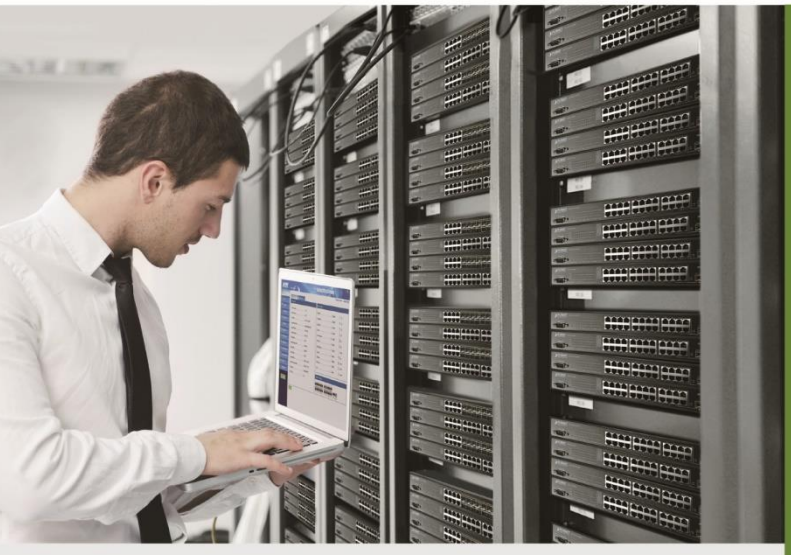
PLANET
Networking & Communication

User's Manual

PLANET Layer 3 Multi-Port 10G/25G + 2-/4-Port 100G QSFP28 Managed Ethernet Switch

- XGS-6350-16X8Y4C
- XGS-6350-24X2C



www.PLANET.com.tw

Trademarks

EU Representative
PLANET Technology Europe B.V.
Address: Posthoornstraat 11, 3011 WD Rotterdam, NL
Email: eu_rep@planet.com.tw
URL: www.planet.com.tw

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 be 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 Multi-port 10G/25G + 2-/4-Port 100G QSFP28 Managed Ethernet Switch

Models:XGS-6350-16X8Y4C, XGS-6350-24X2C
Revision: 1.2
Part No: EM-XGS-6350-16X8Y4C_24X2C Configuration Guide_v1.2

Contents

Chapter 1 INTRODUCTION

Thank you for purchasing PLANET Layer 3 Multi-port 10G/25G +2-/4-Port 100G QSFP28 Managed Switch. The descriptions of these models are shown below:

Model	Description
XGS-6350-16X8Y4C.	Layer 3 16-Port 10G SFP+ + 8-Port 25G SFP28 + 4-Port 100G QSFP28 Managed Ethernet Switch
XGS-6350-24X2C	Layer 3 24-Port 10G SFP+ + 2-Port 100G QSFP28 Managed Ethernet Switch

1.1 Packet Contents

Unless specified, "**Managed Switch**" mentioned in this users manual refers to the XGS-6350-16X8Y4C/XGS-6350-24X2C

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

	XGS-6350-16X8Y4C	XGS-6350-24X2C
QR Code Sheet	■	■
RS232 to RJ45 Console Cable	■	■
Rack Mount Accessory Kit	■	■
AC Power Cord	1	1
Rubber Feet	4	4
SFP Dust Cap	28	26

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

1.2 Product Description

Optimized Data Center and AI Infrastructure Performance

PLANET XGS-6350 Series is a high-performance Layer 3 Managed Switch designed for the next-generation **Metro, Data Center, AI Computing** and **Enterprise network** requirements. It features high-density **40G/100GbE QSFP28, 25G SFP28 and 10G SFP+** fiber interfaces in a compact 1RU chassis, delivering scalable and ultra-high-speed connectivity for AI workloads and cloud applications.

Layer 3 Routing and Multicast Support

The XGS-6350 Series provides comprehensive Layer 3 managed features to streamline service deployment across both traditional L2 networks and fully virtualized data centers. With advanced routing capabilities—including **Static Routing, RIP/OSPF, DHCP Relay, BGP,** and **multicast routing protocols** such as **PIM-DM/SM**—this switch delivers high-performance and scalable network operations for next-generation infrastructures.

Adaptive 10G/25G/40G/100G Transceivers for AI and High-Performance Networks

The administrator can flexibly choose the appropriate transceivers based on the required transmission speed or distance, enabling efficient expansion of **10G/25G/40G/100G** networks for modern **AI, cloud, and high-performance computing workloads**. In addition, with a switching capacity of **1520Gbps,** the XGS-6350 Series can reliably handle massive data flows in secure and scalable topologies, making it ideal for backbone connections or high-capacity servers running **AI inference, real-time analytics, video streaming, and multicast applications**.

Extractive Power Supply Design to Increase Flexibility

The XGS-6350 Series is equipped with one extractive 100~240V AC power supply unit, so it is easy to replace the power for users. Besides, the XGS-6350 Series reserves another backup power slot on the rear panel and users can add the second AC or DC power to the redundant power supply installation. The AC power or DC power is optional. The redundant power system is specifically designed to handle the demands of high-tech facilities requiring the highest power integrity.

High Performance

The XGS-6350 Series boasts a high-performance switch architecture that is capable of providing non-blocking switch capacity as high as **880Gbps to 1520Gbps**, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands.

Rich Multi-layer Networking Protocols

The XGS-6350 Series comes with the complete Layer 3 managed function with comprehensive protocols and applications to facilitate the rapid service deployment and management for both the traditional L2 and L3 networks. With support for advanced features, including **RIP, RIPng, OSPFv2, OSPFv3, BGP, BGP4+**, etc., this switch is ideal for the traditional or fully-virtualized data center.

Strong Multicast

The XGS-6350 Series supports abundant multicast features. In Layer 2, it features IPv4 IGMPv1/v2/v3 snooping and IPv6 MLD v1/v2 snooping. With Multicast VLAN Registration (MVR), multicast receiver/sender control and illegal multicast source detection functions can be had. In Layer 3 multicast protocols, it features **PIM-DM**, **PIM-SM** and **PIM-SSM** which make the XGS-6350 Series great for any robust networking.

Full IPv6 Support

The XGS-6350 Series supports IPv4-to-IPv6 technologies including **IPv4 manual/automatic tunnel**, **IPv6-to-IPv4 tunnel**, and Intra-Site Automatic Tunnel Addressing Protocol (**ISATAP**) tunnel. It comprehensively supports IPv6 Neighbor Discovery, DHCPv6, Path MTU Discovery, IPv6-based Telnet, SSH and ACL, meeting the need of IPv6 network device management and service control.

High Reliability

The key components of the XGS-6350 Series such as management module, power system and the fan system support redundancy design. All system modules support hot-swap and seamless switching without manual intervention.

It supports In-service Software Upgrade (**ISSU**) and Graceful Restart (**GR**) for OSPF/BGP routing protocol, guaranteeing the user data non-stop forwarding when the system is upgrading. It supports Bidirectional Forwarding Detection (**BFD**) that realizes fault detection and service recovery in seconds through linking with Layer 2 or Layer 3 protocol.

Excellent and Secure Traffic Control

The XGS-6350 Series is loaded with powerful traffic management and WRR features to enhance services offered by telecoms and enterprises. The **WRR** functionalities include wire-speed Layer 4 traffic classifiers and bandwidth limitation which are particularly useful for multi-tenant unit, multi-business unit, Telco, or network service applications.

Powerful Security from Layer 2 to Layer 4

The ACL policies supported can classify the traffic by source/destination IP addresses, source/destination MAC addresses, IP protocols, TCP/UDP, IP precedence, time ranges and ToS. Moreover, various policies can be conducted to forward the traffic. The XGS-6350 Series also provides IEEE 802.1x port-based access authentication, which can be deployed with RADIUS, to ensure the port level security and block illegal users. Thus, the XGS-6350 Series empowers enterprises and campuses to take full advantage of the limited network resources and guarantees the best performance in VoIP and video conferencing transmission.

Robust Layer 2 Features

The XGS-6350 Series can be programmed for basic switch management functions such as port speed configuration, port aggregation, VLAN, Spanning Tree Protocol, WRR, bandwidth control and IGMP snooping. It also supports 802.1Q tagged VLAN, Q-in-Q, voice VLAN and GVRP Protocol. In addition, the number of VLAN interfaces is 1K and the number of VLAN IDs is 4K. By supporting port aggregation, the XGS-6350 Series allows the operation of a high-speed trunk combined with multiple ports. It enables up to 32 groups for trunk with a maximum of 8 ports for each group.

Efficient and Secure Management

For efficient management, the XGS-6350 Series Managed 100Gigabit Switch is equipped with console, Web and SNMP management interfaces.

- With its built-in Web-based management interface, the XGS-6350 Series offers an easy-to-use, platform-independent management and configuration facility.
- The XGS-6350 Series supports standard Simple Network Management Protocol (SNMP) and can be managed via any standard-based management software.
- For reducing product learning time, the XGS-6350 Series offers Cisco-like command via Telnet or console port. Moreover, the XGS-6350 Series offers secure remote management by supporting SSH connection which encrypts the packet content at each session.

Moreover, the XGS-6350 Series offers secure remote management by supporting SSHv1/v2 and TLSv1.3 connection which encrypts the packet content at each session.

Centralized Hardware Stacking Management

Up to **10 XGS-6350 Series units** can be stacked to operate as a single logical switch, simplifying network management and expansion. The ring-based stacking design provides redundancy so that data traffic continues even if one unit fails. The switches can also be hot-swapped without service interruption, greatly streamlining upgrades and scaling for increasing bandwidth demands.

Flexibility and Extension Solution

The XGS-6350 Series provides **10Gbps SFP+ and 25G SFP28 and 100Gbps QSFP28** Fiber interfaces. Each of the SFP+ slots supports Dual Speed, 10GBASE-SR/LR or 1000BASE-SX/LX, each of the SFP28 slots supports 25G/10G/1G, and each of the QSFP28 slots supports native **100 Gigabit Ethernet, 40G and 4 x 10 Gigabit Ethernet modes**. Therefore, the administrator can flexibly choose the suitable SFP transceiver according to not only the transmission distance, but also the transmission speed required. The distance can be extended from 550 meters to 2km (multi-mode fiber) or up to 10/20/30/40/50/70/80 km (single-mode fiber or WDM fiber). They are well suited for applications within the enterprise data centers and distributions.

Redundant Ring, Fast Recovery for Critical Network Applications

The XGS-6350 Series supports redundant ring technology and features strong, rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced **ITU-T G.8032 ERPS** (Ethernet Ring Protection Switching) technology and Spanning Tree Protocol (802.1s MSTP) into customer's network to enhance system reliability and uptime in harsh environments. In a certain simple Ring network, the recovery time could be less than 50ms to quickly bring the network back to normal operation.

1.3 Product Features

➢ **Physical Ports**

XGS-6350-24X2C

- 24 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- 2 QSFP28 slots with each having native 100 Gigabit Ethernet, 40G and 4 10 Gigabit Ethernet ports
- RJ45 to DB9 console interface (9600,N,8,1) for switch basic management and setup
- MGMT port for HTTP server access
- USB port

XGS-6350-16X8Y4C

- 16 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- 8 25G SFP28 slots, compatible with 1G/10GBASE-SX/LX/BX SFP
- 4 QSFP28 slots, each supports native 100 Gigabit Ethernet, 40G and 4 x 10 Gigabit Ethernet modes
- RJ45 to DB9 console interface (115200,N,8,1) for switch basic management and setup
- MGMT port for HTTP server access
- USB port

➢ **IPv4 Features**

- Static Routing, RIP v1/v2, OSPFv2 and BGP
- Policy Routing
- BFD for OSPF and BGP

➢ **IPv6 Features**

- ICMPv6, DHCPv6, ACLv6, IPv6 Telnet
- IPv6 Neighbor Discovery
- Path MTU Discovery
- MLD and MLD Snooping
- IPv6 Static Routing, RIPng, OSPFv3 and BGP4+
- Manual Tunnel, ISATAP Tunnel and 6-to-4 Tunnel

➢ **Multicast Routing Features**

- Supports Multicast Routing Protocols:
  - PIM-DM (Protocol Independent Multicast - Dense Mode)
  - PIM-SM (Protocol Independent Multicast - Sparse Mode)
  - PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast Mode)
- Supports IGMP v1/v2/v3

➢ **Layer 2 Features**

- Auto-MDI/MDI-X detection on each RJ45 port
- Prevents packet loss flow control
  - IEEE 802.3x pause frame flow control in full-duplex mode
  - Back-pressure flow control in half-duplex mode
- High performance Store-and-Forward architecture, broadcast storm control, port loopback detects

- Supports VLAN
  - IEEE 802.1Q tag-based VLAN
  - GVRP for dynamic VLAN management
  - Up to 4094 active VLANs
  - Provider Bridging (VLAN Q-in-Q, IEEE 802.1ad) supported
  - Private VLAN Edge (PVE) supported
  - GVRP protocol for Management VLAN
  - Protocol-based VLAN
  - MAC-based VLAN
- Supports Link Aggregation
  - Maximum 32 trunk groups with up to 8 ports per trunk group
  - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
  - Cisco ether-channel (static trunk)
- Supports Spanning Tree Protocol
  - STP, IEEE 802.1D (Classic Spanning Tree Protocol)
  - RSTP, IEEE 802.1w (Rapid Spanning Tree Protocol)
  - MSTP, IEEE 802.1s (Multiple Spanning Tree Protocol, spanning tree by VLAN)
  - BPDU & root guard
- Port mirroring to monitor the incoming or outgoing traffic on a particular port (many to many)
- Provides port mirror (many-to-1)
- Supports G.8032 ERPS (Ethernet Ring Protection Switching)

➢ **Quality of Service**

- 8 priority queues on all switch ports
- Supports strict priority and WRR (Weighted Round Robin) CoS policies
- Traffic classification
  - IEEE 802.1p CoS/ToS
  - IPv4/IPv6 DSCP
  - Port-based WRR
- Strict priority and WRR CoS policies

➢ **Multicast**

- Supports IPv4 IGMP snooping v1, v2 and v3; and IPv6 MLD v1 and v2 snooping
- Querier mode supports
- Supports Multicast VLAN Register (MVR)

➢ **Security**

- Authentication
  - IEEE 802.1x port-based network access authentication
  - Built-in RADIUS client to cooperate with the RADIUS servers
  - RADIUS/TACACS+ users access authentication
  - Change of Authorization (COA)

- Access Control List
  - IP-based Access Control List (ACL)
  - MAC-based Access Control List (ACL)
  - Port-based Access Control List (ACL)
  - Time-based ACL
- DHCP Snooping to filter distrusted DHCP messages
- Dynamic ARP Inspection discards ARP packets with invalid MAC address to IP address binding
- IP Source Guard prevents IP spoofing attacks

➢ **Management**

- IPv4 and IPv6 dual stack management
- Switch Management Interfaces
  - Console and Telnet Command Line Interface
  - HTTP web switch management
  - SNMP v1 and v2c switch management
  - SSHv2, SSLv3, TLSv1.3 and SNMP v3 secure access
- SNMP Management
  - Four RMON groups (history, statistics, alarms, and events)
  - SNMP trap for interface Link Up and Link Down notification
- Built-in Trivial File Transfer Protocol (TFTP) client
- BOOTP and DHCP for IP address assignment
- System Maintenance
  - Firmware upload/download via HTTP
  - Reset button for system reboot or reset to factory default
  - Dual images
- DHCP Functions:
  - DHCP Relay
  - DHCP Option 82
  - DHCP Server
- User Privilege levels control
- Network Time Protocol (NTP)
- Network Diagnostic
  - SFP-DDM (Digital Diagnostic Monitor)
  - ICMP remote IP ping
- Syslog remote alarm
- System Log
- Supports ping, trace route function for IPv4 and IPv6
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS, and CloudNMS for deployment management

➢ **Stacking Management**

- Virtualized multiple XGS-6350 Series switches integrated into one logical device
- Single IP address stack management, supporting up to 10 hardware units stacked together
- Stacking architecture supports redundant Ring mode

1.4 Product Specifications

Product		XGS-6350-24X2C	XGS-6350-16X8Y4C
Hardware Specifications			
QSFP28 Slots		**2**, each supports native 100/40 Gigabit Ethernet and 4 x 10 Gigabit Ethernet modes	**4**, each supports native 100/40 Gigabit Ethernet and 4 x 10 Gigabit Ethernet modes
SFP28 Slots		-	**8** 25G SFP28 interfaces Compatible with 1G/10GBASE-SX/LX/BX SFP+ transceiver
SFP+ Slots		**24** 10GBASE-SR/LR SFP+ interfaces Compatible with 1000BASE-SX/LX/BX SFP transceiver	**16** 10GBASE-SR/LR SFP+ interfaces Compatible with 1000BASE-SX/LX/BX SFP transceiver
MGMT		1 x 10/100/1000BASE-T RJ45 port	1 x 10/100/1000BASE-T RJ45 port
Console		1 x RJ45-to-DB9 serial port (9600, 8, N, 1)	1 x RJ45-to-DB9 serial port (115200, 8, N, 1)
USB		1 x USB 2.0	1 x USB 2.0
LED Indicator		System: PWR, SYS **Green** Ports: 10G SFP+ interfaces: LNK/ACT, **Green** 40G/100G QSFP Port: LNK/ACT **Green**	System: PWR, SYS **Green** Ports: 10G SFP+ interfaces: LNK/ACT, **Green** 25G SFP28 interfaces: LNK/ACT, **Green** 40G/100G QSFP Port: LNK/ACT **Green**
Dimensions (W x D x H)		442.5 x 300.1 x 44.6 mm 1U height	442.5 x 280.25 x 44.6 mm 1U height
Weight		5716g	4333g
Power Consumption	System on	26.5 watts/90.3 BTU (maximum)	54 watts/184.1 BTU (maximum)
	Full loading	65 watts/221.6BTU (maximum)	116.5 watts/397.2BTU (maximum)
Power Requirements		AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Fan		4(Smart FAN)	4(Smart FAN)
Switching Performance			
Switch Architecture		Store-and-forward	Store-and-forward
Switch Capacity		880Gbps/non-blocking	1520Gbps/non-blocking
Switch Throughput		654Mpps	1130Mpps
Address Table		128K MAC address table with auto learning function	112K MAC address table with auto learning function
ARP Table		2K	2K

Routing Table	IPv4: 16K IPv6: 8K	IPv4: 16K IPv6: 8K
VLAN Interface	1K	1K
IP Interface	1021	4096
ACL Table	IPv4 ifp:1791 efp:767 IPv6 ifp: 894 efp: 383	IPv4 ifp:4862 efp:1023 IPv6 ifp: 2301 efp: 511
Routing entries	16K	32K
Shared Data Buffer	4.5MB	8MB
Jumbo Frame	9KB	12KB
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex	Back pressure for half duplex IEEE 802.3x pause frame for full duplex
IPv4 Layer 3 Functions		
IP Routing Protocol	RIP v1/v2 OSPFv2 BGP (Border Gateway Protocol) Static routing	
Multicast Routing Protocol	PIM-DM and PIM-SM PIM-SSM	
VRRP	Configure VRRP in interface VLAN VRRP priority VRRP standby VRRP track	
Routing Features	VRRP Policy routing Load balance through equal-cost routing BFD (Bidirectional Forwarding Detection) for OSPF and BGP	
DHCP	DHCP client DHCP server, default route DHCP relay	
IPv6 Layer 3 Functions		
IP Routing Protocol	RIPng OSPFv3 BGP4+	
Routing Features	Manual tunnel ISATAP tunnel 6-to-4 tunnel	
IPv6 Functions	ICMPv6, DHCPv6, ACLv6, IPv6 Telnet	

	IPv6 Neighbor Discovery Path MTU Discovery
Layer 2 Function	
Port Configuration	Port disable/enable Flow control disable/enable Bandwidth control on each port Port loopbacks detect
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
VLAN	IEEE 802.1Q tag-based VLAN, up to 4K VLAN entries IEEE 802.1ad Q-in-Q VLAN stacking/tunneling GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN IP subnet VLAN
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) BPDU protection, root protection
IPv4 IGMP Snooping	IPv4 IGMP v1/v2/v3 snooping IGMP Fast Leave IPv4 Querier mode support IGMP Filtering and IGMP Throttling IGMP Proxy reporting
IPv6 MLD Snooping	IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR)
Bandwidth Control	Ingress and Egress At least 64Kbps stream
Ring	Supports ITU-T G.8032 ERPS
Link Aggregation	IEEE 802.3ad LACP/static trunk Supports 32 groups with 8 ports per trunk group
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 - Port ACL Policy-based ingress and egress QoS 802.1p and DSCP priority remark
Authentication	IEEE 802.1x port-based network access control AAA authentication: TACACS+ and IPv4/IPv6 over RADIUS
Security Function	
Access Control List	Supports Standard and Expanded ACL IP-based ACL/MAC-based ACL/Port-based ACL Time-based ACL Up to 1K entries
Security	Port isolation Port security, supports IP + MAC + port binding Identification and filtering of L2/L3/L4 based ACL Defend against DOS or TCP attacks Suppression of broadcast, multicast and unknown unicast packet DHCP Snooping, DHCP Option 82 Command line authority control based on user levels
AAA	TACACS+ and IPv4/IPv6 over RADIUS
Network Access Control	IEEE 802.1x port-based network access control
Management Function	
System Configuration	Console and Telnet Web browser SNMP v1, v2c
Secure Management Interfaces	SSHv2, SSLv3 TLS v1.3 and SNMPv3 Maximum 8 sessions for SSH and Telnet connection
System Management	Supports both IPv4 and IPv6 Protocols Supports the user IP security inspection for IPv4/IPv6 SNMP Supports MIB and TRAP Supports TFTP, FTP Supports IPv4/IPv6 NTP Supports RMON 1, 2, 3, 9 groups

	Supports the RADIUS authentication for IPv4/IPv6 Telnet user name and password Supports Change of Authorization (COA) The right configuration for users to adopt RADIUS server's shell management Supports CLI, console, Telnet Supports Security IP safety net management function: avoid unlawful landing at non-restrictive area Supports TACACS+ Supports SPAN, RSPAN PLANET Smart Discovery Utility PLANET NMS, and CloudNMS
Stacking Management	10 members max. 2 software-defined ports function as Stacking Up and Down interfaces Note: The model and firmware version of each switch must be identical.
Event Management	Supports syslog server for IPv4 and IPv6
SNMP MIBs	RFC 1066 TCP/IP-based MIB RFC 1213 MIB-II RFC 1215 Internet Engineering Task Force RFC1757 RMON group 1,2,3,9 RFC 1354 IP-Forwarding MIB RFC 1493 Bridge MIB RFC 1643 Ether-like MIB RFC 1907 SNMPv2 RFC 2011 IP/ICMP MIB RFC 2012 TCP MIB RFC 2013 UDP MIB RFC 2096 IP forward MIB RFC 2233 if MIB RFC 2452 TCP6 MIB RFC 2454 UDP6 MIB RFC 2465 IPv6 MIB RFC 2466 ICMP6 MIB RFC 2573 SNMPv3 notification RFC 2574 SNMPv3 VACM RFC 2674 Bridge MIB Extensions
Standard Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3z Gigabit 1000BASE-SX/LX IEEE 802.3ae 10Gb/s Ethernet

	IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1X port authentication network control IEEE 802.1ab LLDP RFC 768 UDP RFC 783 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2 RFC 3376 IGMP v3 RFC 2710 MLD v1 FRC 3810 MLD v2 RFC 2328 OSPF v2 RFC 1058 RIP v1 RFC 2453 RIP v2 RFC 5176 COA
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 10 ~ 85% (non-condensing)
Storage	Temperature: -40 ~ 80 degrees C Relative Humidity: 5 ~ 95% (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. Below Figures are show the front panel of the Managed Switches.

XGS-6350-16X8Y4C Front Panel

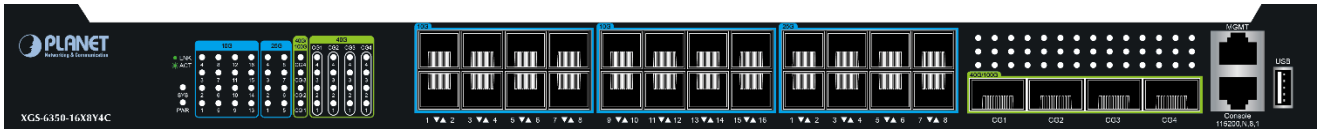


Figure XGS-6350-16X8Y4C front panel

XGS-6350-24X2C Front Panel

Figure XGS-6350-24X2C front panel

■ **SFP/SFP+ slots**

SFP/SFP+ 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).

