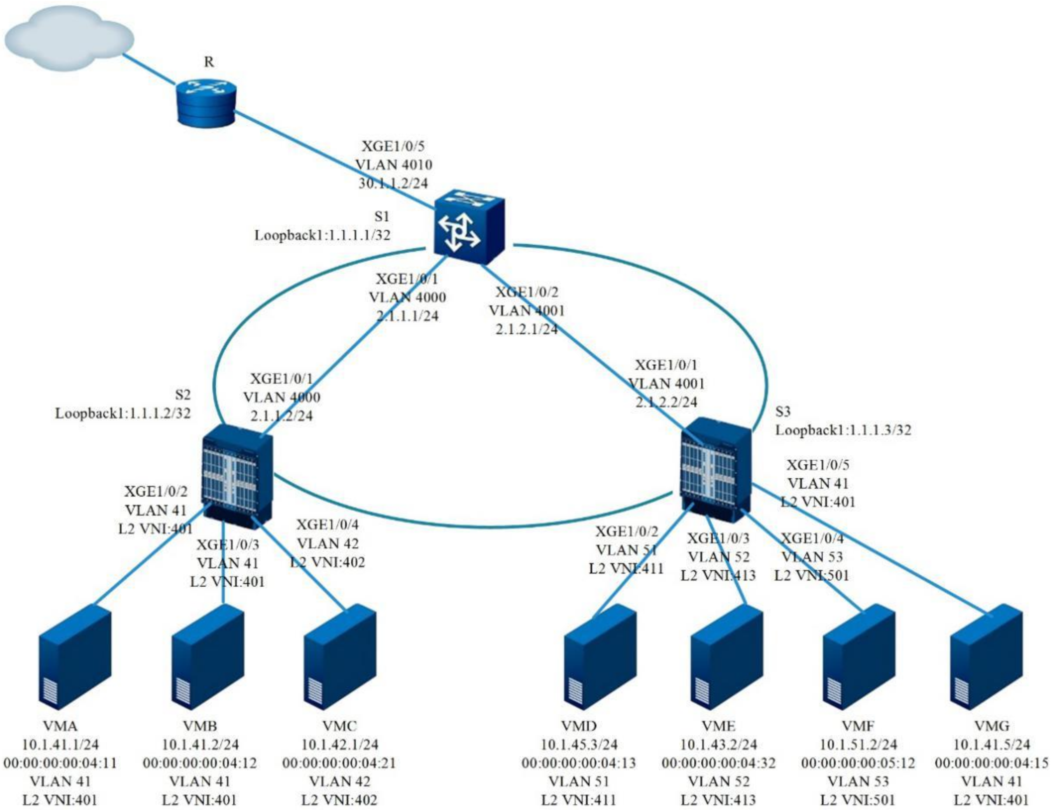


Figure 14-7 EVPN network diagram

Configuration

1. Configure a name for S1, S2, and S3 respectively, create a VLAN, and add interfaces to the VLAN.

// Configure S1:

Switch(config)#

Switch(config)#hostname S1

S1(config)#vlan 4000,4001

Info: This operation may take a few seconds. Please wait for a moment....done.

S1(config)#interface xgigaethernet 1/0/1

S1(config-10ge1/0/1)#port link-type trunk

```
S1(config-10ge1/0/1)#port trunk allow-pass vlan 4000
S1(config-10ge1/0/1)#quit
S1(config)#interface xgigaethernet 1/0/2
S1(config-10ge1/0/2)#port link-type trunk
S1(config-10ge1/0/2)#port trunk allow-pass vlan 4001
S1(config-10ge1/0/2)#

// Configure S2:
Switch(config)#
Switch(config)#hostname S2
S2(config)#vlan 4000
S2(vlan-4000)#quit
S2(config)#interface xgigaethernet 1/0/1
S2(config-10ge1/0/1)#port link-type trunk
S2(config-10ge1/0/1)#port trunk allow-pass vlan 4000
S2(config-10ge1/0/1)#

// Configure S3:
Switch(config)#
Switch(config)#hostname S3
S3(config)#vlan 4001
S3(vlan-4001)#quit
S3(config)#interface xgigaethernet 1/0/1
S3(config-10ge1/0/1)#port link-type trunk
S3(config-10ge1/0/1)#port trunk allow-pass vlan 4001
S3(config-10ge1/0/1)#
```