■ **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.

■ **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 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.

XGS-6350-16X8Y4C

Figure: XGS-6350-16X8Y4C front panel

SystemLED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Blinks to indicate the system is normally starting up.

10G SFP+ Interfaces

LED	Color	Function
LNK/ACT	Green	Blinks to indicate the data are transmitted and received through the port; lights to indicate the link on the port are normal.

25G SFP28 Interfaces

LED	Color	Function
LNK/ACT	Green	Blinks to indicate the data are transmitted and receiving through the port; lights to indicate the link on the port are normal.

40G Status LED (Divided into 4 10G)

LED	Color	Function
LNK/ACT	Green	Blinks to indicate the data is transmitted and receiving through the QSFP+ 40G to 4 10GE ports; lights to indicate the link on the port is normal.

40G/100G Status LED

LED	Color	Function
40G/100G LNK/ACT	Green	Blinks to indicate the data are transmitted and receiving through the port; lights to indicate the link on the port are normal.

XGS-6350-24X2C

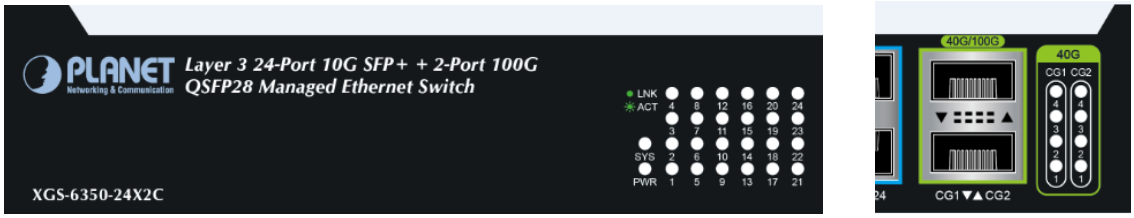


Figure: XGS-6350-24X2C front panel

System

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
	Off	Power is off.
SYS	Green	Blinks to indicate the system is normally starting up.

Interfaces (TG1~TG24)

LED	Color	Function
LNK/ACT	Green	Blinks to indicate the data is transmitting and receiving through the port; lights to indicate the link on the port is normal.

40G Status LED (Divided into 4 10G) (CG1~CG2)

LED	Color	Function
LNK/ACT	Green	Blinks to indicate the data is transmitting and receiving through the QSFP+ 40G to 4 10GE ports; lights to indicate the link on the port is normal.

40G/100G Status LED(CG1~CG2)

LED	Color	Function
40G/100G LNK/ACT	Green	Blinks to indicate the data is transmitting and receiving through the port; lights to indicate the link on the port is normal.

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.

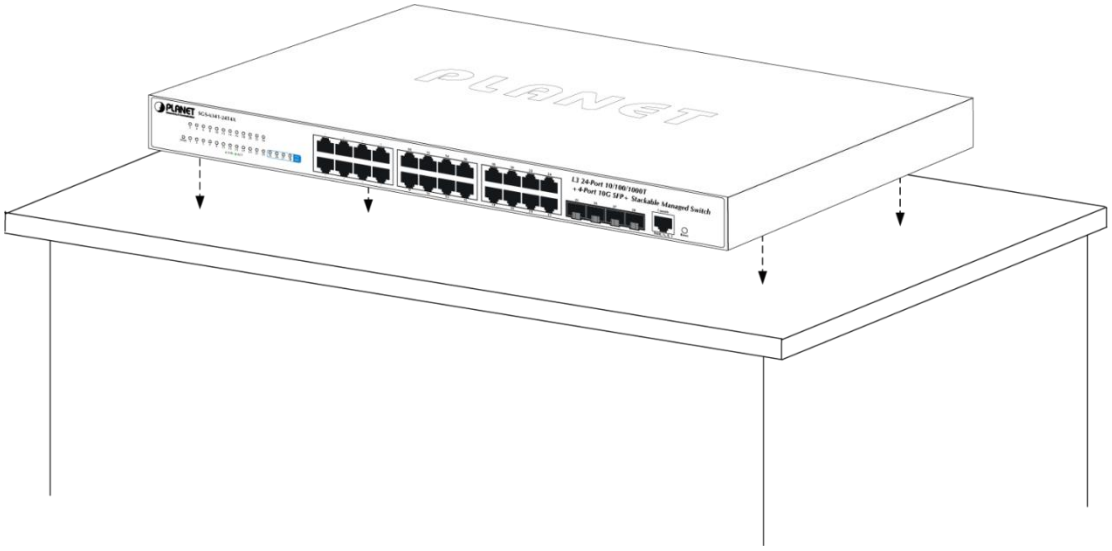


Figure 2-2-1 Place the Managed Switch on the desktop

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 MGMT RJ45 port on the front of the managed switch and the other end of the cable to a network device such as a printer server, workstation, or router.

Note

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 2-2-2-1 shows how to attach brackets to one side of the Managed Switch.

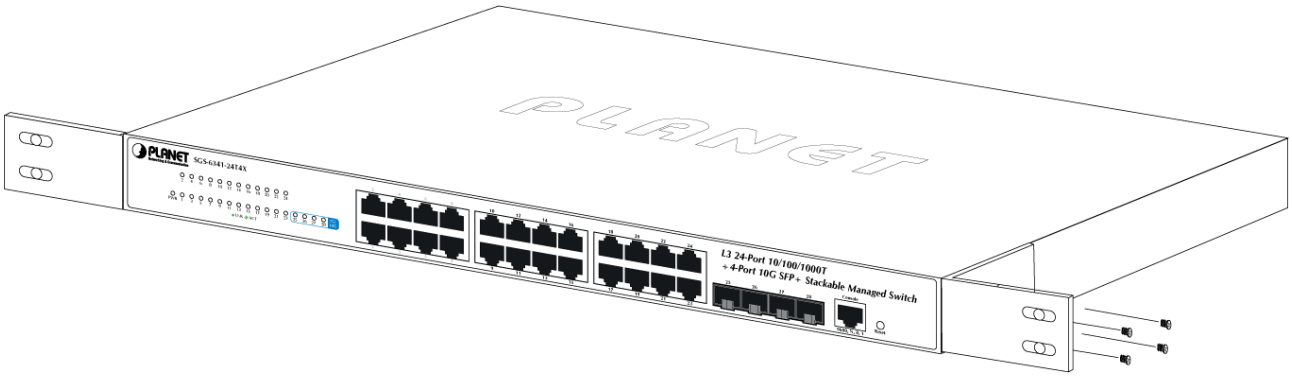


Figure 2-2-2 Attach brackets to the Managed Switch.

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 2-2-2-2.

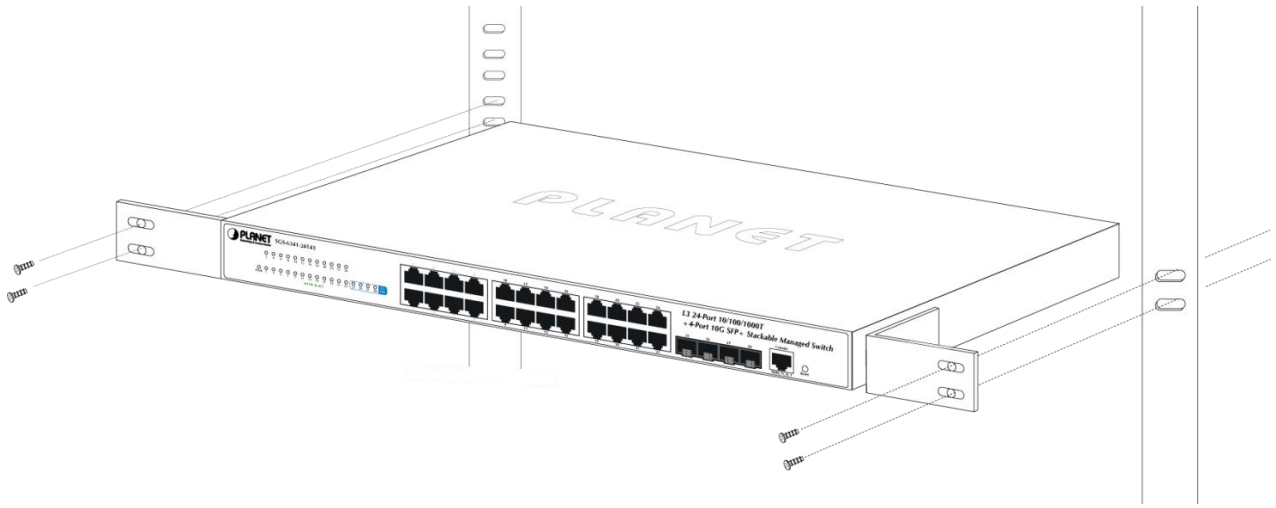


Figure 2-2-2-2 Mounting SGS-6350 Series in a Rack

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.

2.2.3 Installing the SFP+/SFP28/QSFP+/QSFP28 Transceiver

The sections describe how to insert an SFP+/SFP28/QSFP+/QSFP28 transceiver into an SFP+/SFP28/QSFP+/QSFP28 slot. The SFP+/SFP28/QSFP+/QSFP28 transceivers are hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP+/SFP28/QSFP+/QSFP28 port without having to power down the Managed Switch, as the Figure 2-16 shows.

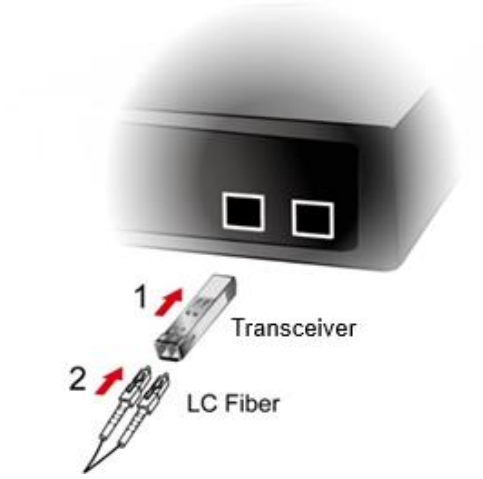


Figure 2-2.3 Plug in the transceiver

➢ **Approved PLANET SFP+/SFP28/QSFP+/QSFP28 Transceivers**

PLANET Managed Switch supports both single mode and multi-mode SFP+/SFP28/QSFP+/QSFP28 transceivers. The following list of approved PLANET SFP+/SFP28/QSFP+/QSFP28 transceivers is correct at the time of publication:

100G Ethernet Transceiver

QSFP-100G-SR4	100GBASE-SR4 QSFP28 Fiber Transceiver (Multimode, MPO, 850nm, DDM) – 100m
QSFP-100G-LR4	100GBASE-LR4 QSFP28 Fiber Transceiver (Single mode, LC, 1310nm, DDM) – 10km

40G Ethernet Transceiver

QSFP-40G-SR4	40GBASE-SR4 QSFP+ Fiber Transceiver (Multimode, MPO, 850nm, DDM) – 100m
QSFP-40G-LR4	40GBASE-LR4 QSFP+ Fiber Transceiver (Single mode, LC, 1310nm, DDM) – 10km

25Gbps QSFP+ (25G Ethernet/25GBASE-SR/LR) for XGS-6350-16X8Y4C

SFP28-25G-SR	25GBASE-SR SFP28 Fiber Transceiver (Multi-mode, 850nm, DDM, 0~70°C) - 100m
SFP28-25G-LR	25GBASE-LR SFP28 Fiber Transceiver (Single mode, 1310nm, DDM, 0~70°C) - 10km
SFP28-25G-LA10	25GBASE-BX SFP28 Fiber Transceiver (Single mode, WDM: TX 1270nm RX 1330nm, DDM, 0~70°C) - 10km
SFP28-25G-LB10	25GBASE-BX SFP28 Fiber Transceiver (Single mode, WDM: TX 1330nm RX 1270nm, DDM, 0~70°C) - 10km

10Gigabit Ethernet Transceiver

MTB-LA10	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 10km (TX:1270nm RX:1330nm)
MTB-LB10	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 10km (TX:1330nm RX:1270nm)
MTB-LA20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1270nm RX:1330nm)
MTB-LB20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1330nm RX:1270nm)
MTB-LA40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1270nm RX:1330nm)
MTB-LB40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1330nm RX:1270nm)
MTB-LA60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1270nm RX:1330nm)
MTB-LB60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1330nm RX:1270nm)
MTB-RJ	1-Port 10GBASE-T SFP+ Copper Fiber Optic Module - 30m
MTB-SR	1-Port 10GBASE-SR SFP+ Fiber Optic Module - 300m
MTB-SR2	1-Port 10GBASE-LR SFP+ Fiber Optic Module – 2km
MTB-LR	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 10km
MTB-LR20	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 20km
MTB-LR40	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 40km
MTB-LR60	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 60km
MTB-LR80	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 80km

Gigabit Ethernet Transceiver (1000BASE-X SFP)

MGB-GT	SFP-Port 1000BASE-T Module
MGB-LX	SFP-Port 1000BASE-LX mini-GBIC module - 20km
MGB-SX	SFP-Port 1000BASE-SX mini-GBIC module - 550m
MGB-SX2	SFP-Port 1000BASE-SX mini-GBIC module - 2km
MGB-L40	SFP-Port 1000BASE-LX mini-GBIC module - 40km
MGB-L80	SFP-Port 1000BASE-LX mini-GBIC module - 80km
MGB-L120	SFP-Port 1000BASE-LX mini-GBIC module - 120km
MGB-LA10	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 10km
MGB-LB10	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 10km
MGB-LA20	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 20km
MGB-LB20	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 20km
MGB-LA40	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 40km
MGB-LB40	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 40km
MGB-LA80	SFP-Port 1000BASE-BX (WDM, TX:1490nm) mini-GBIC module - 80km
MGB-LB80	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 80km

Note

It is recommended to use PLANET SFP+/SFP28/QSFP+/QSFP28 on the Managed Switch. If you insert an transceiver that is not supported, the Managed Switch will not recognize it.

1. Before we connect the XGS-6350 Series to the other network device, we have to make sure both sides of the transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000Bas-LX to 1000BASE-LX.

2. Check whether the fiber-optic cable type matches with the transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ **Connect the Fiber Cable**

1. Insert the duplex LC connector into the transceiver.
2. Connect the other end of the cable to a device with transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to "**100G Force**", "**40G Force**", "**25G Force**", "**10G Force**", "**1000M Force**".

■ **Remove the Transceiver Module**

1. Make sure there is no network activity anymore.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the transceiver module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

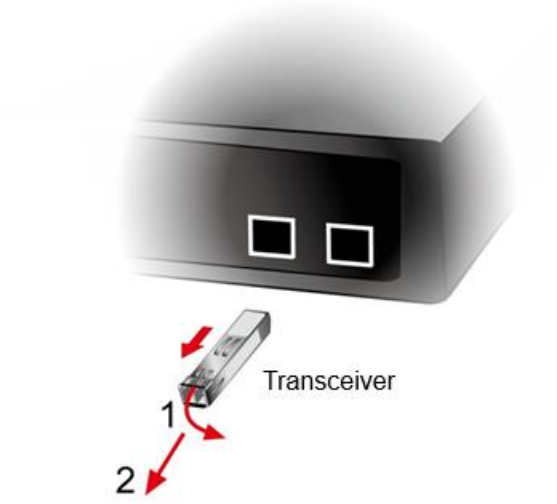


Figure 2-2.3: How to Pull Out the Transceiver

Note

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP+/SFP28/QSFP+/QSFP28 module slot of the Managed Switch.

2.2.4 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 Switch Management

3.1 Management Options

To set up the Managed Switch, the user needs to configure the Managed Switch for network management. The Managed Switch provides two management options: Out-of-Band Management and In-Band Management.

3.2 Out-Of-Band Management

Out-of-band management is the management through console interface. Generally, the user will use out-of-band management for the initial switch configuration, or when in-band management is not available.

3.3 In-band Management

In-band management refers to the management by logging in to the Managed Switch using Telnet or HTTPs, or using SNMP management software to configure the Managed Switch. In-band management enables the management of the Managed Switch to attach some devices to the Switch. The following procedures are required to enable in-band management:

1. Log on to console
2. Assign/Configure IP address
3. Create a remote login account
4. Enable HTTPs or Telnet server on the Managed Switch

In case in-band management fails due to Managed Switch configuration changes, out-of-band management can be used for configuring and managing the Managed Switch.

Important!

The XGS-6350-24X2C, XGS-6350-16X8Y4C. Managed Switches are shipped with Management **Port** IP address 1**92.168.1.1/24** assigned and **VLAN1 interface** IP address **192.168.0.254/24** assigned by default. User can assign another IP address to the Managed Switch via the console interface to be able to remotely access the Managed Switch through Telnet or HTTPs.

3.4 Requirements

Workstations running Windows 10/11, MAC OS 10.16 or later, Linux, UNIX, or other platforms that are compatible with TCP/IP Protocols

Workstations are installed with Ethernet NIC (Network Interface Card)

Serial Port Connection (Terminal)

- The above Workstations come with COM Port (DB9) or USB-to-RS232 converter.
- The above Workstations have been installed with terminal emulator, such as Tera Term or PuTTY.
- Serial cable -- One end is attached to the RS232 serial port, while the other end to the console port of the Managed Switch.

Management Port Connection

- Network cables -- Use standard network (UTP) cables with RJ45 connectors.
- The above PC is installed with Web browser

It is recommended to use Google Chrome or above to access the Managed Switch. If the Web interface of the Managed Switch is not accessible, please turn off the anti-virus software or firewall and then try it again.

3.5 Terminal Setup

To configure the system, connect a serial cable to a **COM port** on a PC or notebook computer and to serial (console) port of the Managed Switch. The console port of the Managed Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

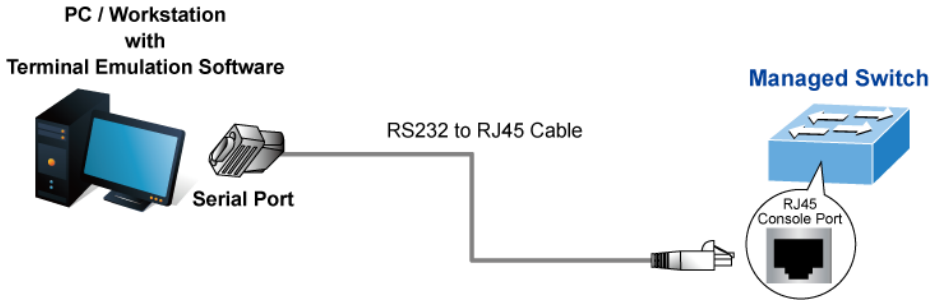


Figure 3-5-1 Managed Switch Console Connectivity

A terminal program is required to make the software connection to the Managed Switch. Tera Term program may be a good choice. The Tera Term can be accessed from the **Start** menu.

➢Click START menu, then Programs, and then Tera Term.

➢When the following screen appears, make sure that the COM port should be configured as:

- **Baud: 9600 (For XGS-6350-24X2C)**
- **Baud: 115200 (For XGS-6350-16X8Y4C)**
- **Parity: None**
- **Data bits: 8**
- **Stop bits: 1**
- **Flow control: None**

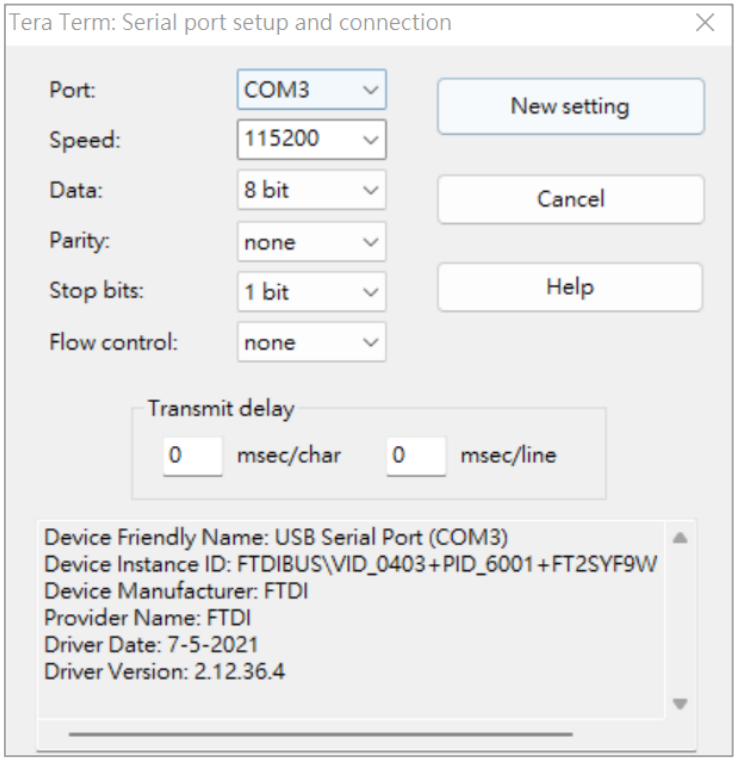


Figure 3-5-2 Tera Term COM Port Configuration

3.6 Logging on to the Console

Once the terminal is connected to the device, power on the Managed Switch, and the terminal will display "running testing procedures".

Then, the following message asks for the login user name and password. The factory default user name and password are as follows as the login screen.

Username: **admin**
Password: **sw + the last 6 characters of the MAC ID in lowercase**

Find the MAC ID on your device label. The default password is "sw" or "mc" followed by the last six lowercase characters of the MAC ID.

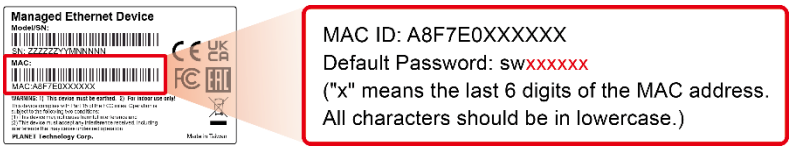


Figure 3-6-1: Industrial Managed Switch MAC ID Label

Enter the default username and password, then set a new password according to the rule-based prompt and confirm it.

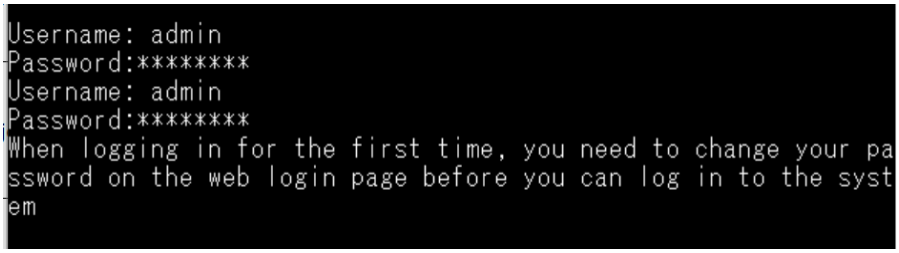


Figure 3-6-2 Managed Switch Console Login Screen

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

Note

1. For security reason, please change and memorize the new password after this first setup.
2. Accept command in lowercase or uppercase letter under console interface.

3.7 Configuring IP Address

The IP address configuration commands for **VLAN1 interface** are listed below. Before using in-band management, the Managed Switch must be configured with an IP address by out-of-band management (i.e. console mode). The configuration commands are as follows:

```
Switch# config
Switch_config# interface vlan1
Switch_config_v1)# ip address 192.168.1.254 255.255.255.0
```

The previous command would apply the following settings for the Managed Switch.

IPv4 Address: 192.168.1.254
Subnet Mask: 255.255.255.0

```
Switch#config
Switch_config#interface vlan1
Switch_config_v1#ip address 192.168.1.254 255.255.255.0
Switch_config_v1#
Switch_config_v1#
Switch_config_v1#
```

Figure 3-7-1 Configuring IPv4 Address Screen

To check the current IP address or modify a new IP address for the Managed Switch, please use the procedures as follows:

- **Show the current IP address**

1. On **"Switch#"** prompt, enter **"show ip interface brief".**
2. The screen displays the current IP address, subnet mask and gateway as shown in below.

```
Switch#config
Switch_config#interface vlan1
Switch_config_v1#ip address 192.168.1.254 255.255.255.0
Switch_config_v1#
Switch_config_v1#
Switch_config_v1#
Switch_config_v1#exit
Switch_config#show ip interface brief
Interface              IP-Address     Method Protocol-Status
Null0                  unassigned     manual up
VLAN1                  192.168.1.254 manual up
Switch_config#
```

Figure 3-7-2 Showing IP Information Screen

If the IP is successfully configured, the Managed Switch will apply the new IP address setting immediately. You can access the Web interface of Managed Switch through the new IP address.