2 Configure the IP addresses of the VLAN interface and loopback interface.

```
// Configure S1:
S1(config)#
S1(config)#interface loopback 1
S1(config-loopback-1)#ip address 1.1.1.1/32
S1(config-loopback-1)#quit
S1(config)#interface vlan 4000
S1(config-vlan-4000)#ip address 2.1.1.1/24
S1(config-vlan-4000)#quit
```

S1(config)#interface vlan 4001
S1(config-vlan-4001)#ip address 2.1.2.1/24
S1(config-vlan-4001)#quit
S1(config)#

// Configure S2:
S2(config)#
S2(config)#interface loopback 1
S2(config-loopback-1)#ip address 1.1.1.2/32
S2(config-loopback-1)#quit
S2(config)#interface vlan 4000
S2(config-vlan-4000)#ip address 2.1.1.2/24
S2(config-vlan-4000)#quit
S2(config)#

// Configure S3:
S3(config)#
S3(config)#interface loopback 1
S3(config-loopback-1)#ip address 1.1.1.3/32
S3(config-loopback-1)#quit
S3(config)#interface vlan 4001
S3(config-vlan-4001)#ip address 2.1.2.2/24
S3(config-vlan-4001)#quit
S3(config)#

3. Enable the OSPF routing protocol for S1, S2, and S3 and implement L3 loopback interface interconnection.

// Configure S1:
S1(config)#router ospf 1
S1(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0
S1(config-ospf-1)#network 2.1.1.0 255.255.255.0 area 0
S1(config-ospf-1)#network 2.1.2.0 255.255.255.0 area 0
S1(config-ospf-1)#

// Configure S2:

```
S2(config)#router ospf 1
S2(config-ospf-1)#network 1.1.1.2 255.255.255.255 area 0
S2(config-ospf-1)#network 2.1.1.0 255.255.255.0 area 0
S2(config-ospf-1)#
```

// Configure S3:

```
S3(config)#router ospf 1
S3(config-ospf-1)#network 1.1.1.3 255.255.255.255 area 0
S3(config-ospf-1)#network 2.1.2.0 255.255.255.0 area 0
S3(config-ospf-1)#
```

4. After the OSPF route is configured, loopback interfaces can be connected with each other. Take S2 ping S3 as an example.

```
S2(config)#ping 1.1.1.3
  Pinging 1.1.1.3 with 64 bytes of data:
  Reply from 1.1.1.3: bytes=64 time=10ms TTL=63 icmp_seq=1
  Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=2
  Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=3
  Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=4
  Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=5

Ping statistics for 1.1.1.3 :
        Packets:Send = 5,   Received = 5 , Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms,   Maximum = 10ms , Average = 2ms
S2(config)#
```

5. Configure EVPN instances on S2 and S3.

// Configure S2:

```
S2(config)#bridge-domain 401
S2(config-bridge-domain401)#vxlan vni 401
S2(config-bridge-domain401)#evpn
S2(config-bridge-domain401)#evpn route-distinguisher 1:401
S2(config-bridge-domain401)#evpn vpn-target 1:401 both
```

// Configure S3:

S3(config)#bridge-domain 401

S2(config-bridge-domain401)#vxlan vni 401

S2(config-bridge-domain401)#evpn

S2(config-bridge-domain401)#evpn route-distinguisher 1:401

S2(config-bridge-domain401)#evpn vpn-target 1:401 both

6. Set the NVE neighbor learning protocol on S2 and S3 to BGP.

// Configure S2:

S2(config)#interface nve 2

S2(config-nve2)#tunnel source 1.1.1.2

S2(config-nve2)#vni 401 replication-protocol bgp

// Configure S3:

S3(config)#interface nve 2

S3(config-nve2)#tunnel source 1.1.1.3

S3(config-nve2)#vni 401 replication-protocol bgp

7. Configure a BGP neighbor of S2 and S3 and enable the EVPN address family.

// Configure S2:

S2(config)#router bgp 100

S2(config-bgp)#neighbor 1.1.1.3 remote-as 100

S2(config-bgp)#neighbor 1.1.1.3 update-source 1.1.1.2

S2(config-bgp)#evpn-family

S2(config-bgp-af-evpn)#neighbor 1.1.1.3 enable

S2(config-bgp-af-evpn)#exit

S2(config-bgp)#exit

S2(config)#

// Configure S3:

S3(config)#router bgp 100

S3(config-bgp)#neighbor 1.1.1.2 remote-as 100

S3(config-bgp)#neighbor 1.1.1.2 update-source 1.1.1.3

S3(config-bgp)#evpn-family

S3(config-bgp-af-evpn)#neighbor 1.1.1.2 enable

S3(config-bgp-af-evpn)#exit

S3(config-bgp)#exit

S3(config)#

14.3 Configuring NETCONF

14.3.1 NETCONF Overview

Overview of NETCONF

Network Configuration Protocol (NETCONF) is an effective method to solve configuration problems in network management and considered as a next-generation network management protocol. NETCONF is defined in RFC 6241 to replace the Command Line Interface (CLI), Simple Network Management Protocol (SNMP), and other proprietary configuration mechanisms. The management software can use NETCONF to write configuration data to and retrieve data from a device. All data is encoded in Extensible Markup Language (XML) and transmitted using Remote Procedure Calls (RPCs) over secure and connection-oriented protocols such as SSL or Transport Layer Security (TLS).

The NETCONF protocol adopts the Client/Server structure:

- NETCONF Manager: Acts as the client in the network, runs in the network, and interacts with the NETCONF Agent to manage devices. The network administrator uses the NETCONF Manager to send RPC requests to the NETCONF Agent. The requests are in XML format.
- NETCONF Agent: Acts as the server in the network. To configure a device, the NETCONF Manager sends configuration management requests to the NETCONF Agent. The NETCONF Agent parses the requests and manages the configuration with the help of the configuration management (CM) component of the NEM. The NETCONF Agent also uses the XML format to send responses to the NETCONF Manager.
-

NETCONF Features Supported by Switch

- Supports the NETCONF Agent function at the server side, which is mainly used for interconnection with data center controllers.
- Supports the SSH-based NETCONF transmission service.
- Supports managing the OpenFlow Controllers.
- Supports managing L2 VXLAN functions.
- Supports configuring EVPN-related function modules and capturing status.

14.3.2 Configuring NETCONF

Purpose

This section describes how to configure NETCONF.

Procedure

Perform the corresponding steps according to different purposes, as shown below.

Purpose	Procedure
Enable or disable the NETCONF protocol	1. Run the **configure** command to access the global configuration view. 2. Run the **netconf** { **enable** | **disable** } command.

14.3.3 Configuration Example

Network Requirements

If you want to manage network devices through in a unified manner, you can use NETCONF to ensure communication between devices.

Switch is used as the server device of NETCONF agent, and as an SSH server. It receives the connection requests of NETCONF Manager as an SSH client. You can manage configuration files through NETCONF by deploying NETCONF Manager.

Network Diagram

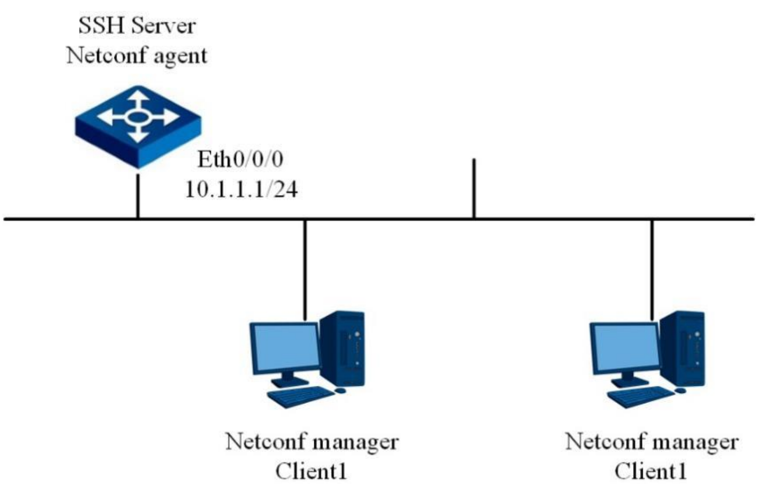


Figure 14-8 NETCONF network diagram

Preparation

You have deployed NETCONF Manager.

Configuration

1. Configure an IP address for Switch management network interface.

Switch(config)#interface ethernet 0/0/0

Switch(config-eth0/0/0)#ip address 10.1.1.1/24

Switch(config-eth0/0/0)#quit

Switch(config)#

2. Configure SSH.

Switch(config)#sshd

Switch(config)#ssh 10.1.1.12 user client1

Switch(config)#ssh login local

3. Enable NETCONF.

Switch(config)#netconf enable

Chapter 15 Virtualization Configuration

This chapter describes the basics, configuration process, and configuration examples of virtualization configuration for switches.

15.1 Stack Command Configuration

15.1.1 Overview of Stack Commands

Main features of the ISS protocol

- Powerful network scalability. A stack system can be easily extended by adding member devices to improve its processing capability and increase ports and bandwidth.
- Safe investment. The robust extension capability protects users' investment by adding of new devices rather than replacement of old ones during network upgrade.
- Low cost. The ISS technique can virtualize low-end devices into a high-end device that delivers the same class of port density and bandwidth at low costs.
- Simplified management: After a stack system is built, users can log into the ISS system over any port of any member switch to manage any switch on the ISS, instead of physically connecting to each member device for configuration and management.
- Easy network operation: The various control protocols enabled on an ISS-based virtual device run as a single device collectively. For example, a set of routing protocols are treated as one device for calculation. This reduces the exchange of many protocol packets between devices, simplifies network operation, and shortens the convergence time in the case of flapping.
- High reliability: The ISS system consists of multiple member devices that provide 1:N backup. Slave devices work as backup but also process services. Once the master device fails, the system automatically elects a new master to keep services running.

ISS protocol operating mode

Stacked devices can operate in two modes: standalone and stack modes. Such modes can be switched conditionally, which may cause a reboot of the device.

Standalone mode allows you to pre-configure stack parameters that take effect after the device is switched to the stack mode.

Before switching from standalone mode to stack mode, you need to configure the stack member number.

Switching from stack mode to standalone mode clears all service configurations and stack-related configurations, while switching from standalone mode to stack mode automatically saves the stack configurations.

A device in standalone mode runs in the same way as an ordinary device. It can only be stacked in stack mode with other devices which are also in stack mode.

Role

Each device in a stack is a member device and takes on either role as below.

- Master: manages the entire stack.
- Slave: runs as a backup device for the master. When the master fails, the system will automatically elect a new one from the slaves to take over the original work.

Both master and slaves in a stack are elected by role. Only one master exists in a stack system, and all other member devices are slaves.

Each member site (switch) will inform the platform of its role to execute the corresponding configuration file after role election is completed.

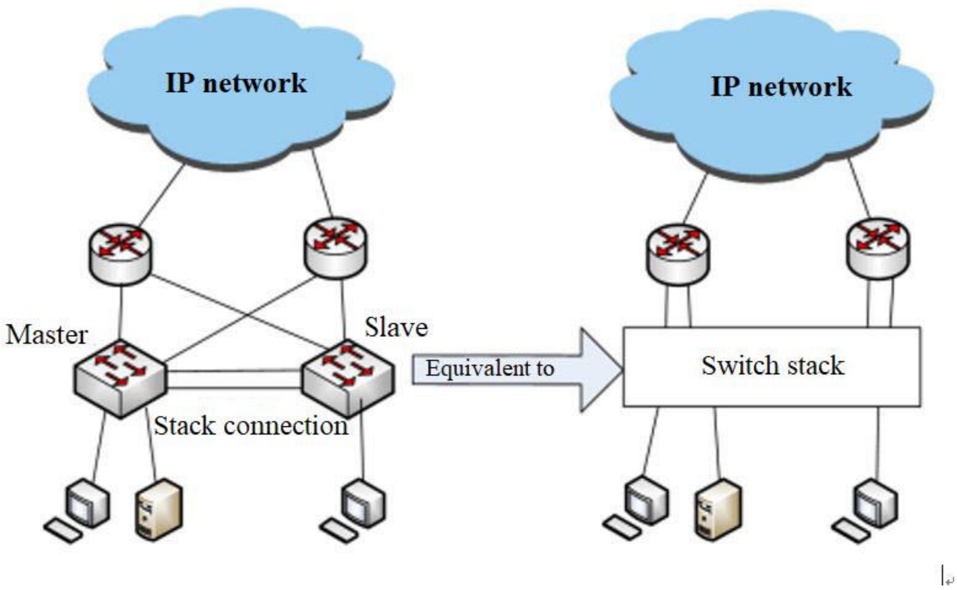


Figure 15-1 Switch Stack Diagram

Stack Port

The member switches in a stack are connected through stack ports, which can be dedicated stack ports or ordinary service ports that are added to the ISS aggregation port (the latter applies to the current ISS version).

At least one stack port or two at most are required for stacked devices to be topologically connected. The figure below shows a stack system with two members.