Note

If you are not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

3.8 Starting Web Management

The Managed Switch provides a built-in browser interface. You can manage it remotely by having a remote host with Web browser, such as Mozilla Firefox, Google Chrome or Apple Safari.

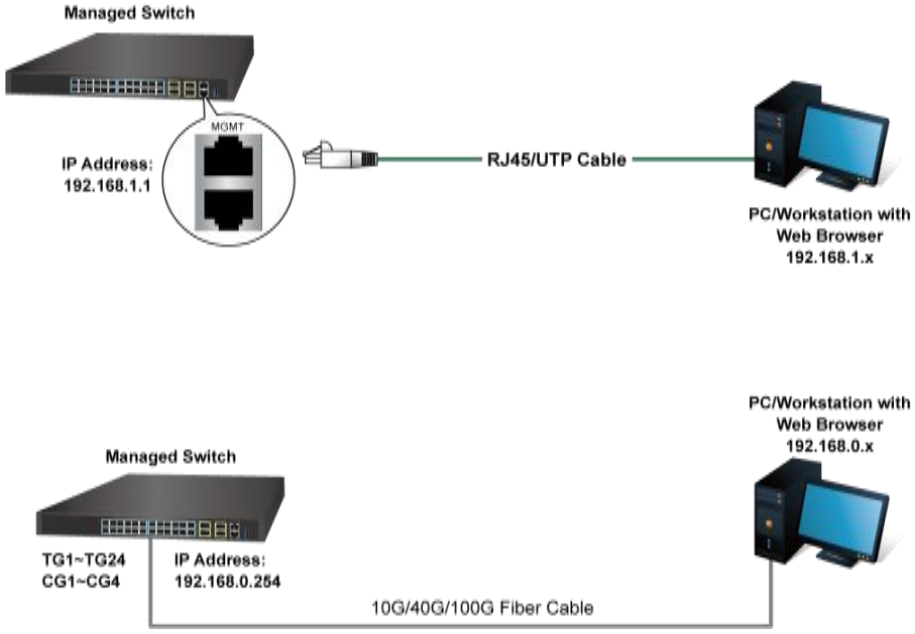


Figure IP Management Diagram

The following shows how to start up the **Web Management** of the Managed Switch. Please note the Managed Switch is configured through an Ethernet connection. Please make sure the manager PC must be set to the same **IP subnet address**.

3.9 Logging in to the Managed Switch from Management Port

1. Use Google Chrome or above Web browser and enter IP address https://192.168.0.254 (that you have just set in console) to access the Web interface.

Important!

The XGS-6350-24X2C, XGS-6350-16X8Y4C Managed Switches are shipped with Management **Port** IP address 1**92.168.1.1/24** assigned and **VLAN1 interface** IP address **192.168.0.254/24** assigned by default. User can assign another IP address to the Managed Switch via the console interface to be able to remotely access the Managed Switch through Telnet or HTTPs.

2. When the following dialog box appears, please enter the default user name and password. Refer to **Section 3-6** to determine your initial login password.

Default IP Address: **192.168.0.254**
Default User Name: **admin**
Default Password: **sw + the last 6 characters of the MAC ID in lowercase**

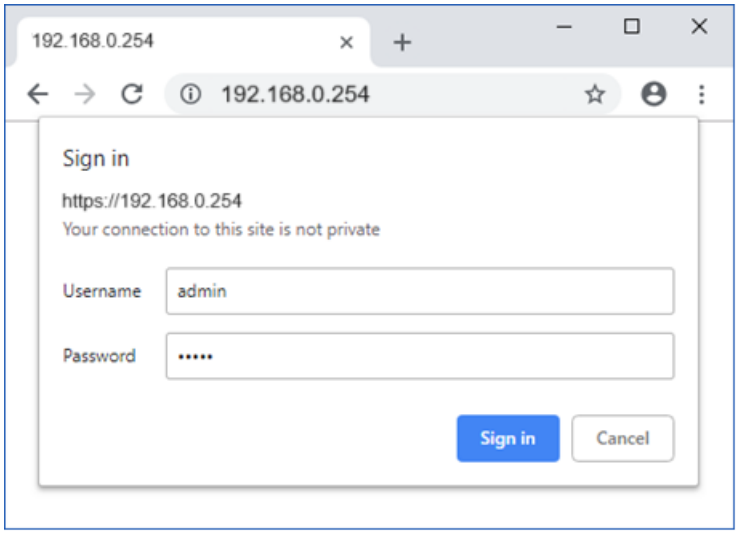


Figure 3-9-1 Login Screen

3. After logging in, you will be prompted to change the initial password to a permanent one.

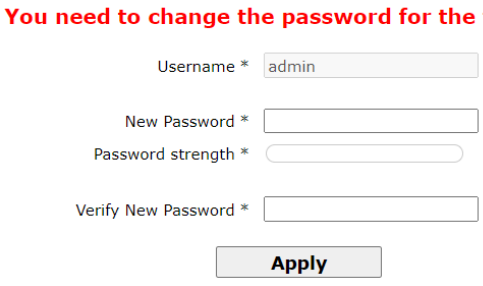


Figure 3-9-2: Create a New Password

4. After entering the password, the main screen appears as shown below.

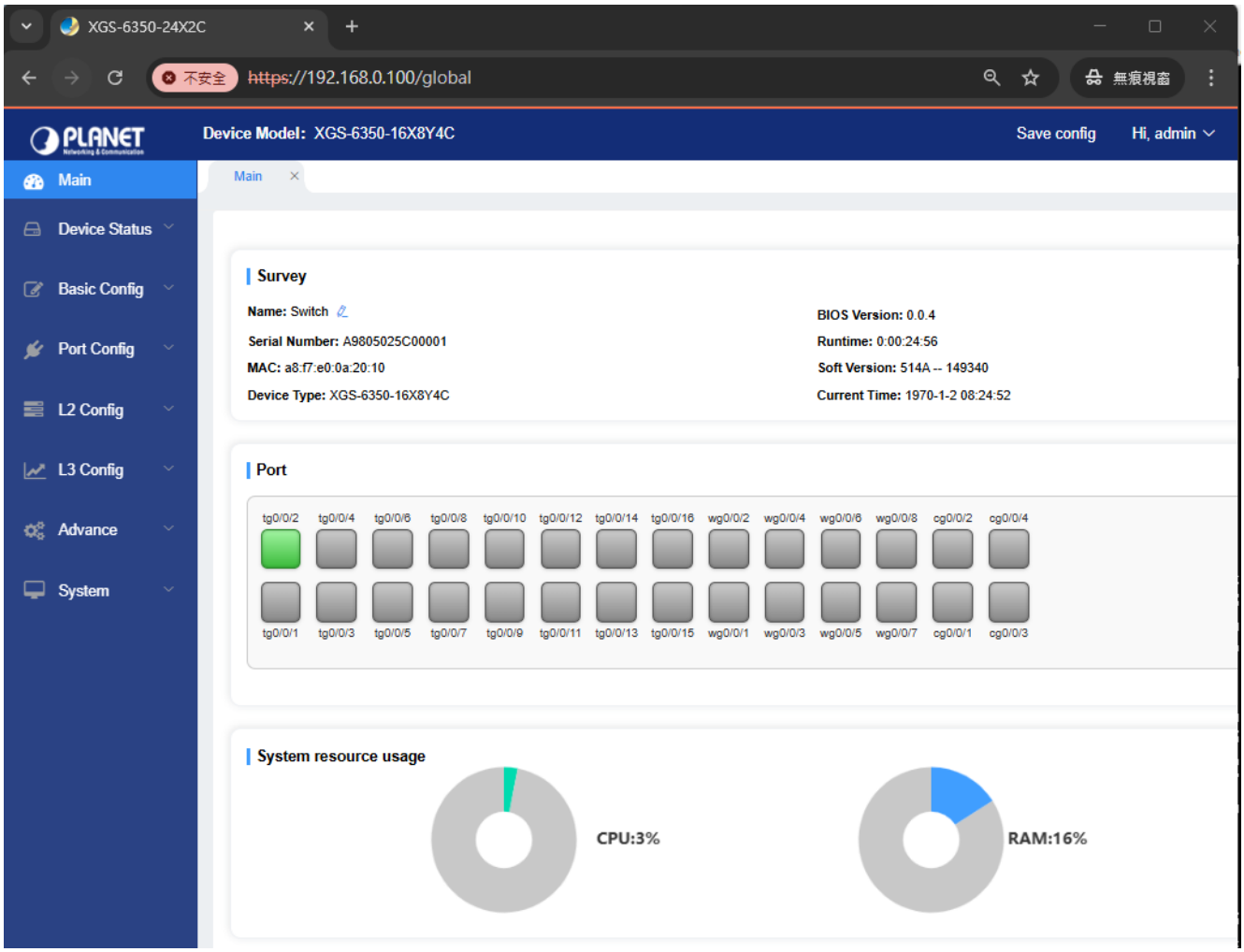


Figure 3-9-3 Web Main Screen of Managed Switch

5. The Switch Menu on the left of the Web page lets you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the Switch management or manage the Managed Switch by console interface. Please refer to the user manual for more.

3.10 Logging in to the Managed Switch

Use Google Chrome or above Web browser and enter IP address http://192.168.0.254 (that you have just set in console) to access the Web interface.

When the following dialog box appears, please enter the configured username "admin" and password "admin" (or the username/password you have changed via console). The login screen in below appears.

Figure Login Screen

After entering the password, the main screen appears as shown in below appears.

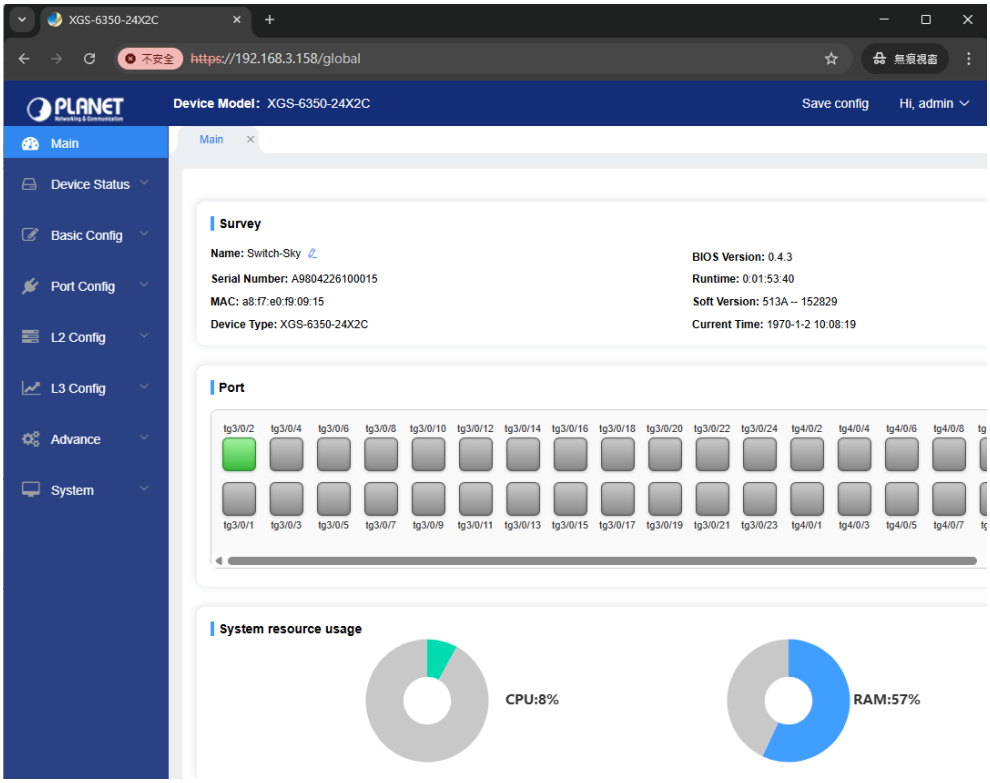


Figure Web Main Screen of Managed Switch

The Switch Menu on the left of the Web page lets you access all the commands and statistics the Switch provides. Now, you can use the Web management interface to continue the switch management or manage the Managed Switch by console interface. Please refer to the user manual for more.

3.11 Saving Configuration via the Web

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, such as "Refresh", "Apply" and "Confirm ".

The "**Apply**" button indicates applying the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file.

To save the configuration, you have to click "**Save config**" on the top control bar. "**Save config**" function is equivalent to the execution of the **write** command.

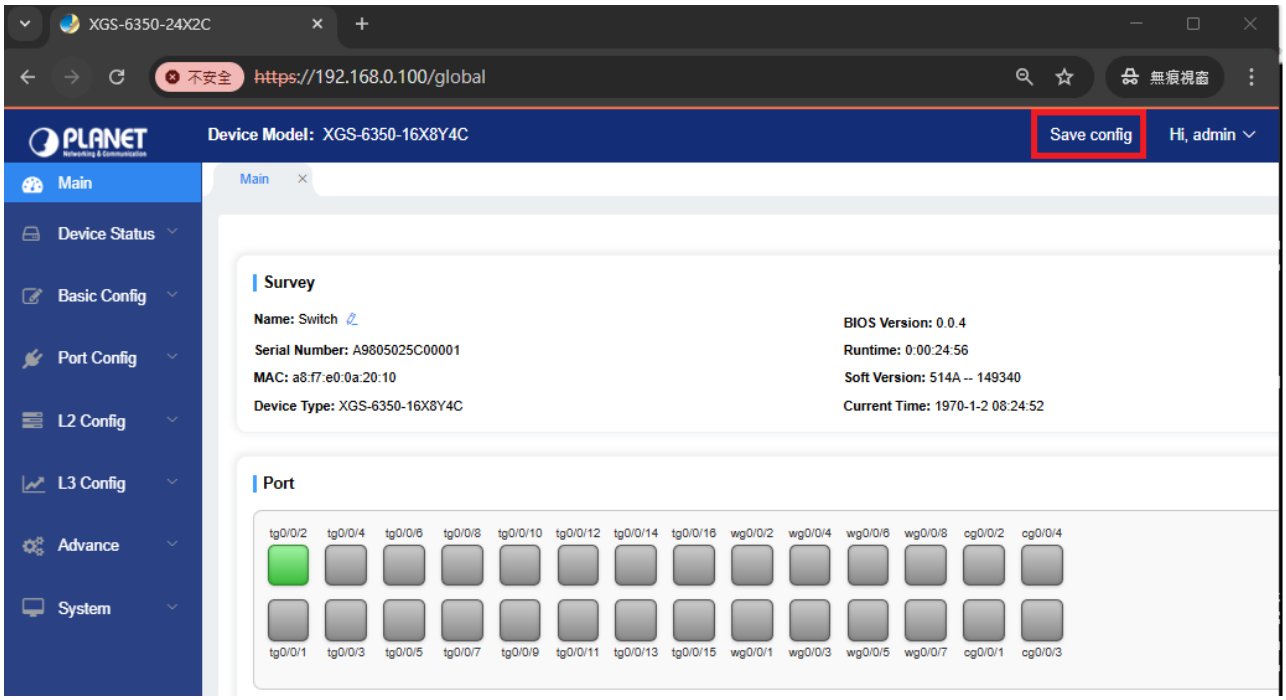


Figure Save Configuration

3.12 Recovering to the Default Configuration

When you forget the login password, use the following procedure to reset the device to the default configuration and restore the password.

- Use a console cable to access the CLI

Use a console cable to connect to the switch and reboot it.

At the **beginning of the boot-up**, press **"Ctrl+P"** to enter Monitor mode.

Enter the command "**format flash**" to restore the switch to factory default settings.

Then, follow the procedure described in below appears to reset the password.

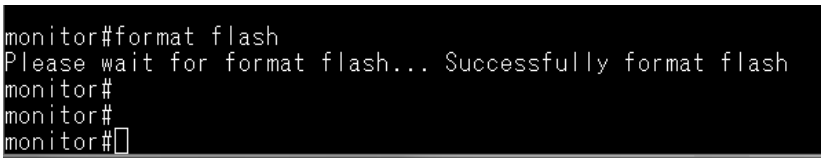


Figure : Restore to factory default settings

3.13 Discovery through PLANET NMS Controller (NMS-500/NMS-1000V)

The XGS-6350 Series is the Layer 3 Managed Ethernet Switch, which can be centrally monitored by PLANET NMS Controller.

Follow the steps below to discover the Layer 3 Managed Ethernet Switch through PLANET NMS controller (NMS-500/NMS-1000V). Please ensure each Layer 3 Managed Ethernet Switch uses a different static IP in the same subnet before physically connecting to the managed network.

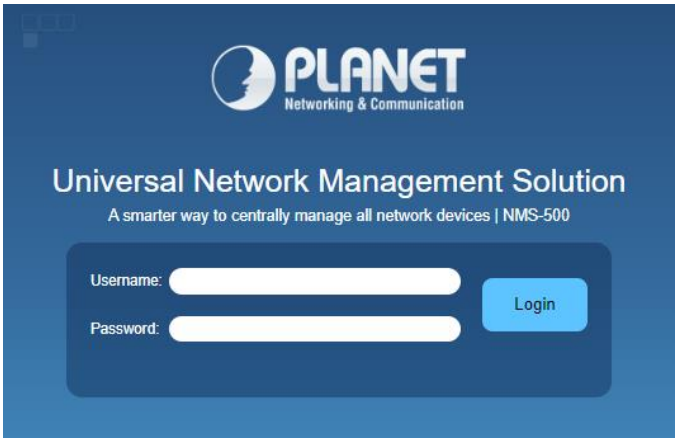
It supports PLANET NMS system and CloudNMS networking feature, which, with PLANET's free cloud service, allows users to quickly and easily detect, configure, deploy and manage devices remotely.

Note

1. Please regularly check PLANET website for the latest compatible list of the Layer 3 Managed Ethernet Switch in each firmware version.
2. Supports XGS-6350-16X8Y4C and XGS-6350-24X2C Layer 3 Managed Ethernet Switch. Please use the versions listed below:
   NMS-500: v1.0b260212 (Newer than the last version)
   NMS-1000V-10/12: v1.0b250410 (Newer than the last version)

Step 1. Launch the Web browser (Google Chrome is recommended.) and enter the default IP address https://192.168.1.100:8888 of the NMS controller. Then, enter the default username and password "admin" to log on to the system.

*The secure login with SSL (HTTPS) prefix is required.



Step 2. Go to the "**Domain**" page to discover and add the Layer 3 Managed Ethernet Switch to the device list. Then, you can search and add them and go to the **"Device List"** and **"Topology View"** page to monitor the Layer 3 Managed Ethernet Switch.

Pleaser refer to NMS-500/NMS-1000V User's Manual for the best experience.

3.14 PLANET Smart Discovery Utility

For easily listing the Layer 3 Managed Ethernet Switch in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution. The following installation instructions are to guide you to running the Planet Smart Discovery Utility.

1. Deposit the Planet Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

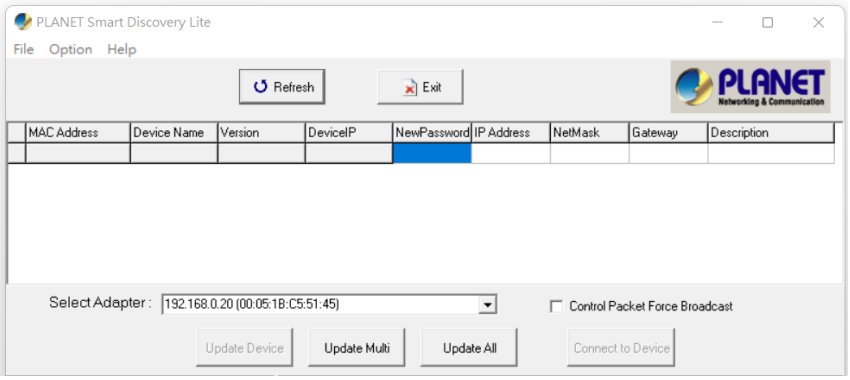


Figure : Planet Smart Discovery Utility Screen

Note

If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

3. Press the "Refresh" button for the currently connected devices in the discovery list as the screen shows below:

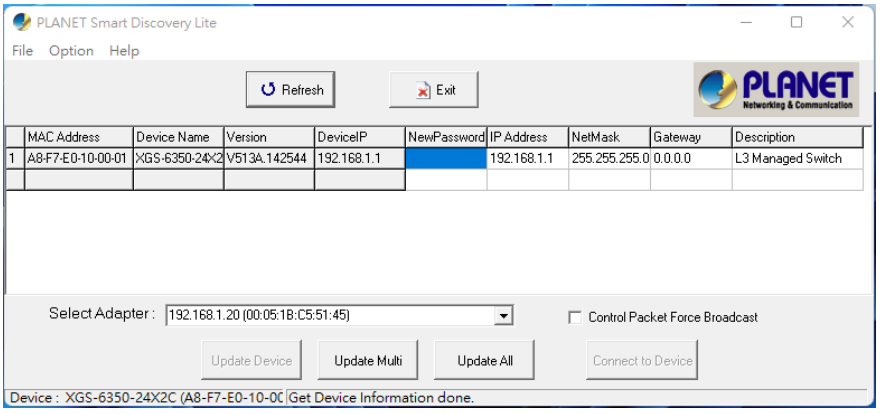


Figure : Planet Smart Discovery Utility Screen

4. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

Chapter 4 Basic Configuration Commands

4.1 Basic Terminal Commands

4.1.1 show version

Syntax

show version

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Display the version information

Example

The model in the example is for reference only.

```
Switch#show version
XGS-6350-24X2C Software, Version 513A Build 142544
PLANET Technology Corporation Internetwork Operating System Software
Copyright (c) 2021 PLANET Technology Corporation
Compiled: 2025-06-27 16:12:31 by SYS
ROM: System Bootstrap, Version: 0.3.5
Serial num:A9804224800001, ID num:0020083600543
Hardware version: 0002
PLANET RISC processor with 2048 MB of memory, 4096 MB of flash
Base ethernet MAC Address: a8:f7:e0:10:00:01
Out-band ethernet MAC Address: a8:f7:e0:10:00:01
In-band ethernet MAC Address: a8:f7:e0:10:00:02
SNMP info:
  vendor_ID:10456 product_ID:1670 system_ID:1.3.6.1.4.1.10456.1.1670.0
Switch uptime is 0:00:05:25, the current time is 1970-1-2 08:04:28
```

4.1.2 show o ir-information

Syntax

```
show oir-information
```

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The command is used to display the slot status information of the current upper and lower online boards, and present indicates that the online is complete and in the in-place state; online node indicates that the current online card is located at the node

Example

Switch#show oir-information

global oir information:

*Slot 0/0 type XGS-6350-24X2C(active present)

4.1.3 reboot

Syntax

reboot [**noconfirm**|**immediate**|**all**|**chassis** *chassis* [**slot** *slot*]]

Parameter Description

Parameter	Parameter Description
noconfirm	No need to confirm and restart the device directly
immediate	Restart your device immediately
all	Restart all devices under the stack
chassis	The chassis number of the chassis to be restarted
slot	The slot number of the slot needs to be restarted

Default Value

A message is prompted to confirm whether to restart

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

Reboot the local device, and the master controller can restart members, chassis, and the entire machine under the stack.

4.1.4 config

Syntax

config

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to switch from EXEC mode to Global Configuration mode.

Example

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

4.1.5 quit

Syntax

quit

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Exit the current configuration management view and go to the previous view, and the command is the same as exit.

Example

```
Switch(config)#
Switch(config)#quit Switch#
```

4.1.6 exit

Syntax

exit

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Equivalent to the quit command, exit the current configuration management view and go back to the previous view.

Example

```
Switch(config)#
Switch(config)#exit Switch#
```

4.1.7 exec-timeout

Syntax

exec-timeout *time* **no exec-timeout**

Parameter Description

Parameter	Parameter Description
time	The idle timeout period of the terminal is in units of 1s, and the range is 0~4294967295

Default Value

900s（ 15min ）

Command Mode

Global Configuration Mode

Usage Guidelines

If you configure the terminal exit time for any interaction behavior of the terminal None, the default is 15 minutes, and when 0s is configured, it does not need to exit. After the terminal is logged out, the user needs to log in again when using the terminal. This configuration is valid for the entire device.