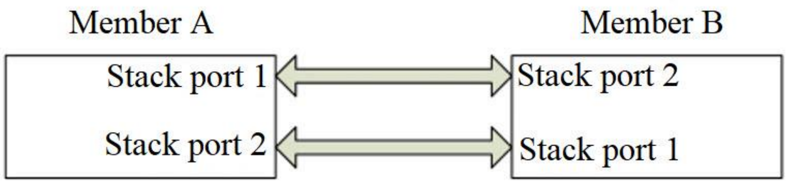


Figure 15-2 Stack System

Stack Domain

Stack domain ID is a mandatory attribute when you enable stack for a device (stack member). Only members with the same stack domain ID can form a stack.

Member number

The member number is an attribute of a stack member, which is unique in a stack. This member number must be configured before switching from standalone mode to stack mode.

The index of the interface in standalone mode is in a two-degree form such as 1/0/1. After the device is switched to stack mode, the original interface index is increased by one degree, from 1/0/1 to x/1/0/1, where x is the site member number.

In addition, if you modify the member number of a device in stack mode, the setting takes effect after you save the configuration and reboot the device.

Member priority

Member priority is an attribute of a member device which determines the chance that it will be elected master. A higher priority value of a stack member increases its likelihood to be elected stack master.

Specify Master

Specify Master is a configuration attribute of a member device that specifies that a device is preferred to be elected stack master.

Operating States of a Stack Site

The member sites operate in four states: Init, Collection, Election, Loading and Done.

Init: default status of a device

Collection: topology collection

Election: being elected

Loading: configuration file being synchronized

Done: site operating in stable state

Stack System State

The state of a stack system can be **Up** or **Down**. A stack system is **Up** only when all member sites in the system are in the **Done** state. You can configure other services (excluding stacking) only after the stack system is **Up.**

15.1.2 How a Switch Stack Works

How to create a switch stack

1. Physical connections

Stack members are connected to each other through stack ports. Each switch has two default stack connections: Stack Connection 1 and Stack Connection 2. If the switch uses dedicated stack ports (e.g., Higig ports), the stack connection is set when the system initially detects the stack ports. If the switch uses ordinary service ports as the stack ports, these service ports need to be added to the stacking aggregation ports. After connections are complete, the stacking module internally records Stack Connection 1 or Stack Connection 2.

2. Connection topology

Chain connection is the basic topology of a switch stack, as shown below.

Figure 15-3 Chain Connection Diagram

3. Establishment of stack port protocol state

After being connected through stack ports, the stacked switches will exchange keepalive message. The protocol state of both stack ports is up only after they both receive the keepalive messages from the other at the same time. Then the hello messages can be sent to carry out topology collection.

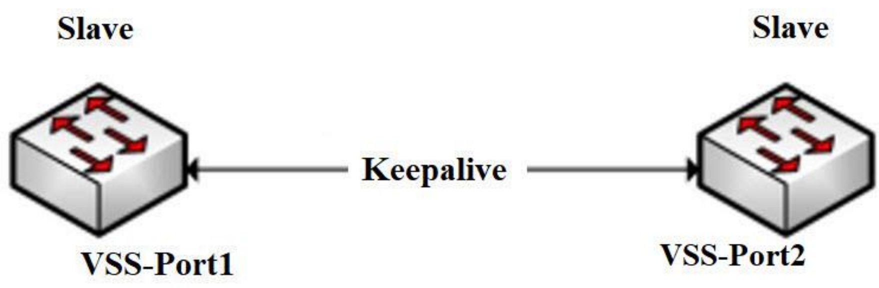


Figure 15-4 Establishment of stack port protocol state

4. Topology collection

Each stack member periodically sends hello messages to all stack members (including itself) through stack ports and locally records the received topology information according to the received hello message. The hello message each switch sent only carries its own information (domain ID, member number, whether to specify as master, priority, runtime, and MAC address, etc.). The hop count is set to 1 when initially sending the hello message, and increased by 1 each time the hello message passes through a member. A member receives the hello message and ascertains whether the source is itself or not, and terminates if so. If the source is not itself, the member receives and updates its topology membership table, and then forwards the hello message from another stack port and increases the hop count in the message. After a period of topology collection, each member can get information about the whole topology.

During topology collection, a member number conflict may occur between different sites. The member number will be selected as per certain rules. The stack port not selected will be shut down and automatically detached from the stack system.

Member sites that are automatically detached can only be added to the stack again after a manual intervention to change the member number and reboot.

Rules for solving member number conflicts are in the order listed:

- The current master outperforms non-master members.
- A specified master member takes precedence.
- The switch with higher member priority takes precedence.
- The switch with longer system uptime takes precedence.
- The switch with a smaller MAC address takes precedence.

5. Role election

Switches will be elected as master or slave after topology collection. A switch stack can have only one master and multiple slaves.

The rules for role elections are in the order listed:

- The current master outperforms non-master members.
- A specified master member takes precedence.
- The switch with higher member priority takes precedence.
- The switch with longer system uptime takes precedence.
- The switch with a smaller MAC address takes precedence.

6. Configuration Synchronization

After role election is completed, two roles exist for member devices: master and slave. A stack master exports or merges configuration files for stack slaves and then enters the Done state (running stably) while executing the local configuration files.

After getting the configuration file from the master, each stack slave needs to compare it with its own local configuration file and updates the local file if it is only a subset. The site is in the Loading state until configuration synchronization is finished. After synchronization is done, the site enters the Done state and executes the updated configuration file.

7. Stack system in stable operation state

Each slave site enters the Done state in turn after the configuration file is synchronized. When all the sites in the stack system have entered the Done state, the whole stack system enters the Up state (stable operation).

Note that service configurations other than stack creation are not allowed until the stack system is formed.

Maintenance of a stack system

To maintain a stack system, you may update the stack topology and take appropriate measures when the stack topology changes.

Such changes include

- Online removal of a master member
- Online removal of a slave member
- Splitting of a stack
- Merging of stacks

Online removal of a master member

As shown in the figure below, after master member 1 is removed from a stack, the system re-elects a master named master member 2 and now comprises only one member.

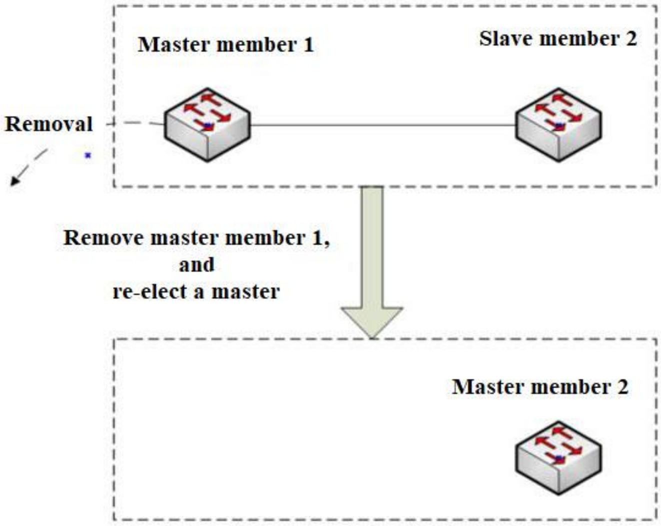


Figure 15-5 Online removal of a master member

Online removal of a slave member

As shown in the figure below, after slave member 2 is removed from a stack, the role of master member 1 is unchanged. The stack system now comprises only one member.

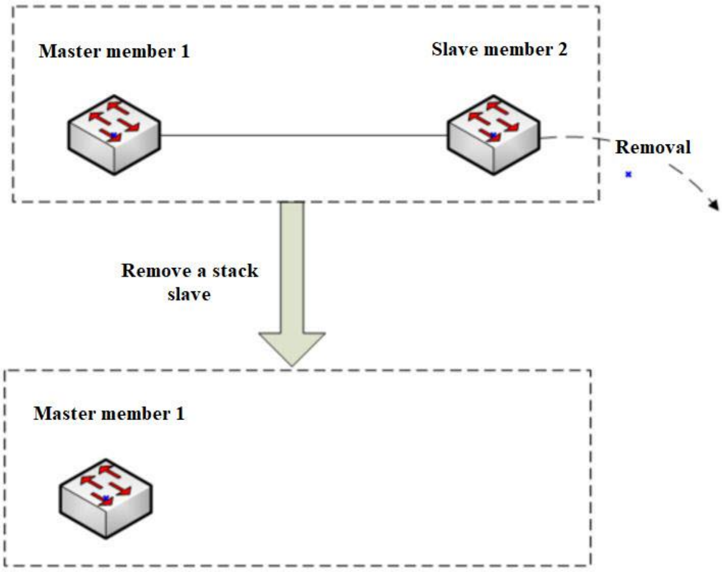


Figure 15-6 Online removal of a slave member

Splitting of a stack

A switch stack is split into two separate stacks when two switch members are disconnected. Each stack comprises only one member.