Example

```
Switch(config)#
Switch(config)#exec-timeout 500
```

4.1.8 logging command

Syntax

[**no**] **logging command** [**hide**]

Parameter Description

Parameter	Parameter Description
hide	Whether to enable the hide special fields mode

Default Value

Disable command display

Command Mode

Global Configuration Mode

Usage Guidelines

Enable the function of displaying and recording the execution of commands on the user terminal, and the display result includes terminal information, user information, command execution information, execution results, etc.

After using hide parameter, the display of special fields will be masked, such as the password configured by the user, which may be replaced by "*". This configuration is valid for the entire device.

Example

```
Switch(config)#logging command
Switch(config)#Jan  3 04:57:35.994973 <5> klish[2518]:  %CMD-5-EXECUTE:  'logging command'
return
```

4.1.9 screen-paging

Syntax

[**no**] **screen-paging**

Parameter Description

None

Default Value

Turn on pagination

Command Mode

Global Configuration Mode

Usage Guidelines

After turning on pagination, most of the results that the user obtains through the command are automatically displayed in pagination, that is, after displaying to a certain number of rows, the user needs to interact and continue to display by responding to the "more" prompt, and the number of rows and columns of pagination is related to the terminal size that the screen command sets; This configuration is valid for the entire device.

The automatic pagination function can be canceled with the no command.

Example

Example is the display effect under the special configuration (screen width 256 length 10), which does not affect the actual effect.

```
Switch(config)#screen-paging Switch#show running-config  Building configuration...

Current configuration: !
! ! !
ip access-list standard test !
! ! !
port-protected 1 !
! ! ! ! ! !
--more--
```

4.1.10 screen

Syntax

screen [**auto**|**width** *width_num* [**length** *length_num*]|**length** *length_num* [**width** *width_num*]]

Parameter Description

Parameter	Parameter Description
auto	Automatically resizes the window based on the current terminal window size
width	Sets the current terminal window width
length	Sets the height of the current terminal window
width_num	Set the value of the current window width, range: 1~512 characters
length_num	Set the current window height value, range: 1~512 characters

Default Value

Width 256, height 40

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

When using screen without a parameter, the size of the current terminal window is displayed; This configuration is valid only for the current terminal. The command can only set the current terminal size and does not affect other terminal conditions. The console terminal is different from the telnet and ssh terminals, and the console terminal is set to a fixed value, but if the telnet and ssh terminals are manually dragged in the terminal window, the size will be automatically reset according to the size after dragging.

Example

```
Switch#screen auto
COLUMNS=200;LINES=67;export COLUMNS LINES; Switch#screen
Vty width  :200 Vty length:67
Switch#screen width 256 length 30 Switch#screen
Vty width  :256 Vty length:30
```

4.1.11 show

Syntax

show [……] [| {**grep**|**more**}|**>**|**>>**]

Parameter Description

Parameter	Parameter Description
grep	Filter the show command results
more	The show command result is displayed in pagination
>	Redirect the result of the show command to a certain path
>>	Append the show command result redirect to a certain path

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The show command is used to display information, and as long as the command starts with show, the relevant suffix can be used for information processing. For grep filtering commands, you can use them in combination with the following parameter:

`-n` : the line number of the filtered information with the original information; `-c` : Show only the number of matching rows; `-o` : Show only matching characters; `-v` : Select unmatched rows;

`-i` : ignore case;

`-w` : Hits are counted only when they match exactly;

`-x` : The hit is only counted when all rows match;

`-F` : The lookup field is a fixed value (not a regular expression); `-E` : The search field is an extended regular expression; `-m num` : only the first num times are matched, and subsequent matches are ignored; `-A num` : prints the num line information with the back of the matching line;

`-B num` : print the num line information with the front of the matching line;

`-C num`: Similar to `"-A num -B num"`, the print comes with the matching line before and after each num information; `-e` : specifies the regular expression to look for;

`-f` : reads the expression from the file as the target of the lookup; `WORD` : The string to be found;

For the more pagination command, you can subdivide it with the following parameter, which can be used in combination, using the more suffix can only be terminated with ctrl+c, and the Never method uses the ESC key, which is determined by the system using the more script:

-d: prompt "Press space to continue, 'q' to quit" to disable the ringing function; -f: When calculating the number of lines, the actual number of lines is used, not the number of lines after word wrapping;

-l: Cancel the function that will be paused when encountering special characters ^L (paper delivery characters); -p: do not scroll, by clearing the screen, then display the message;

-c: do not scroll, through the clear screen display, after the display, the previous screen will be cleared and no longer displayed, and the difference with -p is that -p will retain the previous information on the screen; -s: When there are more than two consecutive blank lines, replace them with one blank line;

-u: Do not show underlining and bolding; -n num : the number of rows displayed on each screen; -<num> : equivalent to -n num;

+<num> : Displays from low num lines;

+/<PATTERN> : STARTS WITH THE MATCHING ROWS;

Example

The example is for reference only and does not distinguish between special models.

```
Switch(config)#show version | grep -A 2 -w "Version"
XGS-6350-24X2C Software, Version 513A Build 142544
PLANET Technology Corporation Internetwork Operating System Software
Copyright (c) 2021 PLANET Technology Corporation
--
ROM: System Bootstrap, Version: 0.3.5
Serial num:A9804224800001, ID num:0020083600543
Hardware version: 0002
Switch(config)#
```

4.1.12 no

Syntax

no {……}

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The command is used to restore a command to its default state.

Example

None

4.1.13 hostname

Syntax

[**no**] **hostname** *name*

Parameter Description

Parameter	Parameter Description
name	The hostname of the device, within 64 characters

Default Value

Switch

Command Mode

Global Configuration Mode

Usage Guidelines

Configure the host name, this command is valid for the entire device.

Example

```
Switch(config)#hostname test test(config)#
```

4.2 File Management Commands

4.2.1 delete

Syntax

delete [*filename*]

Parameter Description

Parameter	Parameter Description
filename	filename

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

You can use the delete command to delete a file, if you don't enter the file name, delete the startup-config file with the default value.

4.2.2 dir

Syntax

dir

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the dir command to display the list of files in the current path.

4.2.3 rename

Syntax

rename *old_filename new_filename*

Parameter Description

Parameter	Parameter Description
old_filename	Original file name
new_filename	New file name

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

You can use the rename command to change the file name.

4.2.4 more

Syntax

more *filename*

Parameter Description

Parameter	Parameter Description
filename	filename

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the more command to view the contents of the file.

4.2.5 format

Syntax

format

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the format command to format the current drive letter.

4.2.6 pwd

Syntax

pwd

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the pwd command to display the current working directory name.

4.2.7 cd

Syntax

cd *directory*

Parameter Description

Parameter	Parameter Description
directory	目录

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the cd command to switch the working directory, which can be either an absolute path or a relative path.

4.2.8 md

Syntax

md *directory*

Parameter Description

Parameter	Parameter Description
directory	directory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the md command to create a new directory.

4.2.9 rd

Syntax

rd *directory*

Parameter Description

Parameter	Parameter Description
directory	directory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Use the rd command to delete a directory.

4.3 File Transfer Commands

4.3.1 copy ftp flash|system

Syntax

copy ftp:*src_filename* {**flash:/|system:/**}[*des_filename*] *server_ip* [*username*] [*password*] [*-m*] Parameter

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
username	Server username
password	The password for the server username
des_filename	Specify the name of the file stored in the flash disk or system disk, if not specified, the file name will be the same src_filename
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the ftp server to the OLT.

Example

```
copy ftp:fileA flash:/fileB 10.0.0.100 admin admin -m
```

4.3.2 copy tftp flash|system

Syntax

copy tftp:*src_filename* {**flash:/|system:/**}[*des_filename*] *server_ip* [*-m*] Parameter

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
des_filename	Specify the name of the file stored in the flash drive letter, if not specified, the file name will be the same as src_filename
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the tftp server to the OLT.

Example

```
copy tftp:fileA flash:/fileB 10.0.0.100 -m
```

4.3.3 copy flash|system ftp

Syntax

copy {**flash:/|system:/**}*src_filename* **ftp:***des_filename server_ip* [*username*] [*password*] Parameter

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the flash disk or system disk
server_ip	The IP address of the server
username	Server username
password	The password for the server username
des_filename	The name of the file on the FTP server

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Upload files from the OLT to the ftp server.

Example

```
copy flash:/fileA ftp:fileB 10.0.0.100 admin admin
```

4.3.4 copy flash|system tftp

Syntax

copy {**flash:/|system:/**}*src_filename* **tftp:***des_filename server_ip* Parameter

Parameter Description

Parameter	Parameter Description
src_filename	Files on flash disks or system disks
server_ip	The IP address of the server
des_filename	The name of the file on the TFTP server

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Upload files from the OLT to the tftp server.

Example

```
copy flash:/fileA tftp:fileB 10.0.0.100
```

4.4 Software Version Updates

4.4.1 copy ftp kernel

Syntax

copy ftp:*src_filename* **kernel** *server_ip* [*username*] [*password*] [*-n*] [*-m*]

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
username	FTP server username
password	The password corresponding to the FTP server username
-n	Version verification is not performed
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the ftp server to the OLT.

Example

```
copy ftp:switch.bin kernel 10.0.0.100 admin admin -n -m
```

4.4.2 copy tftp kernel

Syntax

copy tftp:*src_filename* **kernel** *server_ip* [*-n*] [*-m*]

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
-n	Version verification is not performed
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the tftp server to the OLT.

Example

```
copy tftp:switch.bin kernel 10.0.0.100 -n -m
```

4.5 bootrom Version Update

4.5.1 copy ftp rom

Syntax

copy ftp:*src_filename* **rom** *server_ip* [*username*] [*password*] [*-m*]

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
username	FTP server username
password	The password corresponding to the FTP server username
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the FTP server to the switch.

Example

```
copy ftp:eprom.bin rom 10.0.0.100 admin admin -m
```

4.5.2 copy tftp rom

Syntax

copy tftp:*src_filename* **rom** *server_ip* [*-m*]

Parameter Description

Parameter	Parameter Description
src_filename	The name of the file on the server
server_ip	The IP address of the server
-m	Temporary files are stored in memory

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Download the file from the tftp server to the OLT.

Example

```
copy tftp:eprom.bin rom 10.0.0.100 -m
```

4.6 Configuring Management Commands

4.6.1 show running-config

Syntax

show running-config [**global**|**non-interface**|**non-onu**|**chassis** *chass_num* [**slot** *slot_num*]|**interface** *port*|**slot** *chass_num*/*slot_num*|**pending** [**global**|**chass** *chass_num* [**slot** *slot_num*]]]

Parameter Description

Parameter	Parameter Description
global	Check the global related configurations
non-interface	Check the configurations of the global None port
non-onu	Check the configuration of the NoneONU port (supported only by GPON OLTs)
chassis	Check the configuration of the chassis
slot	Check the slot configurations on the chassis
pending	Check that the pending configuration has not been delivered
chass_num	Frame number, range: 0~10, 0 means single machine
slot_num	Slot number, range: 0~10, 0 means stand-alone
port	The name of the port

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Check the current configuration, in which the management port and logic port belong to the global configuration.

Example

```
Switch#
Switch#show running-config interface tg0/0/2 Building configuration...
Current configuration: !
interface tg0/0/2
storm-control broadcast threshold 500 storm-control multicast threshold 500 storm-control unicast threshold 500
```

4.6.2 write

Syntax

write

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Save the configuration to a persistent file, usually in the **startup-config** file or **config.tar.xz** file stored in flash. For individual models, the configuration will be packaged and persisted in the form of a package, and after the device is started, the relevant configuration will be unpacked and loaded. When you save the configuration, the persistence configuration file is automatically synchronized to all chassis, eliminating the need for manual synchronization

Example

```
Switch(config)#write
Jan  2 08:21:30.778964 <5> device-config:  Saving current configuration...
Jan   2  08:21:32.319457  <5>  device-config:   %DEVCFG-INFO:  Save  configuration  finish!
Switch(config)#
```

4.6.3 clear oir-information

Syntax

clear oir-information pending {**all**|**global**|**chassis** *chassis_num* [**slot** *slot_num*]}

Parameter Description

Parameter	Parameter Description
all	Clear all pending configurations
global	Clear the global pending configuration
chassis	Clear the chassis pending configuration
slot	Clear the pending configuration of the slots on the chassis
chass_num	Frame number, range: 0~10, 0 means single machine
slot_num	Slot number, range: 0~10, 0 means stand-alone

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Clear the pending configuration that has not been delivered, after clearing the relevant pending configuration, the relevant chassis or slot will be online in this run, and the configuration that existed in the pending before will not be delivered. If you need to apply this clearing to the situation after restarting in the future, you need to use write to save the configuration again to make it persistent.

Example

```
Switch#clear oir-information pending all
this configuration will be cleared,are you sure?(y/n) y
Switch#show running-config pending !
!No configurations pending !
Switch#
```

4.6.4 show configuration

Syntax

show configuration

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Check the configuration information saved in the current persistence configuration file.

Example

None

4.7 Calendar and Time Zone Management Commands

4.7.1 date

Syntax

date

Parameter Description

None

Default Value

Display the current date and time, and you can modify the current date and time

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

Display information such as the current date, time, time zone, etc., and can modify the time and date.

4.7.2 timezone

Syntax

[no] **timezone** *area*

Parameter Description

Parameter	Parameter Description
area	Regions where you need to convert time zones

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Modify the time zone of the current switch and restore the default time zone with the no command.

Example

```
timezone Asia/Shanghai
```

4.8 Persistent Log Management Commands

4.8.1 savelog

Syntax

savelog [**interval** *time* | **filemax** *filesnum* | **buffsize** *buffsize* | **filesize** *filesize* | **flush**]*

Parameter Description

Parameter	Parameter Description
interval *time*	Set the interval at which periodically it is saved to the log file. Default Value：3600s.
filemax *filesnum*	Set the number of persistent files to be retained for a long time. Default Value：30.
buffsize *buffsize*	Sets the maximum size of the cache buff. Default Value：1M.
filesize *filesize*	Set the maximum size of the log file to be saved. Default Value：2M.
flush	Save the cached data to a persistent log file.

Default Value

None

Command Mode

EXEC mode 和 Global Configuration Mode

Usage Guidelines

Logs can be persisted by setting the relevant parameter, where the buffsize needs to be less than the file size.

Example

```
Switch(config)#savelog interval 3000 buffsize 102400 filemax 12 filesize 204800 flush
```

4.8.2 show savelog_config

Syntax

show savelog_config

Parameter Description

None

Default Value

None

Command Mode

EXEC mode 或 Global Configuration Mode

Usage Guidelines

The command is used to display the configuration information of the current savelog.

Example

```
Switch#show savelog_config interval=3000
filemax=12
buffsize=102400 filesize=204800
```

4.9 Network Test Tool Commands

4.9.1 ping

Syntax

ping*host* [**-n** *number*] [**-a**] [**-l** *length*] [**-b** *interval*] [**-w** *waittime*] [**-t** *ttl*] [**-s** *tos*] [**-i** *source-address*] [**-6**]

Parameter Description

Parameter	Parameter Description
host	Destination host
-n *number*	The total number of packets sent. Default Value：5.
-a	Packets are sent until they are interrupted.
-l *length*	The length of the ICMP data in the packet. Default Value: 56 bytes.
-b *interval*	The interval at which the packet was sent. Default Value: 50 (unit: 10 milliseconds).
-w *waittime*	The amount of time that each packet waits for a reply. Default Value: 10 seconds.
-t *ttl*	TTL of the sent packet. Default Value：64.
-s *tos*	The TOS that sends the packet. Default Value：0.
-i *source-address*	The source address of the packet.
-6	Enforce the use of IPv6.

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

Test host reachability and network connectivity. Send an ICMP Echo Request packet to the other party and wait for the other party's ICMP Response Reply packet.

Output Information：

Parameter	Parameter Description
bytes	The length of the sent packet.
icmp_seq	The value of the ICMP sequence of the sending packet.
time	The round-trip time of the packet.

Statistics information:

Parameter	Parameter Description
packets transmitted	The total number of packets sent.
received	The number of reply packets received.
packet loss	The proportion of packets that did not receive a reply.
time	The time taken to send all packets.
rttmin/avg/max/mdev	Minimum/Mean/Maximum/Standard Deviation of Round-Trip Time.

Example

```
Switch#ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=255 time=1.83 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=255 time=1.75 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=255 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=255 time=8.35 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=255 time=1.68 ms

--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 2005ms rtt min/avg/max/mdev =
1.628/3.047/8.345/2.649 ms
```

4.9.2 traceroute

Syntax

traceroute *host* [**-w** *waittime*] [**-s** *tos*] [**-q** *probe-count*] [**-p** *port*] [**-t** *ttl*] [**-m** *hop-count*] [**-x**]

Parameter Description

Parameter	Parameter Description
host	Destination host
-w *waittime*	The amount of time that each packet waits for a reply. Default Value: 3 seconds.
-s *tos*	The TOS that sends the packet. Default Value：0.
-q *probe-count*	The number of packets that are detected each time. Default Value：3.
-p *port*	The port number of the destination port for sending UDP packets. Default Value：33434.
-t *ttl*	TTL of the sent packet. Default Value: The minimum value is 1 and the maximum value is 30.
-m *hop-count*	The maximum number of hops that can be passed by a probe packet. Default Value：64.
-x	Destination host

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command is used to detect the route to the destination. The route to the destination is determined by sending UDP packets (or ICMP ECHO packets) with different time-to-live (TTL) to the destination. Each router on the path must subtract its TTL value by 1 before forwarding the probe packet, and when the TTL value of the packet is reduced to 0, the router sends back an ICMP timeout message to the source address. The router on the path to the destination is determined by sending the first probe packet with a TTL of 1 and incrementing the TTL value by 1 each time in subsequent transmissions until the target responds or the maximum TTL value is reached. When the destination arrives, the destination node can only send an ICMP message (Port Unreachable) (if the probe packet is an ICMP ECHO packet, an ICMP reply packet will be sent back) because the probe packet is a UDP packet with port >number 30000.

Example

```
Switch#traceroute 2.1.1.1
traceroute to 2.1.1.1 (2.1.1.1), 64 hops max 1   1.1.1.1   1.814ms  1.597ms  1.613ms
2   2.1.1.1   2.651ms  1.873ms  1.845ms
```

4.10 Troubleshooting Commands

4.10.1 show debug

Syntax

show debug

Parameter Description

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command is used to display all debug information that is currently open for VTY.

Example

```
Switch#show debug
sys error debugging is on sys gs debugging is on
sys mblk debugging is on
```

4.10.2 no debug all

Syntax

no debug all

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode or Global Configuration Mode

Usage Guidelines

The command is used to disable all debug information that is open for the current VTY.

Example

```
switch#no debug all
```

Chapter 5 Monitor Mode Commands

5.1 Start Version Commands

5.1.1 boot kernel

Syntax

boot kernel

Parameter Description

None

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Read out the version from the kernel partition in flash and start the version.

Example

```
monitor#boot kernel
```

5.1.2 boot tftp ram

Syntax

boot tftp[:*file_name*] **ram** *server_ip*

Parameter Description

Parameter	Parameter Description
file_name	If you do not fill in the file name on the TFTP server, a hint will be prompted later
server_ip	The IP address of the TFTP server

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Download the version from the TFTP server into memory and launch the version.

Example

```
monitor#boot tftp:switch.bin ram 192.168.0.100
```

5.2 Copy Commands

5.2.1 copy tftp kernel

Syntax

copy tftp[:*file_name*] **kernel** *server_ip*

Parameter Description

Parameter	Parameter Description
file_name	If you do not fill in the name of the version file on the TFTP server, the user will be prompted to give the file name.
server_ip	The IP address of the TFTP server

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Download the version from the tftp server and write it to the kernel partition of the flash.

Example

Example1：

```
monitor#copy tftp kernel 192.168.0.100 Source file name[]?
```

Example2：

```
monitor#copy tftp:switch.bin kernel 192.168.0.100
```

5.2.2 copy tftp rom

Syntax

copy tftp[:*file_name*] **rom** *server_ip*

Parameter Description

Parameter	Parameter Description
file_name	If you do not fill in the name of the bootrom file on the TFTP server, the user will be prompted to give the file name
server_ip	The IP address of the TFTP server

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Download the file from the TFTP server and update your device's bootrom.

Example

Example1：

```
monitor#copy tftp rom 192.168.0.100 Source file name[]?
```

Example2：

```
monitor#copy tftp:1212128128.bin kernel 192.168.0.100
```

5.3 Erase Command

5.3.1 format

Syntax

format [*kernel*|*flash*|*system*|*all*]

Parameter Description

Parameter	Parameter Description
kernel	Erase the kernel partition
flash	Erase flash partitions
system	Erase the system partition
all	Erase kernel, flash, and system partitions

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Erase the partition

Example

Example1，ormat without parameter, then the kernel partition is erased by default (put the version of the partition)：

```
monitor#format
Please wait for format kernel... Successfully format kernel
monitor# Example2：
monitor#format system
Please wait for format system... Successfully format system monitor#
```

5.4 Configring IP Commands

5.4.1 ip address

Syntax

ip address *ip mask*

Parameter Description

Parameter	Parameter Description
ip	ip 地址
mask	Mask

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Configure the loca IP address and mask

Example

```
monitor#ip address 192.168.0.100 255.255.0.0
```

5.5 Network Test Commands

5.5.1 ping

Syntax

ping *dest_ip*

Parameter Description

Parameter	Parameter Description
dest_ip	ping packet destination IP address

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Ping packet test

Example

```
monitor#ping 192.168.0.200
```

5.6 Restart Commands

5.6.1 reboot

Syntax

reboot [**noconfirm**]

Parameter Description

Parameter	Parameter Description
noconfirm	No need to confirm and restart directly

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

Reboot

Example

```
monitor#reboot noconfirm
```

5.7 Display bootrom Version Information

5.7.1 show version

Syntax

show version [**all**]

Parameter Description

None

Default Value

None

Command Mode

Monitor Mode

Usage Guidelines

The command is used to display bootrom version information.

Example

The model in the example is for reference only.

```
monitor#show version
CLDK v20.07.01 U-Boot 2017.05+ (Sep 20 2024 - 14:39:46 +0800)
PLANET Technology Corporation Internetwork Operating System Software
Copyright (c) 2021 PLANET Technology Corporation
ROM: System Bootstrap, Version 0.3.5
Serial num:A9804224800001,ID num:0020083600543
PLANET XGS-6350-24X2C RISC processor
2048M bytes of memory,4096M bytes of flash
Base ethernet MAC Address: a8:f7:e0:10:00:01


monitor# show version all
  Module       Version        Description
  BSP          0.0.18         bsp lib(2024.9.09)
  MONITOR      0.0.8          monitor lib(2024.7.10)
monitor#
```

Chapter 6 802.1x Configuration Commands

6.1 802.1x Configuration Commands

6.1.1 dot1x enable

Syntax

dot1x enable

no dot1x enable

To enable dot1x, run the first command. To disable dot1x, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

If the 802.1x function is not enabled, you cannot start it on an interface. If the 802.1x function is forbidden, all interfaces do not have the 802.1x function, and at the same time, all 802.1x packets will not be received by CPU but can be forwarded in VLAN like normal multicast packets.

Example

The following example shows how to enable dot1x.

```
Switch(config)#dot1x enable Switch(config)#
```

6.1.2 dot1x port-control

Syntax

dot1x port-control {**auto**|**force-authorized**|**force-unauthorized**}

no dot1x port-control

To enable 802.1x on an interface, run the first command. To disable 802.1x, use the no form of this command.

Parameter Description

Parameter	Parameter Description
auto	Enables the 802.1x authentication mode
force-authorized	Mandatory enables 802.1X on the interface
force-unauthorized	Mandatory disables 802.1X on the interface

Default Value

Force-authorized

Command Mode

Interface Configuration Mode

Usage Guidelines

The 802.1x protocol is an interface-based two-layer authentication mode. You can run the auto command to enable the authentication mode. This authentication mode can be configured only on the physical interface and the interface's attributes cannot include VLAN backbone, dynamical access, security port or Monitoring port.

Example

The following example shows how to enable 802.1x on interface tg0/0/1.

```
Switch(config-tg0/0/1)# dot1x port-control auto Switch(config-tg0/0/1)#
```

The following example shows how to firstly set interface tg0/0/1 to the VLAN backbone and then enable 802.1x.

```
Switch(config-tg0/0/1)#switchport mode trunk Switch(config-tg0/0/1)#dot1x port-control auto
802.1x Control Failed, can 't config 802.1x on vlanTrunk port(tg0/0/1) Switch(config-tg0/0/1)#
```

6.1.3 dot1x authentication multiple-hosts

Syntax

dot1x authentication multiple-hosts

no dot1x authentication multiple-hosts

To configure multi-host access mode of 802.1x, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

Disable multi-host access mode of 802.1x.

Command Mode

Interface Configuration Mode

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. When one user passes the authentication, the port sets to the "up" state. Other users can access the port without authentication.

Note: After modifying the multi-host authentication mode, all users of the port will be authenticated again.

Example

The following example shows how to enable multi-hosts authentication on interface tg0/0/1.

```
Switch(config-tg0/0/1)# dot1x authentication multiple-hosts Switch(config-tg0/0/1)#
```

6.1.4 dot1x authentication multiple-auth

Syntax

dot1x authentication multiple-auth

no dot1x authentication multiple-auth

To configure multiple-auth authentication mode of 802.1x, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

Disable multiple-auth authentication mode of 802.1x

Command Mode

Interface Configuration Mode

Usage Guidelines

Set one port to the multi-hosts mode of 802.1x, and the switch will authenticate different users. Different users' authentications do not affect each other. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exists on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

Note: The multi-auth mode cannot coexist with guest vlan or mab. If an interface is in multi-authen mode, all users on the interface will be authenticated again.

Example

The following example shows how to enable multi-auth authentication on interface tg0/0/1.

```
Switch(config-tg0/0/1)# dot1x authentication multiple-auth Switch(config-tg0/0/1)#
```

6.1.5 dot1x default

Syntax

dot1x default

To resume all dot1x global configurations to the default setting, run the command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

To resume all global configurations to the default setting.

Example

The following command resumes all dot1x configurations to the default setting:

```
Switch(config)#dot1x default Switch(config)#
```

6.1.6 dot1x reauth-max

Syntax

dot1x reauth-max *count*

no dot1x reauth-max

To configure the times of re-authentication, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
count	Maximum re-authentication times, ranging between 1 and 10

Default Value

5

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to set the authentication retry times. If the retry times exceed the maximum retry times and the client has no response, the authentication is mounted.

Example

The following example shows how to configure the maximum times of dot1x identity authentication request to 4.

```
Switch(config)#dot1x reauth-max 4 Switch(config)#
```

6.1.7 dot1x re-authentication

Syntax

dot1x re-authentication

no dot1x re-authentication

To enable re-authentication, run the first command. To disable re-authentication, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After an interface passes authentication, the interface will still perform authentication to hosts in a certain period. You can run dot1x timeout re-authperiod to configure the period.

Example

The following example shows how to enable the re-authentication function.

```
Switch(config)#dot1x re-authentication Switch(config)#
```

6.1.8 dot1x timeout quiet-period

Syntax

dot1x timeout quiet-period *time*

no dot1x timeout quiet-period

To configure the quiet-period after the authentication failure, run the first command. To return to the default value, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time	Period for restarting dot1x authentication, ranging between 0 and 65535 seconds

Default Value

60s

Command Mode

Global Configuration Mode

Usage Guidelines

There is a certain period when the switch cannot perform any authentication after the previous authentication fails.

Example

The following example shows how to set the value of quiet-period to 40.

```
Switch(config)#dot1x timeout quiet-period 40 Switch(config)#
```

6.1.9 dot1x timeout re-authperiod

Syntax

dot1x timeout re-authperiod *time*

no dot1x timeout re-authperiod

To configure the re-authentication period of dot1x, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time	dot1x re-authentication period, ranging between 1 and 600000 seconds

Default Value

3600s

Command Mode

Global Configuration Mode

Usage Guidelines

This command is valid only when the re-authentication function is enabled.

Example

The following example shows how to set the dot1x re-authentication period to 7200 seconds.

```
Switch(config)# dot1x timeout re-authperiod 7200 Switch(config)#
```

6.1.10 dot1x timeout tx-period

Syntax

dot1x timeout tx-period

no dot1x timeout tx-period

To configure the time interval of the host client responses to the authentication request. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time	Time which ranges between 1 and 65535 seconds

Default Value

30s

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to set the client's authentication request response interval. If the interval is exceeded, the switch would re-transmit the authentication request.

Example

The following example shows how to set the transmission frequency to 24.

```
Switch(config)# dot1x timeout tx-period 24 Switch(config)#
```

6.1.11 dot1x mab

Syntax

dot1x mab

no dot1x mab

To enable mab authentication, run the first command. To disable mab authentication, use the no form of this command.

Parameter Description

None

Default Value

Disable

Command Mode

Interface Configuration Mode

Usage Guidelines

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB(MAC Authentication Bypass) authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

When the MAB authentication is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards this case as evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the Radius server has authorized this MAC address.

Note: The MAB authentication mode cannot coexist with the multi-auth mode.

Example

The following example shows how to enable mab authentication on port g0/0/1.

```
Switch(config-g0/0/1)# dot1x mab Switch(config-g0/0/1)#
```

6.1.12 dot1x mabformat

Syntax

dot1x mabformat {**1**|**2**|**3**|**4**|**5**|**6**}

no dot1x mabformat

To configure the mac address format of switch forwarding to radius server. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
1	Format of the MAC address: aa:bb:cc:dd:ee:ff
2	Format of the MAC address: AA:BB:CC:DD:EE:FF
3	Format of the MAC address: aabbccddeeff
4	Format of the MAC address: AABBCCDDEEFF
5	Format of the MAC address: ： aa-bb-cc-dd-ee-ff
6	Format of the MAC address: AA-BB-CC-DD-EE-FF

Default Value

The default is 1.

Command Mode

Global Configuration Mode

Usage Guidelines

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

Example

The following example shows how to set the format of MAC to 3.

```
Switch(config)# dot1x mabformat 3 Switch(config)#
```

6.1.13 dot1x user-permit

Syntax

dot1x user-permit *xxx*

no dot1x user-permit

To configure the port binding user, use the first command.To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
xxx	A username

Default Value

No user is bound, and all users will pass.

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be used to bind users on an interface. Each interface can be bound to one user. When the 802.1x authentication is enabled, the authentication is performed only to those bound users. However, to those unbound users, the authentication must fail.

Example

The following example shows how to bind users a on interface g0/0/1.

```
Switch(config-g0/0/1)# dot1x user-permit a Switch(config-g0/0/1)#
```

6.1.14 dot1x authen-type

Syntax

dot1x authen-type {**eap**|**chap**}

no dot1x authen-type

To configure the dot1x authentication type in global configuration mode, run dot1x authen-type. To resume the default settings in global configuration mode, run no dot1x authen-type.

Parameter Description

None

Default Value

The default dot1x authentication type is eap.

The default dot1x authentication type in global configuration mode is also used applied by default in interface configuration mode.

Command Mode

Global Configuration Mode

Usage Guidelines

The authentication type decides whether AAA uses CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server.

Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

Example

The following example shows how to set the authentication type on interface g0/1 to chap and the global authentication type to eap.

```
Switch(config)#dot1x authen-type eap
```

6.1.15 dot1x mac-permit

Syntax

dot1x mac-permit *h:h:h:h:h:h*

no dot1x mac-permit

To configure the 802.1x mac address binding, run the first command. To disable the 802.1x mac address, use the no form of this command.

Parameter Description

Parameter	Parameter Description
h:h:h:h:h:h	Configures the mac address binding on the interface

Default Value

There is no mac address binding, and all mac addresses are passed.

Command Mode

Interface Configuration Mode

Usage Guidelines

This command configures the MAC address bound to the port. One MAC address can be bound to each port. When 802.1x authentication is enabled, only the bound MAC address user will be authenticated. Other users will not be authenticated and will definitely fail.

Example

The following example shows how to set the mac address binding on interface g0/0/1 to aa:bb:cc:dd:ee:ff.

```
Switch(config-g0/0/1)# dot1x mac-permit aa:bb:cc:dd:ee:ff Switch(config-g0/0/1)#
```

6.1.16 dot1x guest-vlan

Syntax

dot1x guest-vlan

no dot1x guest-vlan

To enable the guest-vlan function of dot1x in global configuration mode, run dot1x guest-vlan. To disable the guest-vlan function of dot1x in global configuration mode, run no dot1x guest-vlan.

Parameter Description

None

Default Value

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the dot1x guest-vlan id command.

Note: This command cannot be set together with the multiple-auth command.

Example

The following example shows how to enable guest-vlan in the global configuration mode:

```
Switch(config)#dot1x guest-vlan
```

6.1.17 dot1x guest-vlan id

Syntax

dot1x guest-vlan *id*

no dot1x guest-vlan

The value of guest-vlan ranges from 1 to 4094.

To configure the dot1x guest-vlanid value of the port, run the first command. To delete the setting, use the no form of this command.

Parameter Description

ID: stands for the value of guest vlan, which can be any vlan ID configured in the system.

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

After the guest-vlan function is enabled, the corresponding port can be grouped into the guest vlan and specific network access rights are attributed to the port if a guest terminal does not respond.

This command is used together with the dot1x guest-vlan id command.

Note: This command cannot be set together with the multiple-auth command.

Example

The following example shows how to configure the guest-vlan id on port g0/0/1.

```
Switch(config-g0/0/1)#dot1x guest-vlan 2
```

6.1.18 dot1x keepalive

Syntax

dot1x keepalive

no dot1x keepalive

To enable the keepalive detection for the authentication user in the global configuration mode, run the first command. To disable the keepalive detection for the authentication user in the global configuration mode, use the no form of this command.

Parameter Description

None

Default Value

Enabled

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the switch to perform keepalive detection on the authentication client. The keepalive detection is enabled by default.

Example

The following example shows how to disable the keepalive detection for the authentication user.

```
Switch(config)#no dot1x keepalive Switch(config)#
```

6.1.19 dot1x vendor-permit

Syntax

dot1x vendor-permit

no dot1x vendor-permit

To enable vendor forwarding function in the global configuration mode, run the first command. To disable vendor forwarding function in the global configuration mode, use the no form of this command.

Parameter Description

None

Default Value

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to enable vendor forwarding function. The command enables the switch forwards vendor information to the radius authentication server during the authentication. The command is disabled by default.

The command is used with dot1x vendor command.

Example

The following example shows how to enable the vendor forwarding function in global configuration mode.

```
Switch(config)#dot1x vendor-permit Switch(config)#
```

6.1.20 dot1x vendor

Syntax

dot1x vendor *word*

no dot1x vendor

To set vendor information provided by radius server, run the first command.

Parameter Description

Parameter	Parameter Description
word	Vendor information

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the vendor information.

Example

The following example shows how to set the name of vendor to LENOVO in the global configuration mode.

```
Switch(config)#dot1x vendor LENOVO Switch(config)#
```

6.1.21 aaa authentication dot1x

Syntax

aaa authentication dot1x default *method*

no aaa authentication dot1x default

To configure the dot1x authentication mode, run the first command.

To disable the setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
method	Radius, local

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The method parameter provides a series of methods to authenticate the password of the client host. You'd better adopt the radius as the AAA authentication mode of 802.1x. You can also use the local configuration data for authentication, such as the user password saved in the local configuration.

Example

The following example shows how to configure the dot1x authentication method to RADIUS.

```
Switch(config)#aaa authentication dot1x default radius Switch(config)#
```

6.1.22 debug dot1x errors

Syntax

debug dot1x errors

To enable the dot1x error debugging information, run the first command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is used to export all error information occurred during dot1x running. The error information can help locate the errors.

6.1.23 debug dot1x state

Syntax

debug dot1x state

To output the status information in running dot1x.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The following shows the format of information output:

```
2003-3-18 17:40:09 802.1x:AuthSM(tg0/0/1) state Connecting-> Authenticating, event rxRespId
2003-3-18 17:40:09 802.1x:g0/0/1 Create user for Enter authentication
2003-3-18 17:40:09 802.1x:BauthSM(tg0/0/1) state Idle-> Response, event authStart 2003-3-18 17:40:09 802.1x:g0/0/1 user "myname" denied, Authentication Force Failed 2003-3-18 17:40:09 802.1x:g0/0/1 Authentication Fail
2003-3-18 17:40:09 802.1x:BauthSM(tg0/0/1) state Response-> Fail, event aFail
```

6.1.24 debug dot1x packet

Syntax

debug dot1x packet

To output the packet information in running dot1x, run the first command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

```
2003-3-18 17:40:09 802.1x:tg0/0/1 Tx --> Supplicant(0008.74bb.d21f) EAPOL  ver:01, type:00, len:5
EAP    code:01, id:03, type:01, len:5
00
2003-3-18 17:40:09 802.1x:tg0/0/1 Rx <-- Supplicant(0008.74bb.d21f) EAPOL  ver:01, type:00, len:10
EAP    code:02, id:03, type:01, len:10 62 64 63 6f 6d a5
```

6.1.25 show dot1x

Syntax

show dot1x [**interface** *intf-id*|**statistics**|**run-config** [**interface** *intf-id*]|**debug**]

To display the 802.1x configuration information, run the above command.

Parameter Description

Parameter	Parameter Description
interface	Displays dot1x interface information
intf-id	Stands for a specific physical interface
statistics	Displays dot1x statistics information
run-config	Displays dot1x configuration information
debug	Displays enabled debug information

Default Value

None

Command Mode

EXEC mode, configuring mode

Usage Guidelines

This command is used to display the 802.1x configuration information.

Example

The following example shows how to display 802.1x configuration information.

```
Switch_config#show dot1x 802.1X Parameters
reAuthen        No
reAuth-Period    3
quiet-Period     10
```

```
Tx-Period        30
Supp-timeout     30
Server-timeout   30
reAuth-max       4
max-request      2
authen-type      Eap
IEEE 802.1x on port tg0/0/1 enabled Authorized                    Yes
Authen Type                   Eap
Authen Method                default
Permit Users                  All Users
Multiple Hosts                Disallowed
Supplicant                    aaa(0008.74bb.d21f)
Current Identifier            21
Authenticator State Machine
State                         Authenticated
Reauth Count                  0
Backend State Machine
State                         Idle
Request Count                 0
Identifier (Server)           20
Port Timer Machine
Auth Tx While Time            16
Backend While Time            16
reAuth Wait Time              3
Hold Wait Time                0
```

Chapter 7 DHCP-snooping Configuration Commands

7.1 DHCP-snooping Global Configuration Commands

7.1.1 ip dhcp-relay snooping

Syntax

ip dhcp-relay snooping

no ip dhcp-relay snooping

To enable the DHCP-relay snooping function in a VLAN, run **ip dhcp-relay snooping**.

To return to the default setting, run **no ip dhcp-relay snooping**.

Parameter Description

None

Default Value

The dhcp-relay snooping function is disabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to enable the DHCP-relay snooping function:

```
Switch(config)#ip dhcp-relay snooping Switch(config)#
```

7.1.2 ip dhcp-relay snooping vlan

Syntax

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

To enable the DHCP snooping function in a VLAN, run **ip dhcp-relay snooping vlan**.

To disable the DHCP snooping function, run **no ip dhcp-relay snooping vlan**.

Parameter Description

Parameter	Parameter Description
vlan_id	ID of a VLAN Range: 1-4094

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the DHCP snooping in a VLAN.

Example

The following example shows how to conduct the snooping inspection of DHCP messages in VLAN2.

```
Switch(config)#ip dhcp-relay snooping vlan 2 Switch(config)#
```

7.1.3 ip dhcp-relay snooping vlan vlan_id max-client

Syntax

ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*

no ip dhcp-relay snooping vlan *vlan_id* **max-client**

To enable the DHCP attack protection function in a VLAN, run the first command.

To disable the DHCP attack protection in a VLAN, use the no form of this command.

Parameter Description

Parameter	Parameter Description
vlan_id	ID of a VLAN Range: 1-4094
number	Maximum number of users allowed: 0-65535.

Default Value

The default maximum number of users is 65535.

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the maximum number of users of the DHCP snooping in a VLAN, which implements the first-come, first-served principle. When the number of users in a VLAN reaches the configured maximum value, no new clients are allowed to be assigned.

Example

The following example shows how to conduct the snooping inspection to DHCP messages in VLAN2. The maximum number of users allowed is 3.

```
Switch(config)#ip dhcp-relay snooping vlan 2 max-client 3 Switch(config)#
```

7.1.4 ip dhcp-relay snooping log

Syntax

ip dhcp-relay snooping log

no ip dhcp-relay snooping log

To enable the DHCP-snooping log function, run the first command.

To disable the DHCP-snooping log function, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After the log function is enabled, if there is a message from the DHCP server on a distrusted port, the syslog will be reported to indicate which port has an illegal DHCP server.

Example

The following example shows how to enable the DHCP-snooping log function.

```
Switch(config)#ip dhcp-relay snooping log Switch(config)#
```

7.1.5 ip dhcp-relay snooping rapid-refresh-bind

Syntax

ip dhcp-relay snooping rapid-refresh-bind

no ip dhcp-relay snooping rapid-refresh-bind

To enable the DHCP snooping rapid-refresh-bind function, run the first command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After this function is enabled, the DHCP attack of forged MAC will be closed. While the client will be allowed to directly obtain the address after changing the access port without waiting for the IP address lease to expire.

After this function is disabled, if the client changes the access port, the device with snooping enabled will regard it as a DHCP message attack with a forged MAC and will drop the DHCP message.

Example

None

7.1.6 ip dhcp-relay snooping information option

Syntax

ip dhcp-relay snooping information option [**format** {**snmp-ifindex**|**manual**|**cm-type**|**hw-type**|**hn- type** [**host**]}]

no ip dhcp-relay snooping information option [**format** {**snmp-ifindex**|**manual**|**cm-type**|**hw- type**|**hn-type** [**host**]}]

To configure DHCP-snooping to forward DHCP messages with option 82, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
format snmp-ifindex	Fills in option82 in **SNMP ifindex** mode (optional).
format manual	Use manual configuration to fill in option82 (optional)
format cm-type	Fill in option82 using cm-type format (optional)
format hw-type	Fill in option82 using Huawei format (optional)
format hn-type [**host**]	Fill in option82 using cisco format (optional), and Host means the device is configured as the primary device

Default Value

Option 82 will not be added to or removed from the report by default.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If **format snmp-ifindex** is designated, Use the **SNMP ifindex** mode to fill in option 82. If format manual is designated, the circuit-id option of option82 is filled in using the string configured on each port using the command dhcp snooping information circuit-id string. Otherwise, fill in option 82 according to RFC3046.

Example

The following example shows how to fill in option 82 in **SNMP ifindex** mode.

```
Switch(config)#ip dhcp-relay snooping

Switch(config)#ip dhcp-relay snooping information option format snmp-ifindex
```

The following example shows how to fill in option 82 in manual mode.

```
Switch(config)#ip dhcp-relay snooping

Switch(config)#ip dhcp-relay snooping vlan [WORD]   //[WORD] is the VLAN name for which
the snooping function needs to be enabled

 Switch(config)#ip dhcp-relay snooping information option format manual
```

7.1.7 ip dhcp-relay snooping upper-filter

Syntax

ip dhcp-relay snooping upper-filter

no ip dhcp-relay snooping upper-filter

To enable the DHCP message upper filter function, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is mainly used to check whether the destination port number of the DHCP message received by the uplink port is correct. When the uplink port opens dhcpsnooping trust and ip dhcp-relay snooping upper-filter, if the destination port number of the message sent by the server is DHCP_SPORT (67), the message will be dropped.

Example

The following command will enable DHCP message upper filter.

```
Switch(config)#ip dhcp-relay snooping upper-filter Switch(config)#
```

7.1.8 ip verify source vlan

Syntax

ip verify source vlan *vlanid*

no ip verify source vlan *vlanid*

To enable the packet source IP address detection function for all distrusted interfaces in the VLAN, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
vlanid	ID of a VLAN Range: 1-4094

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to configure a VLAN for monitoring the source IP address. The "no" form of this command is used to cancel this VLAN. If the source IP and source MAC of the IP message are not the legal client addresses assigned by the DHCP server monitored by DHCP snooping, then such messages will be regarded as illegal messages in the VLAN where IP source address monitoring is enabled and will be dropped.

Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch(config)#ip verify source vlan 2 Switch(config)#
```

7.1.9 ip arp inspection vlan

Syntax

ip arp inspection vlan *vlanid*

no ip arp inspection vlan *vlanid*

To enable dynamic ARP monitoring for all distrusted ports in the VLAN, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
vlanid	ID of a VLAN Range: 1-4094

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the VLAN for ARP message source address monitoring and use the no command to remove the monitoring. In the VLAN where ARP message source address monitoring is enabled, the ARP message with SIP and SMAC that do not match the IP address and MAC address assigned by the DHCP server to the client will be dropped.

Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch(config)#ip arp inspection vlan 2 Switch(config)#
```

7.1.10 ip source binding

Syntax

ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **interface** *name* **vlan** *vlan-id*

no ip source binding *xx:xx:xx:xx:xx:xx A.B.C.D* **vlan** *vlan-id*

To add or delete the MAC-to-IP address binding on an interface manually, run the first command.

Parameter Description

Parameter	Parameter Description
xx:xx:xx:xx:xx:xx	MAC address.
A.B.C.D	IP address
Name	Name of the interface
vlan-id	Vlanid number

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to bind MAC address 08:00:3e:00:00:01 to IP address **192.168.1.2** on interface tg0/0/1.

```
Switch(config)#ip source binding 08:00:3e:00:00:01 192.168.1.2 interface tg0/0/1
Switch(config)#
```

7.2 DHCP-snooping Interface Configuration Commands

7.2.1 arp inspection trust

Syntax

arp inspection trust

no arp inspection trust

To configure the interface is an ARP monitoring trusted interface, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

The interfaces are distrusted ones by default.

Command Mode

Interface Configuration Mode

Usage Guidelines

The ARP monitoring is not run with the ARP-trusted interface. The "no" form of this command is used to configure the default value of this interface.

Example

The following example shows how to set the interface tg0/0/1 to an ARP-trusted interface.

```
Switch(config-tg0/0/1)#arp inspection trust
```

7.2.2 dhcp snooping trust

Syntax

dhcp snooping trust

no dhcp snooping trust

To configure the interface as a DHCP trusted interface, run the first command.

To return to the default setting, run the no form of this command.

Parameter Description

None

Default Value

The default interface is a distrusted one.

Command Mode

Interface Configuration Mode

Usage Guidelines

DHCP snooping is not run with the DHCP-trusted interface. The "no" form of this command is used to resume the default value of this interface.

Example

The following example shows how to set the interface GigaEthernet0/0/1 to a DHCP-trusted interface.

```
Switch(config-tg0/0/1)#dhcp snooping  trust
```

7.2.3 dhcp snooping deny

Syntax

dhcp snooping deny

no dhcp snooping deny

To disable snooping monitoring on the port, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

DHCP snooping is allowed on the default interface.

Command Mode

Interface Configuration Mode

Usage Guidelines

Disable DHCP snooping monitoring on the port. After this command is configured, DHCP snooping trust, IP-source trust and ARP inspection trust are automatically enabled. The "no" form of this command is used to configure the default value of this interface.

Example

The following example shows how to disable DHCP snooping on interface GigaEthernet0/0/1.

```
Switch(config-tg0/0/1)#dhcp snooping deny
```

7.2.4 dhcp snooping information circuit-id

Syntax

dhcp snooping information circuit-id {**string** *STRING*|**hex** *xx-xx-xx-xx-xx-xx*}

no dhcp snooping information circuit-id

To configure the circuit-id sub-option in interface configuration mode, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
string *STRING*	String carried by the Option82 circuit-id suboption
hex *xx-xx-xx-xx-xx-xx*	Hexadecimal number carried by the Option82 circuit-id suboption

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured on each port connected to the client. This command can be used to configure the option 82 sub-option of the DHCP message sent by the DHCP client monitored by DHCP snooping to the DHCP server. (The option 82 switch needs to be turned on manually, see the command ip dhcp- relay snooping information option format manual).