As shown in the figure below, after stack splitting, stack system 1 still operates properly since its master (i.e., master member 1) does not change. Nevertheless, stack system 2 elects slave member 2 as its master. These two stack systems run independently.

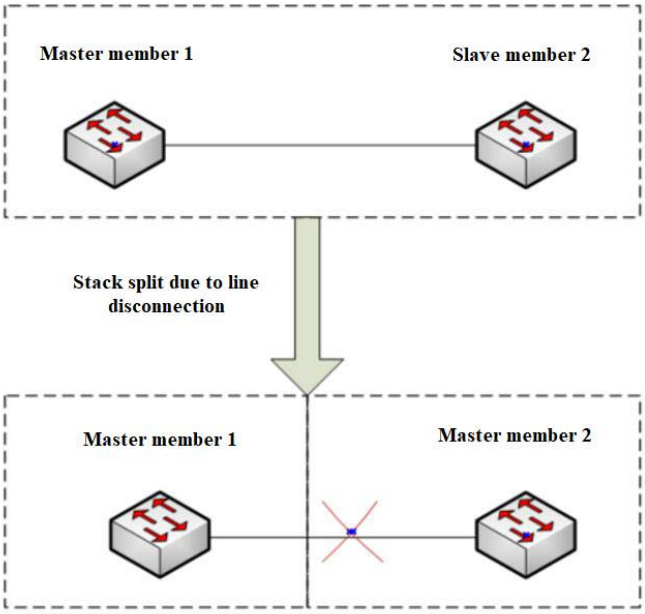


Figure 15-7 Splitting of a Stack

Note that two independent stacks using the same system configuration (MAC/IP) may lead to anomalies in the switch system. To address that issue, the ISS stack provides a MAC/IP delay modification function:

When a stack system is split, if the running MAC address of the stack system is not the original MAC address of any member site, the master will start the**Modify Running MAC timer** (delay is 30 minutes by default). During that delay, if the device of the running MAC address returns to the stack, the timer will be turned off and the MAC address will not be modified. If delay of the timer is reached, the running MAC address of the stack system is modified to the original MAC address of the master.

Merging of stacks

Two independent stack systems can be merged into a new one. The merging process involves topology collection, role election, master-slave configuration synchronization, etc. The figure below shows how stack systems 1 (master member 1) and 2 (master member 2) are merged into a new stack.

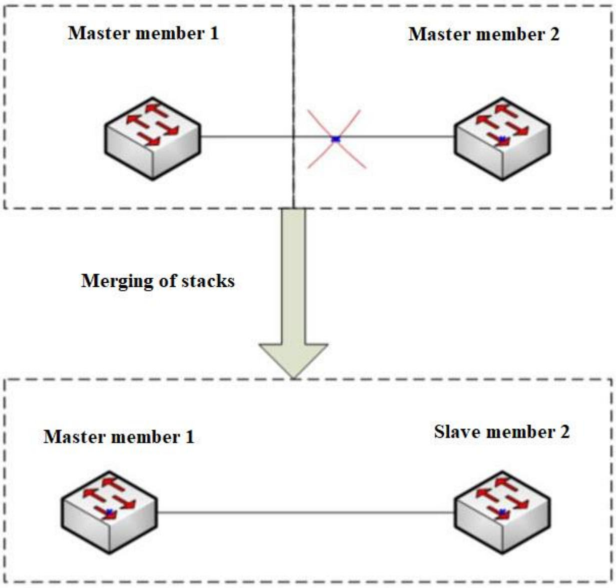


Figure 15-8 Merging of Stacks

15.1.3 Configuring the Link Topology

Purpose

Configure the link topology.

Procedure

Connect port 1 of Site 1 to port 1 of Site 2.

Perform appropriate steps for your purposes by referring to the table below, and refer to the *Switch Command Line Manual* for parameter descriptions.