Example

Configuring the option 82 sub-option to group 1 manually on port g0/0/3, which port belongs to vlan 1.

```
Switch(config)#ip dhcp-relay snooping
Switch(config)#ip dhcp-relay snooping vlan 1
Switch(config)#ip dhcp-relay snooping information option format manual
Switch(config)#interface g0/0/3
Switch(config-g0/0/3)#dhcp snooping information circuit-id string group1
```

7.2.5 dhcp snooping information remote-id

Syntax

dhcp snooping information remote-id {**string** *STRING*|**hex** *xx-xx-xx-xx-xx-xx*}

no dhcp snooping information remote-id

To configure the remote-id sub-option in interface configuration mode, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
string *STRING*	String carried by the Option82 remote-id suboption
hex *xx-xx-xx-xx-xx-xx*	Hexadecimal number carried by the Option82 remote-id suboption

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client. This command can be used to configure the option 82 sub-option of the DHCP message sent by the DHCP client monitored by DHCP snooping to the DHCP server. (The option 82 switch needs to be turned on manually, see the command ip dhcp- relay snooping information option format manual).

Example

Configuring the option 82 sub-option to group 1manually on port g0/0/3, which port belongs to vlan 1.

```
Switch(config)#ip dhcp-relay snooping
Switch(config)#ip dhcp-relay snooping vlan 1
Switch(config)#ip dhcp-relay snooping information option format manual
Switch(config)#interface g0/0/3
Switch(config-g0/0/3)# dhcp snooping information remote-id string group1
```

7.2.6 dhcp snooping information vendor-specific

Syntax

dhcp snooping information vendor-specific {**string** *STRING*|**hex** *xx-xx-xx-xx-xx-xx*} **no dhcp snooping information vendor-specific**

To configure the vendor-specific sub-option in interface configuration mode, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
string *STRING*	String carried by the Option82 vendor-specific suboption
hex *xx-xx-xx-xx-xx-xx*	Hexadecimal number carried by the Option82 vendor-specific suboption

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client. This command can be used to configure the option 82 sub-option of the DHCP message sent by the DHCP client monitored by DHCP snooping to the DHCP server. (The option 82 switch needs to be turned on manually, see the command **ip dhcp- relay snooping information option format manual.**

Example

Configuring option82 vendor-specific (suboption 9) with hexadecimal 00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34 on port tg0/0/3.

```
Switch(config)# ip dhcp-relay snooping

Switch(config)# ip dhcp-relay snooping vlan 1

Switch(config)#ip dhcp-relay snooping information option format manual
Switch(config)#interface tg0/0/3

Switch(config-tg0/0/3)# dhcp snooping information vendor-specific hex 00-00-00-09-0d-01-0b-78-69
```

7.2.7 dhcp snooping information append

Syntax

dhcp snooping information append

dhcp snooping information append first-subop9-param {**hex** *xx-xx-xx-xx-xx-xx*|**hostname**|**vlanip**}

dhcp snooping information append second-subop9-param {**hex** *xx-xx-xx-xx-xx-xx*|**hostname**|**vlanip**}

no dhcp snooping information append

no dhcp snooping information append first-subop9-param

no dhcp snooping information append second-subop9-param

To append request packets containing option82, run the first command. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
first-subop9-param hex [*xx-xx- xx-xx-xx-xx*]	Option82 vendor-specific (suboption9) The hexadecimal value of the first Parameter in the suboption
second-subop9-param hex [*xx- xx-xx-xx-xx-xx*]	Option82 vendor-specific (suboption9) The hexadecimal value of the second Parameter in the suboption
hostname	Option82 vendor-specific (suboption9) The parameter of the suboption is the host name
vlanip	Option82 vendor-specific (suboption9) The parameter of the suboption is the IP address of the interface vlan

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client. This command can be used to configure the option 82 sub-option of the DHCP message sent by the DHCP client monitored by DHCP snooping to the DHCP server.

This command is a switch command when it does not have Parameter. When append is enabled, it will add its own information to suboption9 of option82. The additional information is first-subop9-param and second-subop9-param.

Example

On port tg0/0/3, expand the DHCP message with option 82 and configure sub-option 9 with hexadecimal 61-62-63-61-62-63 to add Parameter.

```
Switch(config-tg0/0/3)#dhcp snooping information append
```

```
Switch(config-tg0/0/3)#dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
```

61-62-63-61-62-63 is the hexadecimal value of the parameter to be added.

7.2.8 dhcp snooping information drop

Syntax

dhcp snooping information drop

no dhcp snooping information drop

To drop the request packets containing option 82, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client.

Configure to drop the request packets containing option 82.

After this command is configured, the request packets containing option 82 will be dropped on the specified port.

Example

Drop the DHCP message with option 82 on port tg0/0/3

```
Switch(config-tg0/0/3)# dhcp snooping information drop
```

7.2.9 dhcp snooping information replace

Syntax

dhcp snooping information replace

no dhcp snooping information replace

To replace the request packet containing option82, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client.

After this command is configured, option 82 in the message received from the downlink port will be stripped, and then the global configuration option 82 will be added.

Example

The following command shows how to replace the DHCP message with option 82 on port tg0/0/3.

```
Switch(config-tg0/0/3)#dhcp snooping information replace
```

7.2.10 dhcp snooping information transmit

Syntax

dhcp snooping information transmit

no dhcp snooping information transmit

To forward the request packets containing option 82, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be configured at each port connected to the client.

After this command is configured, DHCP packets with Option 82 coming from the relay are directly forwarded without packet loss.

Example

Configure to forward DHCP packets with option 82 on port tg0/0/3.

```
Switch(config-tg0/0/3)# dhcp snooping information transmit
```

7.2.11 ip-source trust

Syntax

ip-source trust

no ip-source trust

To configure the interface as an IP source address trusted interface, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

The default interface is a distrusted one.

Command Mode

Interface Configuration Mode

Usage Guidelines

Source IP address snooping is not conducted to the source-IP-trusted interface. The "no" form of this command is used to resume the default value of this interface.

Example

The following example shows how to set the interface tg0/0/1 to a source-ip-trusted interface.

```
Switch(config-tg0/0/1)#ip-source trust
```

7.2.12 dhcp max-client

Syntax

dhcp max-client *number* **no dhcp max-client**

To configure the maximum number of users allowed on the interface, run the first command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
number	The maximum number of users allowed ranges from 0 to 1024.

Default Value

By default, the maximum number of users allowed is 65535.

Command Mode

Interface Configuration Mode

Usage Guidelines

Configured on the downlink port.

Example

The following command limits the maximum number of users on port tg0/0/1 to 100.

```
Switch(config-tg0/0/1)#dhcp max-client 100
```

7.3 DHCP-snooping Display Configuration Commands

7.3.1 show ip dhcp-relay snooping

Syntax

show ip dhcp-relay snooping

To display the DHCP snooping configuration information, run the command.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

Display Dhcp-relay snooping configuration information

Example

This command is used to display information about DHCP-relay snooping configuration.

```
Switch(config)#show ip dhcp-relay snooping
```

7.3.2 show ip dhcp-relay snooping binding

Syntax

show ip dhcp-relay snooping binding [**all**]

To display the address binding entries that are effective on the interface, run the command.

All means that all binding entries generated by DHCP snooping are displayed.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

The command is used to display the added-to-port binding information of dhcp-relay snooping.

The command all displays all DHCP-relay snooping binding information.

Example

The following example shows how to display the binding information about DHCP-relay snooping.

```
Switch(config)#show ip dhcp-relay snooping binding
```

7.3.3 show ip dhcp-relay snooping statistics

Syntax

show ip dhcp-relay snooping statistics

To display dhcp-relay snooping data information, run the command.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

The command is used to display dhcp-relay snooping data information.

Example

The following example shows how to display data information about DHCP-relay snooping.

```
Switch(config)#show ip dhcp-relay snooping statistics
```

7.3.4 show ip dhcp-relay snooping debug

Syntax

show ip dhcp-relay snooping debug

To display the dhcp-relay snooping debug information, run the command.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

Display debug information for enabling dhcp-relay snooping.

Example

The following example shows how to display the debug information about DHCP-relay snooping.

```
Switch(config)#show ip dhcp-relay snooping debug
```

7.3.5 show ip dhcp-relay snooping run-config

Syntax

show ip dhcp-relay snooping run-config [**interface** *name*]

To display the global or interface configuration information of dhcp-relay snooping, run the command.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

The command is used to display the global or interface configuration information of dhcp-relay snooping.

Example

The following example shows how to display the global configuration information about DHCP-relay snooping.

```
Switch(config)#show ip dhcp-relay snooping run-config
```

7.4 DHCP-snooping Debug Commands

7.4.1 debug ip dhcp-relay snooping

Syntax

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

To enable DHCP-relay snooping debugging, run the first command. To disable DHCP-relay snooping debugging, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable DHCP-relay snooping debugging.

Example

The following example shows how to enable DHCP-relay snooping debugging.

```
Switch#debug ip dhcp-relay snooping Switch#
```

7.4.2 debug ip dhcp-relay event

Syntax

debug ip dhcp-relay event

no debug ip dhcp-relay event

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable the DHCP-relay event debugging.

Example

The following example shows how to enable DHCP-relay event debugging.

```
Switch#debug ip dhcp-relay event Switch#
```

7.4.3 debug ip dhcp-relay binding

Syntax

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

To enable the DHCP-relay snooping binding debugging, run the first command. To disable the DHCP-relay snooping binding debugging, use the no form of this command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable the DHCP-relay snooping binding debugging.

Example

The following example shows how to enable the DHCP-relay snooping binding debugging.

```
Switch#debug ip dhcp-relay binding
```

7.4.4 debug ip dhcp-relay all

Syntax

debug ip dhcp-relay all

no debug ip dhcp-relay all

To enable all debugging switches of DHCP-relay snooping, run the first command. To disable all debugging switches of DHCP-relay snooping, use no form of this command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable all debugging switches of DHCP-relay snooping.

Example

The following example shows how to enable all debugging switches of DHCP-relay snooping.

```
Switch#debug ip dhcp-relay all
```

Chapter 8 DNS Configuration Commands

8.1 DNS Configuration Commands

8.1.1 ip name-server

Syntax

[**no**] **ip name-server** *server_ip*

Parameter Description

Parameter	Parameter Description
server_ip	DNS server IP address

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

You can configure multiple DNS name-servers locally, and the configured IP address can be used as the server side for query. When querying a domain name, the configured name-server is used as the query target to send the query.

Example

The following command adds the IP address of a DNS server.

```
Switch(config)#ip name-server 8.8.8.8
```

The following command deletes all name-servers with the no prefix.

```
Switch(config)#no ip name-server
```

The following command uses the no prefix to delete the specified name-server.

```
Switch(config)#no ip name-server 8.8.8.8
```

8.1.2 ip domain-list

Syntax

[**no**] **ip domian-list** *search-domain*

Parameter Description

Parameter	Parameter Description
search-domain	DNS search domains.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Multiple domain lists can be configured locally, and these domain lists will be added to the domain name to be queried as a suffix, and then sent to the name-server query after combination.

Example

The following command adds a search domain.

```
Switch(config)#ip domain-list com
```

The following command deletes all search domains.

```
Switch(config)#no ip domain-list
```

The following command deletes the specified search domain.

```
Switch(config)#no ip domain-list com
```

8.1.3 ip host

Syntax

[**no**] **ip host** *domain-name ip-address*

Parameter Description

Parameter	Parameter Description
domain-name	Domain name.
ip-address	The IP address of the domain name.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The local IP HOST can be configured and saved as a static domain name mapping. After configuration, the static IP address will be used in preference to the configured static IP address.

Example

The following command adds a domain mapping.

```
Switch(config)#ip host www.test.com 1.1.1.1
```

The following command deletes a domain mapping.

```
Switch(config)#no ip host www.test.com
```

8.1.4 clear dns cache

Syntax

clear dns cache

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to clean the DNS cache. DNS caching can temporarily store records on the DNS server locally after querying, avoiding queries every time a domain name is resolved . After the DNS cache is cleared, the query request is resent when the domain name is resolved.

Example

The following command clears the DNS cache.

```
Switch#clear dns cache
```

8.2 DNS Display Commands

8.2.1 show dns config

Syntax

show dns config

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to display the DNS information that is currently configured.

Example

The following command displays the currently configured DNS information.

```
Switch#show dns config Static DNS:
10.1.1.1

DHCP DNS:

Hosts:
www.test.com    1.1.1.1

Domains: cn com
```

Chapter 9 DoS-Attack Prevention Configuration Commands

9.1 DoS-Attack Prevention Configuration Commands

9.1.1 dos enable

Syntax

[**no**] **dos enable** {**all** | **icmp** | **ip** | **l4port** | **mac** | **smac** | **pingflood** | **synflood** | **tcpflags** | **tcp smurf** | **icmpsmurf** | **ipsmurf** | **nullscan** }

Parameter Description

Parameter	Parameter Description
all	Enable to defend against all kinds of DoS attack messages.
icmp	Enable ICMP messages detection
ip	Enable detection of IP messages with the same source IP and destination IP.
l4port	Enable detection of TCP messages with the same source layer 4 port and destination layer 4 port.
mac	Enable detection of messages with the same source MAC and destination MAC
smac	Enables detection of multicast and broadcast messages
pingflood	Enable detection of pingflood type messages
synflood	Enable defense against SYN flood attacks
tcpflags	Enable detection of TCP messages with illegal flags
tcpsmurf	Enable detection of TCP messages with tcmsmurf type
icmpsmurf	Enable detection of icmp messages with icmpsmurf type
ipsmurf	Enable detection of ipsmurf messages with ipsmurf type
nullscan	Enable detection of TCP messages with TCP flag set to 0

Default Value

DoS attack prevention is disabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

DoS attack prevention is configured in global mode.

The DoS ICMP sub-function can drop ICMP messages.

The DoS IP sub-function can drop those IP messages with the same source IP and destination IP

The DoS l4port sub-function can drop the TCP messages with the same source layer 4 port and destination layer 4 port.

The DoS MAC sub-function can drop messages with the same source MAC and destination MAC.

The DoS smac sub-function can drop multicast and broadcast messages.

The DoS pingflood sub-function can drop ICMP messages.

The DoS synflood sub-function can drop the messages with tcp SYN=1.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP messages: 1.TCP SYN flag = 1 & source port<1024; 2.TCP control flags = 0 & sequence = 0; 3.TCP FIN URG PSH =1 & sequence = 0; 4.TCP FIN SYN =1.

The DoS tcpsmurf sub-function can drop the TCP messages whose last 8 bits of the destination IP address are 255.

The DoS icmpsmurf sub-function can drop the ICMP messages whose last 8 bits of the source IP and destination IP addresses are both 255.

The DoS ipsmurf sub-function can drop the IP messages whose last 8 bits of the destination IP address are 255.

The DoS nullscan sub-function can drop the TCP messages with the tcp flag set to 0.

Example

The following example shows how to set DoS attack prevention in global mode to defense against those TCP messages whose last 8 bits of the destination IP address are 255.

```
Switch(config)#dos enable tcpsmurf
```

Chapter 10 CPU Enhanced Protection Configuration Commands

10.1 CPU Rate Limit and Packet Rate Limit Configuration

CPU protection can be implemented by limiting the rate of different types of packets globally.

10.1.1 cpu threshold value

Syntax

cpu threshold *value*

no cpu threshold

Parameter Description

Parameter	Parameter Description
value	Rate limit

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to set a rate limit on CPU global in the global configuration mode.

Example

```
Switch(config)#
Switch(config)#cpu threshold ?
<1-4147>     -- Config PIR (Peak Information Rate)(unit pps)
packet-type   -- packet-type
Switch(config)#cpu threshold 2000 Switch(config)#no cpu threshold
```

10.1.2 cpu threshold packet-type all

Syntax

[**no**] **cpu threshold packet-type all**

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

In global configuration mode, the command is used to configure all packets to be the default value or cancel the rate limit.

Example

```
Switch(config)#cpu threshold packet-type all
Switch(config)#no cpu threshold packet-type all
```

10.1.3 cpu threshold packet-type packet-type

Syntax

cpu threshold packet-type *packet-type* [**cir** *cir-value* **cbs** *cbs-value*] **no cpu threshold packet-type packet-type**

Parameter Description

Parameter	Parameter Description
packet-type	rate-limit packet type
cir-value	limit rate
cbs-value	burst Rate Limit value

Default Value

None

Command Mode

Global Configuration Mode。

Usage Guidelines

In global configuration mode, configure the default or custom CIR and CBS configurations for packets. The following types of rate-limited packets are used:

Type	Type Description
arp	Arp message
igmp	igmp message
ipv4-ttl-failure	ipv4-ttl-failure message
ipuc	ipuc message
resv-mac	resv-mac message
bcast	broadcast message
acl-copy	acl-copy message
acl-redirect	acl-redirect message

Example

```
Switch(config)#cpu threshold packet-type arp
Switch(config)#cpu threshold packet-type arp cir 200 cbs 300 Switch(config)#no cpu threshold packet-type arp
```

10.2 Check Rate Limit Configuration and Packet Statistics

The commands enable you to view the configuration information related to the rate limit, so that you can intuitively collect statistics and manage the CPU rate limit configuration and the rate limit configuration of each packet.

10.2.1 show cpu-threshold configuration

Syntax

show cpu-threshold configuration

Parameter Description

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command is used to check the configuration information of CPU enhanced protection rate limit.

Example

```
Switch(config)#show cpu-threshold configuration cpu threshold global configuration: 2500

  Packet type       Status          Cir(pps)              Cbs(packet)
  arp               enable          256                           384
  igmp              enable          256                           384
  ipv4-ttl-         enable          128                           192
  failure
  ipuc              enable          512                           768
  resv-mac          enable          256                           384
  bcast             enable          512                           768
  acl-copy          enable          256                           384
  acl-redirect      enable          256                           384
```

10.2.2 show cpu-threshold statistics

Syntax

show cpu-threshold statistics [**packet-type** *packet-type*]

Parameter Description

Parameter	Parameter Description
packet-type	*Packet type*

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command is used to check statistics on CPU packets.

Example

```
Switch(config)#show cpu-threshold statistics
   cpu            threshold
   statistics:
   Packet type               Pass(Packet)       Drop(Packet)
   all                       82832                         0
   stack                     0                             0
   arp                       17277                         0
   igmp                      36                            0
   ipv4-ttl-failure          0                             0
   ipuc                      16968                         0
   resv-mac                  43500                         0
   bcast                     4442                          0
   acl-copy                  0                             0
   acl-redirect              609                           0
```

10.2.3 show cpu-threshold rate

Syntax

show cpu-threshold rate [**packet-type** *packet-type*]

Parameter Description

Parameter	Parameter Description
packet-type	Packet type

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command is used to check the rate of CPU packets.

Example

```
Switch(config)#show cpu-threshold rate cpu threshold packet rate:
 Packet type           Pass(Packet/s)        Drop(Packet/s)
 all                   2                                   0
 stack                 0                                   0
 arp                   1                                   0
 igmp                  0                                   0
 ipv4-ttl-failure      0                                   0
 ipuc                  0                                   0
 resv-mac              1                                   0
 bcast                 0                                   0
 acl-copy              0                                   0
 acl-redirect          0                                   0
```

Chapter 11 Fast Ethernet Ring Protection Configuration Commands

11.1 Global Configuration Commands

11.1.1 ether-ring

Syntax

To set an instance of ring and enter the node mode, run the following command:

ether-ring id

To cancel an instance of ring, run the following command:

no ether-ring id

Parameter Description

Parameter	Parameter Description
id	ID of the node, ranges from 0 to 7.

Default Value

By default, the ring node is not configured.

Command Mode

Global configuration mode

Usage Guidelines

STP should not be disabled before the configuration of node instance.

Example

```
S1(config)#ether
-ring           1
S1(config_ring1)
#
```

Related Command

None

11.1.2 control-vlan

Syntax

To set the control VLAN of the ring node, run the following command:

control-vlan *vlan-id*

Parameter Description

Parameter	Parameter Description
vlan-id	ID of the control VLAN Value range: 1-4094

Default Value

By default, the control VLAN of a node is not configured.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. Any VLAN can be configured as the control VLAN of the node. If you specify the control VLAN, the system VLAN will be created consequently. The user doesn't need to create the system VLAN manually.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the Ethernet ring has already been started.

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#control-vlan 2
```

Related Command

ether-ring

master-node transit-node

11.1.3 master-node

Syntax

To configure an Ethernet ring as a master node, run the following command:

master-node

Parameter Description

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can only be configured as either a master-node or a transit-node.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already started.

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#control-
vlan                    2
S1(config_ring1)#master-
node
```

Related Command

control-vlan transit-node

11.1.4 transit-node

Syntax

To configure the node type to be a transit node, run the following command.

transit-node

Parameter Description

None

Default Value

By default, the node type is not configured.

Command Mode

Node configuration mode

Usage Guidelines

1. A node can only be configured as either a master-node or a transit-node.
2. After the control VLAN and node types of the Ethernet ring are configured, you cannot modify the control VLAN even if the system exits from the Ethernet ring configuration mode because the node of the Ethernet ring has already started.

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#control
-vlan                   2
S1(config_ring1)#transit
-node
```

Related Command

control-vlan ***master-node***

11.1.5 hello-time

Syntax

To configure the cycle for the master node to transmit the HEALTH packets of the Ethernet ring, run the following command:

hello-time *value*

To return to the default value of the cycle, run the following command:

no hello-time

Parameter Description

Parameter	Parameter Description
value	Stands for a time value, whose unit is second. The default value is one second. The value ranges between 1 and 10 seconds.

Default Value

By default, the hello-time is one second.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The hello-time configuration validates only on the master node.
2. By default, the value of the hello-time is smaller than that of the fail-time, which prevents the Ethernet ring protocol from being shocked. The fail-time needs to be modified after modifying hello-time.

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#control
-vlan                    2
S1(config_ring1)#master-
node
S1(config_ring1)#hello-time 2
```

Related Command

fail-time

11.1.6 fail-time

Syntax

To configure the time cap of waiting for the HEALTH packets for the secondary port of the master node, run the following command:

fail-time *value*

To return to the default value of the fail-time, run the following command:

no fail-time

Parameter Description

Parameter	Parameter Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default Value

By default, the fail-time is 3 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The fail-time configuration validates only on the master node.
2. By default, the value of the fail-time is triple of the hello-time, which avoids the Ethernet ring protocol from being shocked. The fail-time needs to be modified after modifying hello-time.

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#control
-vlan                   2
S1(config_ring1)#master-
node
S1(config_ring1)#hello
-time                 2
S1(config_ring1)#fail-
time 6
```

Related Command

hello-time

11.1.7 pre-forward-time

Syntax

To configure the time of maintaining the pre-forward state on the transit port, run the following command.

pre-forward-time *value*

To return to the default value of the pre-forward-time, run the following command.

no pre-forward-time

Parameter Description

Parameter	Parameter Description
value	Stands for a time value, whose unit is second. The default value is three seconds. The value ranges between 3 and 30 seconds.

Default Value

By default, the pre-forward-time is 3 seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

1. The pre-forward-time configuration validates only on the transit node.
2. By default, the pre-forward-time on the transit node is triple the value of the hello-time on the master node, which avoids the network loop from occurring after the transmission link recovers from disconnection. After the hello-time of the master node is modified, the corresponding pre-forward-time on the transit node needs to be adjusted.

Example

```
S1(config)#ether-ring 1

S1(config_ring1)#control-vlan     2
S1(config_ring1)#transit-node

S1(config_ring1)#pre-forward-time 8
```

Related Command

None

11.1.8 compatible-mode

Syntax

The configuration control message format is RFC3619.

compatible-mode

To restore the control message format to a private format, run the following command.

no compatible-mode

Parameter Description

None

Default Value

By default, the message format is private format.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#compatible-mode
```

Related Command

None

11.1.9 fast-aging

Syntax

To enable fast aging, run the following command, run the following command.

fast-aging

To disable fast aging, run the following command, run the following command.

no fast-aging

Parameter Description

None

Default Value

By default, fast aging is enabled.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#fast-aging
```

Related Command

None

11.1.10 fdb-flush

Syntax

To enable the fdb aging, run the following command, run the following command.

fdb-flush

To disable the fdb aging, run the following command, run the following command.

no fdb-flush

Parameter Description

None

Default Value

By default, fdb aging is enabled.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#fdb-flush
```

Related Command

None

11.1.11 ring-description

Syntax

To enable the ring description, run the following command.

ring-description *WORD*

To disable the ring description, run the following command.

no ring-description

Parameter Description

Parameter	Parameter Description
WORD	The string size does not exceed 128 bytes.

Default Value

None

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#ring-description ringA
```

Related Command

None

11.1.12 warning-log-flag

Syntax

To enable the warning print, run the following command.

warning-log-flag

To disable the warning print, run the following command.

no warning-log-flag

Parameter Description

None

Default Value

By default, the warning print is disabled.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
S1(config)#ether-ring 1
S1(config_ring1)#warning-log-flag
```

Related Command

None

11.2 Port Configuration Commands

11.2.1 primary-port

Syntax

To set a port to be the primary port of a master node, run the following command:

ether-ring *id* **primary-port**

To cancel the primary port configuration of a port, run the following command:

no ether-ring *id* **primary-port**

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

The primary port is not configured by default.

Command Mode

Physical Port Configuration Mode and Aggregate Port Configuration Mode.

Note: Switch software versions prior to 2.0.1L and high-end switch versions prior to 4.0.0M do not support the configuration of aggregated ports.

Usage Guidelines

The primary port can be configured only after the ring control VLAN and node type are fully configured, and the node type must be a primary node.

Example

```
S1(config)#interface tg0/0/1
S1(config-tg0/0/1)#ether-ring        1
primary-port S1(config-tg0/0/1)#exit
```

Related Command

master-node

ether-ring secondary-port

11.2.2 secondary-port

Syntax

To configure the port as the secondary port of the primary node.

ether-ring id secondary-port

To cancel the secondary port configuration of a port.

no ether-ring id secondary-port

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

By default, the secondary port of the master node is not configured.

Command Mode

Physical Port Configuration Mode and Aggregate Port Configuration Mode.

Note: Switch software versions prior to 2.0.1L and high-end switch versions prior to 4.0.0M do not support the configuration of aggregated ports.

Usage Guidelines

The secondary port can be configured only after the ring control VLAN and node type are fully configured, and the node type must be a secondary node.

Example

```
S1(config)#interface tg0/0/3
S1(config-tg0/0/3)#ether-ring          1
secondary-port S1(config-tg0/0/3)#exit
```

Related Command

master-node

ether-ring primary-port

11.2.3 transit-port

Syntax

To set a port to be the transit port of a transit node, run the following command:

ether-ring *id* **transit-port**

To cancel the transit port, run the following command:

no ether-ring *id* **transit-port**

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

The transit port on the transit node is not configured by default.

Command Mode

Physical Port Configuration Mode and Aggregate Port Configuration Mode.

Note: Switch software versions prior to 2.0.1L and high-end switch versions prior to 4.0.0M do not support the configuration of aggregated ports.

Usage Guidelines

The transit port can be configured only after the ring control VLAN and node type are fully configured, and the node type must be a transit node. Each transit node can be configured with two transit ports.

Example

```
S1(config_ring1)#exit
S1(config)#interface tg0/0/1
S1(config-tg0/0/1)#ether-ring        1
transit-port S1(config-tg0/0/1)#exit
S1(config)#interface tg0/0/3
S1(config-tg0/0/3)#ether-ring        1
transit-port S1(config-tg0/0/3)#exit
```

Related Command

transit-node

11.3 Show Commands

11.3.1 show ether-ring

Syntax

To display the summary information about the Ethernet-ring node, run the following command:

show ether-ring *id*

To display detailed information about the Ethernet-ring node, run the following command:

show ether-ring *id* **detail**

To display the information about the Ethernet-ring port, run the following command:

show ether-ring *id* **interface** *intf-name*

To display all summary information about the Ethernet-ring node, run the following command:

show ether-ring <cr>

Parameter Description

Parameter	Parameter Description
id	ID of the node
intf-name	Name of an interface

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Node configuration mode or Port Configuration Mode.

Usage Guidelines

None

Example

None

Related Command

None

Chapter 12 Interface Configuration Commands

12.1 Interface Configuration Commands

12.1.1 interface

Syntax

[**no**] **interface** *port*

To enter the interface configuration mode, run the command. For a logical port, if the port does not exist, create the port first and enter the port mode. For a non-existent physical port, the command fails to execute.

no interface *logical-port*

To delete the logic interface, run this command.

Parameter Description

Parameter	Parameter Description
port	Stands for the existent physical or logical port.

Default Value

The default mode is not the port configuration mode.

Usage Guidelines

When you execute this command in configuration mode, you have to enable this command to the port configuration mode first. When the port command is configured, you can use the exit command to exit the port mode.

Example

The following example shows how to enter the port mode of tg0/0/1.

```
Switch(config)#
Switch(config)#interface
tg0/0/1     Switch(config-
tg0/0/1)#exit
Switch(config)#
```

12.1.2 interface range

Syntax

interface range *port-range*

To enter interface range configuration mode, which is used for batch operations of port configuration, run the command.

Parameter Description

Parameter	Parameter Description
port-range	Port name range separated by "-", "," such as tg0/0/1-2,4

Default Value

None

Usage Guidelines

When executing this command in configuration mode, if you need to configure port commands in batches, you need to first use this command to enter port range configuration mode. When you have completed configuring port commands, use the exit command to exit port range configuration mode.

Example

To enter the port range configuration mode of tg0/0/1, tg0/0/2, and tg0/0/4:

```
Switch(config)#interface range tg0/0/1-2,4
Switch(config-tg0/0/1-2,4)#
Switch(config-tg0/0/1-
2,4)#exit Switch(config)#
```

12.1.3 description

Syntax

[no] description *line*

To set the description information of a port, run the command.

Parameter Description

Parameter	Parameter Description
line	Stands for the description string

Default Value

There is no description information by default.

Usage Guidelines

This command is configured in port configuration mode.

Example

The following example shows how to set the description information of port `tg0/0/1` to up link.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#description uplink
```

12.1.4 shutdown

Syntax

[no] shutdown

To enable and disable the port, run the command.

Parameter Description

None

Default Value

The physical port is enabled by default.

Usage Guidelines

This command can be used (in the PON port or the uplink port) to enable or disable port.

Example

The following example shows how to enable port tg0/0/1.

```
Switch(config)#interface
tg0/0/1       Switch(config-
tg0/0/1)#no         shutdown
Switch(config-tg0/0/1)#
```

12.1.5 show interface

Syntax

show interface *port*

To browse the state of an interface, run the command.

Parameter Description

Parameter	Parameter Description
port	Name of an interface. If no specific interface is specified in the command, the status of all interfaces in the system will be displayed.

Default Value

None

Usage Guidelines

This command can be used in EXEC and configuration modes to show the physical status and packet reception statistics of a port.

Example

The following example shows the port information of tg0/0/1:

```
Switch(config)#show interface tg0/0/1  tg0/0/1 is down, line protocol is down Ifindex is 3
Hardware is Giga-TX, address is 8479.7335.06c1 (bia 8479.7335.06c1)
Encapsulation ARPA
Auto-duplex, Auto-speed, Flow-Control Off

5 minutes input rate 0 bits/sec, 0 packets/sec

5 minutes output rate 0 bits/sec, 0 packets/sec

Real time input rate 0%, 0 bits/sec, 0 packets/sec  Real
time output rate 0%, 0 bits/sec, 0 packets/sec Received 0
packets, 0 bytes
```

0 broadcasts, 0 ucasts 0 multicasts

0 FCS, 0 PAUSE 0 jabber, 0 jumbo

0 undersize, 0 collision 0 error

0 overrun, 0 oversize

0 63B packets, 0 64B packets

0 65B\~127B packets, 0 128B\~255B packets 0 256B\~511B packets, 0 512B\~1023B packets 0 good 1519B packets, 0 bad 1519B packets Transmitted 0 packets, 0 bytes

0 broadcasts, 0 ucasts 0 multicasts

0 FCS, 0 jumbo 0 underrun

0 63B packets, 0 64B packets

0 65B\~127B packets, 0 128B\~255B packets 0 256B\~511B packets, 0 512B\~1023B packets 0 good 1519B packets, 0 pause

12.1.6 show running-config interface

Syntax

show running-config interface

port

To display the port configuration, run the command.

Parameter Description

Parameter	Parameter Description
Port	Stands for the existing port

Default Value

None

Usage Guidelines

This command can be executed in EXEC or configuration mode to browse the configuration of a port.

Example

The following example shows the configuration information of port tg0/0/1:

```
Switch(config)#show  running-config  interface  tg0/0/1
Building configuration...
Current configuration: !
interface tg0/0/1


shutdown


description     uplink
Switch(config)#
```

12.2 Configuration Example

The following example shows how to create a VLAN port, configure its description and IP address. Use the show command to browse the port status and configuration.

```
Switch(config)#interface vlan1
Switch(config-vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(config-vlan1)#exit
Switch(config)#
Switch(config)#interface vlan1
Switch(config-vlan1)#description uplink
Switch(config-vlan1)#
Switch(config-vlan1)#ip address 192.168.1.1 255.255.255.0
Switch(config-vlan1)#exit
Switch(config)#
Switch(config)#show running-config interface vlan1
Building configuration...
Current configuration: !
interface vlan1
description uplink
ip address 192.168.1.1 255.255.255.0
Switch(config)#
Switch(config)#show interface vlan1 vlan1
is up, line protocol is up
Ifindex is 449
Encapsulation ARPA
Peak input rate 0 pps, output 0 pps
5987 packets input, 363924 bytes
Received 5987 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls input discards
0 input errors, 0 discards, 0 protocol unknown
0 packets output, 0 bytes
Transmited 0 broadcasts, 0 multicasts
0 mpls unicasts, 0 mpls multicasts, 0 mpls output discards
0 output errors, 0 discards
Switch(config)#
```

Chapter 13 Configuring IP Access List Command

13.1 IP Access List Configuration Commands

13.1.1 ip access-list

Syntax

After using this command, you will enter the IP access list configuration mode. In this state, you can add and delete access rules. Use the exit command to return to the global configuration mode.

Use the no command to delete the IP access list.

ip access-list {**standard | extended**} *name*

no ip access-list {**standard | extended**} *name*

Parameter Description

Parameter	Parameter Description
standard	Specifies a standard access list.
extended	Specifies an extended access list.
name	Access list name. This is a string of up to 20 characters.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to enter the IP access list configuration mode. In the IP access list configuration mode, you can use the deny or permit command to configure access rules.

Example

The following example shows how to configure a standard access list.

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#deny           192.168.1.0
255.255.255.0 Switch(config-filter)#permit any
```

Related commands

- deny
- permit
- ip access-group
- ip access_group
- show ip access-list

13.1.2 permit

Syntax

The command is used to configure an allow rule in the IP access list configuration mode, and to remove the permit rule from the IP access list, prefixing the no prefix before the command.

Standard IP access list:

permit {*source* [*source-mask*] | **any**}

no permit {*source* [*source-mask*] | **any**}

Expand IP access list:

permit *protocol* {*source-address source-mask* | **interface** *source-vlan-name* | **any**} [**eq**

src_port_number | **lt** *src_port_number* | **gt** *src_port_number* | **neq** *src_port_number* | **src-portrange** *src_port_number_begin src_port_number_end*] {*destination destination-mask* | **interface** *destination-*

vlan-name | **any**} [**eq** *dst_port_number* | **lt** *dst_port_number* | **gt** *dst_port_number* | **neq**

dst_port_number | **dst-portrange***dst_port_number_begin dst_port_number_end*] [*icmp-type*] [**tcp- flags** *tcp-flags*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**cos** *cos*] [**donotfragment-set** |

donotfragment-notset] [**is-fragment** | **not-fragment**] [**offset-zero** | **offset-not-zero**] [**ttl** *ttl*] [**totallen** *totallen*]

no permit *protocol* {*source-address source-mask* | **interface** *source-vlan-name* | **any**} [**eq**

src_port_number | **lt** *src_port_number* | **gt** *src_port_number* | **neq** *src_port_number* | **src-portrange** *src_port_number_begin src_port_number_end*] {*destination destination-mask* | **interface** *destination-*

vlan-name | **any**} [**eq** *dst_port_number* | **lt** *dst_port_number* | **gt** *dst_port_number* | **neq**

dst_port_number | **dst-portrange***dst_port_number_begin dst_port_number_end*] [*icmp-type*] [**tcp- flags** *tcp-flags*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**cos** *cos*] [**donotfragment-set** |

donotfragment-notset] [**is-fragment** | **not-fragment**] [**offset-zero** | **offset-not-zero**] [**ttl** *ttl*] [**totallen** *totallen*]

Parameter Description

Parameter	Parameter Description
protocol	Protocol name or IP protocol number. It can be a keyword gre, ip, ospf, icmp, igmp, sctp, tcp, or udp, and it can also be an integer from 0 to 255 of the table IP protocol number. To match any Internet protocol, the keyword ip is used.
extended	Specifies it as an extended access list.

source	Source address
source-mask	Source address network mask.
interface	Uses the IP address in the VLAN as the source or destination address for matching.
source-vlan-name	Uses the Source address vlan value.
any	Uses the keyword any as the source address for 0.0.0.0 and the source mask abbreviation for 0.0.0.0.
eq	(Optional) If the protocol is set to tcp/udp/sctp, select to follow the source address to indicate that the source address port number is equal to *src_port_number*, and the destination address port number is equal to *dst_port_number*.
lt	(Optional) If the protocol is tcp/udp, select to follow the source address to indicate that the source address port number is less than *src_port_number*, and the destination address port number is less than *dst_port_number*.
gt	(Optional) If the protocol is TCP/UDP, select to follow the source address to indicate that the source address port number is greater than *src_port_number*, and to follow the destination address to indicate that the destination port number is greater than *dst_port_number*.
neq	(Optional) If the protocol is tcp/udp, select to follow the source address to indicate that the source address port number is not equal to *src_port_number*, and to follow the destination address to indicate that the destination address port number is not equal to *dst_port_number*.
src-portrange	(Optional) If the protocol is tcp/udp, the source address port number is greater than *src_port_number_begin* and less than *src_port_number_end*.
src_port_number	It is used to match the source address port number, which is 0 ~ 65535 after **eq** and **neq**, 1 ~ 65535 after **lt**, and 0 ~ 65534 after **gt**.
src_port_number_begin	It is used to match the starting digit of the Source address port number range, which is 0 ~ 65535.
src_port_number_end	It is used to match the end digit of the Source address port number range, which is 0 ~ 65535.
destination	Destination address.

destination-mask	Destination address network mask.
destination-vlan-name	The destination address vlan value. The VLAN value of the destination address used.
dst-portrange	(Optional)
dst_port_number	It is used to match the destination address port number, which is followed by **eq** and **neq** in the range of 0 ~ 65535, followed by **lt** in the range of 1 ~ 65535, and followed by **gt** in the range of 0 ~ 65534.
dst_port_number_begin	It is used to match the starting digit of the destination address port number range, which is 0 ~ 65535.
dst_port_number_end	It is used to match the end digit of the destination address port number range, which is 0 ~ 65535.
icmp-type	(Optional) ICMP packets can be filtered by ICMP packet type and are displayed only if the protocol is ICMP. The type is a number from 0 to 255.
tcp-flags	(Optional) TCP packets can be filtered by the tcp-flags type and will only be displayed if the protocol is TCP.
tcp-flags	The type is a number from 0 to 4095.
established	(Optional) TCP packets can be filtered to the established type and will only be displayed if the protocol is TCP.
precedence	(Optional) Packets can be filtered using the service layer.
precedence	It can be specified using a number from 0 to 7.
tos	(Optional) Packets can be filtered using the service layer.
tos	It can be specified using a number from 0 to 15.
cos	(Optional) Specifies the priority of the packet.
cos	It can be specified using a number from 0 to 7.
donotfragment-set	(Optional) The non-fragment tag is set.
donotfragment-	(Optional) The non-fragment tag is not set.
is-fragment	(Optional) The fragment packet.
not-fragment	(Optional) The non-fragment packet
offset-zero	(Optional) The offset-zero packet.

offset-not-zero	(Optional) The offset-not-zero packet.
ttl	(Optional) Meets the specified survival time.
ttl	The lifetime of the packet.
totallen	(Optional) Meets the specified length of the IP packet.
totallen	IP packet length.

Command Mode

IP access list editing mode

Usage Guidelines

The command allows you to use access tables to control the transmission of packages on interfaces, control virtual terminal line access, and restrict the content of routing updates. Stop checking the extended access table after a match has occurred.

The fragmented IP packet, rather than the initial segment, is immediately received by any extended IP access table. Extended access tables are used to control access to virtual terminal lines or restrict routing updates, regardless of the TCP source port, the type of service value, or the priority of the packet.

Note: After the initial establishment of the access table, any subsequent additions (possibly typed by the terminal) are placed at the end of the list.

Example

The following example enables the network segment 192.168.5.0.

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#permit 192.168.5.0 255.255.255.0
```

Note: The IP access list ends with a ***deny any*** / ***deny ip any any*** rule.

Related commands

- ip access-list
- deny
- ip access-group
- ip access_group
- show ip access-list

13.1.3 deny

Syntax

The command is used to configure an allow rule in the IP access list configuration mode, and to remove the permit rule from the IP access list, prefixing the no prefix before the command.

Standard IP access list:

deny {*source* [*source-mask*] | **any**}

no deny {*source* [*source-mask*] | **any**}

Extended IP access list:

deny *protocol* {*source-address source-mask* | **interface** *source-vlan-name* | **any**} [**eq** *src_port_number* | **lt** *src_port_number* | **gt** *src_port_number* | **neq** *src_port_number* | **src-portrange**

src_port_number_begin src_port_number_end] {*destination destination-mask* | **interface** *destination- vlan-name* | **any**} [**eq** *dst_port_number* | **lt** *dst_port_number* | **gt** *dst_port_number* | **neq**

dst_port_number | **dst-portrange***dst_port_number_begin dst_port_number_end*] [*icmp-type*] [**tcp-**

flags *tcp-flags*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**cos** *cos*] [**donotfragment-set** |

donotfragment-notset] [**is-fragment** | **not-fragment**] [**offset-zero** | **offset-not-zero**] [**ttl** *ttl*] [**totallen** *totallen*]

no deny *protocol* {*source-address source-mask* | **interface** *source-vlan-name* | **any**} [**eq**

src_port_number | **lt** *src_port_number* | **gt** *src_port_number* | **neq** *src_port_number* | **src-portrange** *src_port_number_begin src_port_number_end*] {*destination destination-mask* | **interface** *destination-*

vlan-name | **any**} [**eq** *dst_port_number* | **lt** *dst_port_number* | **gt** *dst_port_number* | **neq**

dst_port_number | **dst-portrange***dst_port_number_begin dst_port_number_end*] [*icmp-type*] [**tcp- flags** *tcp-flags*] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**cos** *cos*] [**donotfragment-set** |

donotfragment-notset] [**is-fragment** | **not-fragment**] [**offset-zero** | **offset-not-zero**] [**ttl** *ttl*] [**totallen** *totallen*]

Parameter Description

Parameter	Parameter Description
protocol	Protocol name or IP protocol number. It can be a keyword gre, ip, ospf, icmp, igmp, sctp, tcp, or udp, and it can also be an integer from 0 to 255 of the table IP protocol number. To match any Internet protocol, the keyword ip is used.
extended	Specify it as an extended access list.

source	Source address.
source-mask	Source address network mask.
interface	Use the IP address in the VLAN as the source or destination address for matching.
source-vlan-name	Use the Source address vlan value.
any	Use the keyword any as the source address for 0.0.0.0 and the source mask abbreviation for 0.0.0.0.
eq	(Optional) If the protocol is set to tcp/udp/sctp, select to follow the source address to indicate that the source address port number is equal to *src_port_number*, and the destination address port number is equal to *dst_port_number*.
lt	(Optional) If the protocol is tcp/udp, select to follow the source address to indicate that the source address port number is less than *src_port_number*, and the destination address port number is less than *dst_port_number*.
gt	(Optional) If the protocol is TCP/UDP, select to follow the source address to indicate that the source address port number is greater than *src_port_number*, and to follow the destination address to indicate that the destination port number is greater than *dst_port_number*.
neq	(Optional) If the protocol is tcp/udp, select to follow the source address to indicate that the source address port number is not equal to *src_port_number*, and to follow the destination address to indicate that the destination address port number is not equal to *dst_port_number*.
src-portrange	(Optional) If the protocol is tcp/udp, the source address port number is greater than *src_port_number_begin* and less than *src_port_number_end*.
src_port_number	It is used to match the source address port number, which is 0 ~ 65535 after **eq** and **neq**, 1 ~ 65535 after **lt**, and 0 ~ 65534 after **gt**.
src_port_number_begin	It is used to match the starting digit of the Source address port number range, which is 0 ~ 65535.
src_port_number_end	It is used to match the end digit of the Source address port number range, which is 0 ~ 65535.
destination	Source address.

destination-mask	Destination address network mask.
destination-vlan-name	The destination address vlan value.
dst-portrange	(Optional)
dst_port_number	It is used to match the destination address port number, which is followed by **eq** and **neq** in the range of 0 ~ 65535, followed by **lt** in the range of 1 ~ 65535, and followed by **gt** in the range of 0 ~ 65534.
dst_port_number_begin	It is used to match the starting digit of the destination address port number range, which is 0 ~ 65535.
dst_port_number_end	It is used to match the end digit of the destination address port number range, which is 0 ~ 65535.
icmp-type	(Optional) ICMP packets can be filtered by ICMP packet type and are displayed only if the protocol is ICMP. The type is a number from 0 to 255.
tcp-flags	(Optional) TCP packets can be filtered by the tcp-flags type and will only be displayed if the protocol is TCP.
tcp-flags	The type is a number from 0 to 4095.
established	(Optional) TCP packets can be filtered to the established type, and will only be displayed if the protocol is TCP.
precedence	(Optional) Packets can be filtered using the service layer.
precedence	It can be specified using a number from 0 to 7.
tos	(Optional) Packets can be filtered using the service layer.
tos	It can be specified using a number from 0 to 15.
cos	(Optional) Specifies the priority of the packet.
cos	It can be specified using a number from 0 to 7.
donotfragment-set	(Optional) The non-fragment tag is set.
donotfragment-notset	(Optional) The non-fragment tag is not set.
is-fragment	(Optional) The fragment packet.

not-fragment	(Optional) The non-fragment packet.
offset-zero	(Optional) The offset-zero packet.
offset-not-zero	(Optional) The offset-not-zero packet.
ttl	(Optional) Meets the specified survival time
ttl	The lifetime of the packet.
totallen	(Optional) Meets the specified length of the IP packet.
totallen	IP packet length.

Command Mode

IP access list editing mode

Usage Guidelines

The command allows you to use access tables to control the transmission of packages on interfaces, control virtual terminal line access, and restrict the content of routing updates. Stop checking the extended access table after a match has occurred.

The fragmented IP packet, rather than the initial segment, is immediately received by any extended IP access table. Extended access tables are used to control access to virtual terminal lines or restrict routing updates, regardless of the TCP source port, the type of service value, or the priority of the packet.

Note: After the initial establishment of the access table, any subsequent additions (possibly typed by the terminal) are placed at the end of the list.

Example

The following example disables the network segment 192.168.5.0.

```
Switch(config)#ip access-list standard filter
Switch(config-filter)#deny 192.168.5.0 255.255.255.0
```

Note: The IP access list ends with a ***deny any*** / ***deny ip any any*** rule.

Related commands

- ip access-list
- permit
- ip access-group
- ip access_group
- show ip access-list

13.1.4 ip access_group

Syntax

To configure access list rules for an interface, use the ip access_group interface configuration command. To delete this specified access list, use the no form of this command.

ip access_group {*access-list-name*} {**input** | **output**}

no ip access_group {*access-list-name*} {**input** | **output**}

Parameter Description

Parameter	Parameter Description
access-list-name	Access the table name. This is a string with a maximum of 20.
input	Use the access list when entering the interface.
output	Use access lists when exiting interfaces.

Command Mode

vlan interface configuration mode

Usage Guidelines

The access list is used in the interface of the ingress. For standard access lists, check the source address of the package against the access list after receiving the package. For the extended access list, the switch also checks the destination address. If the address is allowed in the access table, then the software continues to process the package. If the access table does not allow the address, the software discards the package.

If the specified access list does not exist, all packages are allowed to pass through.

Note: The IP access list ends with a ***deny any*** / ***deny ip any any*** rule.

Example

The following example shows how to apply the list filter on the output of interface vlan 2.