Site	Purpose	Procedure
Site 1	Setting the member ID	1. Enter the global configuration view. 2. Run the following commands: ● Switch#conf ● Switch(config)#iss member 1
	Configuring the election priority	1. Enter the global configuration view. 2. Run the **Switch(config)#iss priority 3** command.
	Enable the stack port (Enable a stack port of Site 1)	1. Enter the global configuration view. 2. Run the following commands: ● Switch(config)interface stack-port 1 ● Switch(config-stack-port-1) add xgigaethernet 1/0/48

Site	Purpose	Procedure
		• Switch(config-stack-port-1) no shutdown • Switch(config-stack-port-1) quit
	Switching to stack mode (reboot required, select "Y")	1. Enter the global configuration view. 2. Run the **Switch (config)#iss mode iss** command.
Site 2	Setting the member ID	1. Enter the global configuration view. 2. Run the following commands: • Switch#conf • Switch(config)#iss member 2
	Configuring the election priority	1. Enter the global configuration view. 2. Run the **Switch(config)#iss priority 2** command.
	Enable the stack port (Enable a stack port of Site 2)	1. Enter the global configuration view. 2. Run the following commands: • Switch(config-stack-port-1) add xgigaethernet 1/0/48 • Switch(config-stack-port-1) no shutdown • Switch(config-stack-port-1) quit
	Switching to stack mode (reboot required, select "Y")	1. Enter the global configuration view. 2. Run the **Switch (config)#iss mode iss** command.

800-watt AC Power Supply

For DCS-7342-Series Switch

DCS-PWR800-AC

User's Manual

1. Overview

Thank you for purchasing PLANET 800-watt AC power supply.

Power Supply Unit	Input Range
DCS-PWR800-AC	90 to 264V AC

Open the box of the Redundant Power Supply unit and carefully unpack it. The box should contain the following item:

- The AC Power Supply unit x 1

If any item is found missing or damaged, please contact your local reseller for replacement.

Note	The DCS-PWR800-AC is for DCS-7342-Series only.

2. Introduction

Before installation, please be sure to read this user's manual carefully to successfully complete the correct installation of the DCS-PWR800-AC Power Supply Unit. This manual shows how to quickly install the power supply unit in the DCS-7342-Series.

The following figure shows the front panel of the DCS-PWR800 power supply.

Figure 2-1: DCS-PWR800-AC Front View

3. Installing Redundant Power Supply Unit

Note	The DCS-PWR800-AC is hot-swappable, so there is no need to power off the switch before removing the redundant power supply unit from the switch.

Follow these steps to install the redundant power supply unit in the switch:

1. Place the switch on a flat surface. Use a screwdriver to unscrew screws on both sides of the blank plate to remove the blank plate. Do not discard the blank plate as it can be used again when removing the power supply unit from the switch.

Figure 3-1: Removing the Blank Plate

2. Install the redundant power supply unit by sliding it into the compartment.

Figure 3-2: Sliding the Power Supply Unit into the Compartment

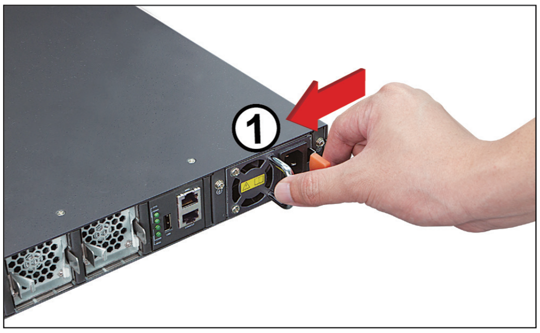
Note	Ensure the DCS-PWR800-AC is fully inserted and securely locked in place.

4. Removing Redundant Power Supply Unit

Follow these steps to remove the redundant power supply unit from the switch:

1. Remove AC power cord from the DCS-PWR800-AC.
2. To remove the redundant power supply unit from the DCS-7342-Series, use the handle to pull it out.

Note	The following images are based on the XGS-6350-48X2Q4C. DCS-7342-Series can be used in the same way.



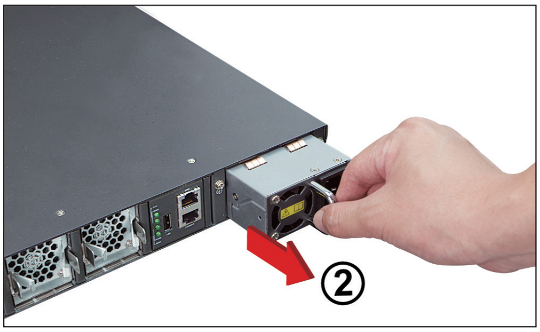


Figure 4-1: Removing the power supply unit