```
Switch(config)#interface vlan2
Switch(config-vlan2)#ip access_group filter output
```

13.1.5 show ip access-list

Syntax

To display the contents of all current IP access lists, use the show ip access-list command

show ip access-list [*access-list-name*]

Parameter Description

Parameter	Parameter Description
access-list-name	(Optional) Name of the IP access list. It is a string of up to 20 characters.

Default Value

All standard and extended IP access lists are displayed.

Command Mode

EXEC/Global Configuration Mode (Port Configuration Mode)

Usage Guidelines

The show ip access-list command allows you to display a specific access list or to all access lists.

Example

The following is an example output of the show ip access-list command when the access list is not specified:

```
Switch#show ip access-list
Standard IP access list test1
Index          Rule content
  ----------------------------------------------------------------
1          permit 10.1.1.2 255.255.255.255
2          deny   any
Extended IP access list test2 Index
Rule content
  ----------------------------------------------------------------
```

```
1          deny   ip interface VLAN4 any

2          deny   icmp interface VLAN4 any

3          permit icmp interface VLAN4 any
```

The following is an example output of the show ip access-list command when the access list is specified:

```
Switch#show   ip   access-list   test1
Standard IP access list test1

Index          Rule content

----------------------------------------------------------------------

1          permit 10.1.1.2 255.255.255.255

2          deny   any
```

Chapter 14 Configuring Port Aggregation Commands

14.1 Configuring Port Aggregation Commands

14.1.1 aggregator-group

Syntax

aggregator-group *id* **mode** {lacp|static} **no aggregator-group**

To configure port aggregation, use the **aggregator-group** command. To resume the default settings, run no aggregator-group command.

Parameter Description

Parameter	Parameter Description
id	The ID of a logistic port. Value range: 1-8
lacp	Enables LACP negotiation.
static	Disables port negotiation.

Default Value

The port is not aggregated.

Usage Guidelines

Port link aggregation is to bundle several ports with the same attributes into one logical port. This bundling process can be negotiated through LACP or can be forcibly bundled together without negotiation.

If you implement static aggregation, aggregation can be performed as long as the ports are linked up and the VLAN attributes are consistent.

When configuring port aggregation, you can select the LACP negotiation mode. In Active mode, the port will transmit the LACP massages actively for LACP negotiation; in passive mode, the port responds to the LACP massages passively and conducts the LACP negotiation passively.

Some device models do not support dynamic negotiation mode and therefore do not provide corresponding configuration commands.

Command Mode

Interface Configuration Mode

Example

The following example shows how to bundle port `tg0/0/1` and `tg0/0/2` to logic port port-aggregator 3, and use LACP negotiation.

```
Switch(config)# interface tg0/0/1
Switch(config-tg0/0/1)# aggregator-group 3 mode lacp Switch(config-tg0/0/1)# interface tg0/0/2
Switch(config-tg0/0/2)# aggregator-group 3 mode lacp
```

14.1.2 aggregator-group load-balance

Syntax

aggregator-group load-balance {dst-mac|src-mac|both-mac|dst-ip|src-ip|both-ip|l4-sport|l4- dport|both-l4port}

no aggregator-group load-balance

To configure load balance after port aggregation, run aggregator-group load-balance command. To resume the default settings, run no aggregator-group load-balance command.

Parameter Description

Parameter	Parameter Description
dst-mac	Stands for taking the destination MAC address as the standard.
src-mac	Stands for taking the source MAC address as the standard.
both-mac	Stands for taking the destination and source MAC address as the standard.
dst-ip	Stands for taking the destination IP address as the standard.
src-ip	Stands for taking the source IP address as the standard.
both-ip	Stands for taking the source and destination IP address as the standard.
l4-sport	Stands for taking the Source port +ip as the standard.
l4-dport	Stands for taking the destination port +ip as the standard.
both-l4port	Stands for taking the Source and destination port +ip as the standard.

Default Value

scr-mac

Usage Guidelines

To ensure each physical port to reach load balance after port aggregation, you need to distribute data flow on each physical port. This configuration can be used to achieve this.

When the dst-mac mode is chosen, the distributed data flow takes the destination MAC address of the data message as the standard. And the same mac address is only sent from a certain physical port. The SRC-MAC mode takes the source MAC address as the standard.

Different models of devices have different capabilities to support flow balancing strategies. The command prompt will only display the sharing strategies supported by the device. If no sharing strategy is supported or only one is supported, the relevant sub-commands will not be displayed.

Command Mode

Global Configuration Mode

Example

The following example shows how to change the load balance mode of port-aggregator to the src mode.

```
Switch(config)# interface p1 Switch(config-p1)#exit
Switch(config)# aggregator-group load-balance src-mac
```

14.1.3 show aggregator-group

Syntax

show aggregator-group [*id*] {*detail*|*brief*|*summary*}

This command is used to display detailed information of aggregator-group.

Parameter Description

Parameter	Parameter Description
id	ID of a specific logic port
detail|*brief*|*summary*	Information display type: detail, brief, summary

Default Value

None

Usage Guidelines

Displays port aggregation information.

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

14.1.4 show interface port-aggregator

Syntax

show interface p*id*

This command is used to display detailed information of interface port-aggregator.

Parameter Description

Parameter	Parameter Description
id	ID of a specific port

Default Value

None

Usage Guidelines

This command is used to display the information of port aggregation.

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

The following example shows how to display the information of aggregated port 1.

```
Switch#show interface p1
Port-aggregator1 is down, line protocol is down
Hardware is PortAggregator, Address is 0000.0000.0000(0000.0000.0000)
MTU 1500 bytes, BW 1000 kbit, DLY 2000 usec Encapsulation ARPA, loopback not set
Members in this Aggregator:
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 multicasts 0 input errors, 0 input discards

0 CRC, 0 frame, 0 overrun, 0 ignored   0 packets output, 0 bytes, 0 underruns Transmited 0
broadcasts, 0 multicasts  0 output errors, , 0 discards

0 output buffer failures, 0 output buffers swapped out
```

Note: Members in this Aggregator means physical ports which are aggregated to the logical port.

The statistics are explained as follows:

Packets input means the input of all messages, including unicast, multicast, and broadcast.

Bytes means the byte volume of all messages.

Broadcasts means received broadcast messages.

Multicasts means received multicasts messages.

Input errors means received error messages.

input discard means that the received messages are dropped, such as the received messages when the interface protocol is down.

packets Output means the output of all messages, including broadcast, multicast and unicast messages.

bytes means the byte volume of all transmitted messages.

broadcasts means transmitted broadcast messages.

multicasts means transmitted multicast messages.

output errors means transmitting error messages.

output discards means that the transmitted messages are dropped, such as the transmitted messages when the interface protocol is down.

14.1.5 debug lacp errors

Syntax

[**no**] **debug lacp errors**

This command is used to output LACP error debugging information.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to export all error information occurred during LACP running. The error information can help locate the errors.

Command Mode

EXEC mode

Example

```
Switch# debug lacp errors
```

14.1.6 debug lacp state

Syntax

[**no**] **debug lacp state**

This command is used to output the information of lacp state machine.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to output the information of lacp state machine.

Command Mode

EXEC mode

Example

```
Switch# debug lacp state
```

14.1.7 debug lacp packet

Syntax

[**no**] **debug lacp packet**

This command is used to output the information of lacp receiving or transmitting messages.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to output the information of lacp receiving or transmitting messages.

Command Mode

EXEC mode

Example

```
Switch# debug lacp packet
```

14.1.8 debug lacp interface

Syntax

debug lacp interface *dilD* **no debug lacp interface**

This command is used to debug lacp port information.

Parameter Description

Parameter	Parameter Description
dilD	Port number, range is 40-680s

Default Value

None

Usage Guidelines

This command is used to debug lacp port information.

Command Mode

EXEC mode

Example

```
Switch# debug lacp interface 41
```

14.1.9 debug lacp record

Syntax

[**no**] **debug lacp record**

This command is used to debug the port join/exit aggregation record information.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to debug lacp record information.

Command Mode

EXEC mode

Example

```
Switch# debug lacp record
```

Chapter 15 LLDP Configuration Commands

15.1 LLDP Commands

15.1.1 lldp run

Syntax

lldp run

no lldp run

To enable LLDP, run the command **lldp run**.

To disable LLDP, run the command **no lldp run**.

Parameter Description

None

Default Value

Disabled

Usage Guidelines

The port will periodically send lldp packets after the lldp function is enabled.

Command Mode

Global Configuration Mode

Example

The following command is used to enable LLDP.

```
switch(config)# lldp run
```

15.1.2 lldp holdtime

Syntax

lldp holdtime *time* **no lldp holdtime**

To configure the ttl value of LLDP, run the command lldp holdtime time. To resume the default value, run the command no lldp holdtime.

Parameter Description

Parameter	Parameter Description
time	Holdtime of the to-be-transmitted packet Range: 0-65535 seconds

Default Value

120s

Usage Guidelines

Normally, the remote information stored in MIB will update before aging. But the frame may loss during the sending process causing the information in the MIB ages. For avoiding this, you need to set the value of TTL and ensure the update LLDP frame is forwarded multiple times.

Command Mode

Global Configuration Mode

Example

The following example shows how to configure the ttl value of LLDP sending messages to 100 seconds.`switch(config)# lldp holdtime 100 switch(config)#`

15.1.3 lldp timer

Syntax

lldp timer *time* **no lldp timer**

To configure the transmission interval of LLDP messages, run lldp timer time. To resume the default value, run no lldp timer.

Parameter Description

Parameter	Parameter Description
time	The transmission Interval of LLDP messages. Range: 5-65534 seconds.

Default Value

30s

Usage Guidelines

The transmission interval of the LLDP message should be shorter than its storage time, ensuring multiple updates in the storage time and preventing errors caused by message loss.

Command Mode

Global Configuration Mode

Example

The following example shows how to configure the transmission interval of LLDP to 24 seconds.

```
switch(config)# lldp timer 24 switch(config)#
```

15.1.4 lldp reinit

Syntax

lldp reinit *time*

no lldp reinit

To configure the transmission delay of LLDP, run lldp reinit time. To resume the default transmission delay, run no lldp reinit.

Parameter Description

Parameter	Parameter Description
time	Transmission delay of LLDP. Range: 2-5 seconds

Default Value

2s

Usage Guidelines

LLDP information will be forwarded automatically in two conditions: first, the status or value of one or more information elements (management objects) in the local system have changed; second, the sending timer timeouts. A single information change causes the LLDP packet is forwarded and a series of continuous information changes may trigger many LLDP frames forwarded, but each frame can only report one change. To avoid this situation, the network management defines the interval of two continuous LLDP frames.

Command Mode

Global Configuration Mode

Example

The following example shows how to set the transmission delay of LLDP to five seconds.

```
switch(config)# lldp reinit 5 switch(config)#
```

15.1.5 lldp transmit

Syntax

lldp transmit

no lldp transmit

To set the port to transmit the LLDP messages, run lldp transmit. To forbid transmitting LLDP messages, run no lldp transmit.

Parameter Description

None

Default Value

Transmittable LLDP message mode

Usage Guidelines

This configuration command is valid only when the lldp module is started. You can set the port to a state where it cannot transmit lldp frames.

Command Mode

Interface configuration mode

Example

The following command configures port g0/0/1 to not transmit lldp messages mode.

```
switch(config-g0/0/1)# no lldp transmit switch(config-g0/0/1)#
```

15.1.6 lldp receive

Syntax

lldp receive

no lld preceive

To configure the port to the receivable LLDP message mode, run lldp receive. To disable receiving the LLDP message, run no lldp receive.

Parameter Description

None

Default Value

Receivable LLDP message mode

Usage Guidelines

This configuration is only valid when the lldp module is enabled. You can disable the port from receiving lldp frames.

Command Mode

Interface configuration mode

Example

The following example shows how to set port g0/0/1 not to receive the LLDP messages.

```
switch(config-g0/0/1)# no lldp receive switch(config-g0/0/1)#
```

15.1.7 lldp management-ip

Syntax

lldp management-ip *A.B.C.D* **no lldp management-ip**

To configure the management address of the LLDP port, run lldp management-ip. To resume the default value, run no lldp management-ip.

Parameter Description

Parameter	Parameter Description
A.B.C.D	Stands for the management IP address that will be specified.

Default Value

The default management address is the IP address of the VLAN interface corresponding to the port pvid; if this IP address does not exist, the default management address is 0.0.0.0.

Usage Guidelines

The configured management IP address should be the IP address related to a port.

Command Mode

Interface configuration mode

Example

The following example shows how to configure the management IP address of port g0/0/1 to 90.0.0.99.

```
switch(config-g0/0/1)# lldp management-ip 90.0.0.99 switch(config-g0/0/1)#
```

15.1.8 show lldp neighbors

Syntax

show lldp neighbors

This command is used to display brief information about neighbors.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to display brief information about neighbors, including Device-ID, Local-Intf, Hldtme, Port-ID and Capability.

Command Mode

EXEC/Global Configuration Mode

Example

```
switch(config)#show lldp neighbors Capability Codes:
(R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone (W)WLAN Access Point,
(P)Repeater,(s)station,(O)Other
Device-ID       Local-Intf      Hldtme       Port-ID      Capability
switch          Gig0/0/2          115          Gig0/0/32      B
switch          Gig0/0/32         114          Gig0/0/2       B

Total entries dispalyed: 2 switch(config)#
```

15.1.9 show lldp neighbors detail

Syntax

show lldp neighbors detail

This command is used to display detailed information about neighbors.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC/Global Configuration Mode

Example

```
switch(config)#show lldp neighbors detail
chassis id: 00e0.0f61.ca53 port id: Gig0/0/32
port description: GigaEthernet0/0/32 system name: switch

system description: s3448 software, Version 2.0.1K serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 98
system capabilities: R B enabled capabilities: B  Managment Address:
IP: 192.168.213.62
```

```
Auto Negotiation -- supported,enabled Physical media capabilitise:
100baseTX(FD) 100baseTX(HD) 10baseT(FD)   10baseT(HD)
Media Attachment Unit type: 16

----------------------------------------


chassis id: 00e0.0f61.ca35 port id: Gig0/0/2
port description: GigaEthernet0/0/2 system name: switch

system description: s3448 software, Version 2.0.1K serial: s35000456
Compiled: 2008-11-13 13:33:36 by 16170F032B9F

Time remaining: 95
system capabilities: R B enabled capabilities: B  Managment Address:
IP: 90.0.0.66

Auto Negotiation -- supported,enabled
Physical media capabilitise:
100baseTX(FD) 100baseTX(HD) 10baseT(FD)   10baseT(HD)
Media Attachment Unit type: 16


----------------------------------------


Total entries displayed: 2 switch#
```

Chapter 16 MAC Access List Configuration Commands

16.1 MAC Access List Configuration Commands

16.1.1 mac access-list

Syntax

[**no**] **mac access-list** *name*

To add/delete a MAC access list, run the command.

Parameter Description

Parameter	Parameter Description
name	Name of the MAC access list. Its length is 1-20 characters.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used in global configuration mode. The masks of multiple entries in an access list must be the same, otherwise the configuration will fail. At the same time, the same entry can only be configured once in an access list.

Example

The following example shows how to configure a MAC access list named mac-acl..

```
Switch(config)#mac access-list mac-acl Switch(config-macl)#
```

16.1.2 permit

Syntax

[**no**] **permit** {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* | *dst- mac-addrdst-mac-mask*}[**arp** | **ip** [{**any** | *src-ip-addr src-ip-mask*} {**any** | *dst-ip-addrdst-ip-mask*}] |

ethertype | **cos** *cos_value* | **vlan** *vlan-id* | **location** *locat_num*]

To add/delete a MAC access list item, run the command.

Parameter Description

Parameter	Parameter Description	Value Range
any	Any value	-
host	Host	-
src-mac-addr	Source MAC address	AA:BB:CC:DD:EE:FF
src-mac-mask	Source MAC mask	AA:BB:CC:DD:EE:FF
dst-mac-addr	Destination MAC address	AA:BB:CC:DD:EE:FF
dst-mac-mask	Destination mac mask	AA:BB:CC:DD:EE:FF
arp	Matched arp messages	-
ip	Matched IP messages	-
src-ip-addr	Source IP address	A.B.C.D
src-ip-mask	Source IP mask	A.B.C.D
dst-ip-addr	destination IP address	A.B.C.D
dst-ip-mask	destination IP mask	A.B.C.D
ethertype	Type of the matched Ethernet packet	0x0600-0xFFFF
cos_value	Cos priority of the message	0-7
vlan_id	vlan-id of the message	1-4094
locat_num	The location to the inserted entry	-

Default Value

Deny all

Command Mode

MAC access list configuration mode

Usage Guidelines

This command is running in MAC access list configuration mode.

Example

The following example shows how to configure a host with a source MAC address of 12:34:56:78:ae:cd.

```
Switch(config-macl)#permit host 12:34:56:78:ae:cd any 0x806
```

16.1.3 deny

Syntax

[**no**] **deny** {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* | *dst- mac-addrdst-mac-mask*}[**arp** | **ip** [{**any** | *src-ip-addr src-ip-mask*} {**any** | *dst-ip-addrdst-ip-mask*}] |

ethertype | **cos** *cos_value* | **vlan** *vlan-id* | **location** *locat_num*]

To add/delete an item rejected by MAC access list item, run the command.

Parameter Description

Parameter	Parameter Description	Value Range
any	Any value	-
host	host	-
src-mac-addr	source MAC address	AA:BB:CC:DD:EE:FF
src-mac-mask	source mac mask	AA:BB:CC:DD:EE:FF
dst-mac-addr	destination MAC address	AA:BB:CC:DD:EE:FF
dst-mac-mask	destination mac mask	AA:BB:CC:DD:EE:FF
arp	matched arp messages	-
ip	matched ip messages	-
src-ip-addr	source IP address	A.B.C.D
src-ip-mask	source IP mask	A.B.C.D
dst-ip-addr	Destination IP address	A.B.C.D
dst-ip-mask	destination IP mask	A.B.C.D
ethertype	Type of the matched Ethernet packet	0x0600-0xFFFF
cos_value	Cos priority of the message	0-7
vlan_id	vlan-id of the message	1-4094
locat_num	The location to the inserted entry	-

Default Value

Deny all

Command Mode

MAC access list configuration mode

Usage Guidelines

This command is running in MAC access list configuration mode.

Example

The following example shows how to reject a host whose MAC address is 12:34:56:78:ae:cd.

```
Switch(config-macl)#deny host 12:34:56:78:ae:cd any 0x806
```

16.1.4 mac access-group

Syntax

1. Global:

mac access-group name { **vlan** {*word* **| add** *word* | **remove** *word*}} [**egress**] [**stat-packet** | **stat-byte**] [**no**] **mac access-group** *name* [**vlan** [**egress**]]

2. Port:

[**no**] **mac access-group** *name* **[egress] [stat-packet | stat-byte]**

To apply the established MAC access list to an interface, a global mode or a VLAN. To cancel a MAC access list which is applied to an interface, a global mode, or a VLAN.

Parameter Description

Parameter	Parameter Description
name	Name of the MAC access list
egress	The access list is applied in egress.
vlan	The access list is applied in ingress.
word	vlan range table
add	add vlan range table
remove	Delete vlan range table
stat-packet	Statistics of messages
stat-byte	Statistics of bytes

Default Value

No MAC access list is applied to an interface

Command Mode

Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The command is used in Layer 2 physical port configuration mode or global configuration mode.

Example

The following example shows how to configure the MAC access list named macacl on port tg0/0/1 in ingress.

```
Switch(config-tg0/0/1)#mac access-group macacl
```

The following example shows how to configure the global MAC access list named macacl in ingress.

```
Switch(config)#mac access-group macacl
```

16.1.5 show mac access-list

Syntax

show mac access-list [*name*]

This command is used to display all or specified mac access lists.

Parameter Description

Parameter	Parameter Description
name	The name of the mac access list.

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to show MAC access list.

```
Switch(config)#show mac access-list mac access-list 1
index:1 permit host 0001.0001.0001 any Switch(config)#
```

16.1.6 show mac access-group

Syntax

show mac access-group *name* {**vlan** | **interface** *interface-name*} [**egress**]

To display the statistics information of mac access list, run the command.

Parameter Description

Parameter	Parameter Description
name	The name of the mac access list.
interface-name	*interface*

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to display the statistics information of mac access list.

```
Switch(config)#show mac access-group 1 mac access-list 1
permit host 00:01:00:01:00:01 any  statistics: 10 packets
```

Chapter 17 MAC Address Related Configuration Commands

17.1 MAC Address Configuration Commands

17.1.1 mac address-table static

Syntax

[**no**] **mac address-table static** *mac-addr***vlan** *vlan-id* **interface** *interface-id*

The command is used to add/delete a static MAC address.

Parameter Description

Parameter	Parameter Description
mac-addr	MAC address, such as AA:BB:CC:DD:EE:FF.
vlan-id	A VLAN that the MAC address belongs to. Value range: 1-4094
interface-id	Physical port that the MAC address belongs to

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to bundle MAC address 00:04:56:00:67:ab to port g1/0/2 in VLAN1.

```
Switch(config)# mac address-table static 00:04:56:00:67:ab vlan 1 interface g1/0/2
```

17.1.2 mac address-table aging-time

Syntax

mac address-table aging-time {*0* | *10-1000000*}

This command is used to configure the aging time of the MAC address table.

Parameter Description

Parameter	Parameter Description
0	The MAC address never ages.
10-1000000	Aging time of the MAC address whose unit is second. The default value is 300s.

Default Value

300s

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to set the ageing time of the MAC address to 100 seconds.

```
Switch(config)# mac address-table aging-time 100
```

17.1.3 mac address-table blackhole

Syntax

[no] mac address-table blackhole *mac-addr***vlan** *vlan-id*

This command is used to configure a MAC blackhole address.

Parameter Description

Parameter	Parameter Description
mac-addr	MAC address, such as AA:BB:CC:DD:EE:FF.
vlan-id	VLAN belonged to the MAC address. The value ranges from 1 to 4094.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to Set the MAC address 00:04:56:00:67:ab of VLAN 1 as a blackhole address.

```
Switch(config)# mac address-table blackhole 00:04:56:00:67:ab vlan 1
```

17.1.4 show mac address-table

Syntax

show mac address-table [**dynamic** [**interface** *interface-id* | **vlan** *vlan-id*] |**security** [**interface** *interface-id*] | **static** | **brief** | **multicast** | **interface** *interface-id* | **vlan** *vlan-id* | **mac**

AA:BB:CC:DD:EE:FF | **blackhole**]

This command is used to display the MAC address table of the switch.

Parameter Description

Parameter	Parameter Description
dynamic	Dynamically-learned MAC address table
interface-id	Name of an interface
vlan-id	VLAN ID Value range: 1-4094
security	The mac address in port security mode can be viewed in full or on a specific port.
static	Static MAC address table
brief	Brief information about the MAC address
multicast	Multicast MAC address table
interface	Interface MAC address table
vlan	Vlan mac address table
mac	A specific address
blackhole	Black hole MAC address table

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

This command is used to display the MAC address table.

Example

The following example shows how to display all dynamic MAC address tables.

```
Switch(config)#show mac address-table Mac Address Table (Total 2)


Vlan    Mac Address     Type     Ports
1       00:26:5a:7c:fa:d3     DYNAMIC     tg0/0/1
1       00:00:00:00:00:04     DYNAMIC     tg0/0/1
```

17.1.5 clear mac address-table

Syntax

clear mac address-table dynamic [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*]

This command is used to delete the dynamic MAC address.

Parameter Description

Parameter	Parameter Description
mac-addr	MAC address, such as AA:BB:CC:DD:EE:FF.
interface-id	Layer 2 port name
vlan-id	VLAN ID Value range: 1-4094

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is configured in EXEC configuration mode.

Example

The following example shows how to clear all dynamically learned MAC addresses on the port tg0/0/2.

```
Switch# clear mac address-table dynamic interface tg0/0/2
```

17.2 Mac Notify Configuration Commands

17.2.1 mac address-table notify learn

Syntax

[**no**] **mac address-table notify learn** {**syslog** | **trap-snmp**}

This command is used to enable log notification or trap notification when mac address learns.

Parameter Description

None

Default Value

Disabled by default

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to enable log notification and trap notification when mac address learns.

```
Switch(config)#mac address-table notify learn syslog
Switch(config)#mac address-table notify learn trap-snmp
```

17.2.2 mac address-table notify mac-move

Syntax

[**no**] **mac address-table notify mac-move** {**syslog** | **trap-snmp**}

This command is used to configure log notification or trap notification when mac address moves.

Parameter Description

None

Default Value

Disabled by default

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to configure log notification or trap notification when mac address learns.

```
Switch(config)#mac address-table mac-move learn syslog
Switch(config)#mac address-table mac-move learn trap-snmp
```

17.2.3 mac address-table notify interval

Syntax

[**no**] **mac address-table notify interval** *time*

This command is used to configure the notification interval for learning and mac-move.

Parameter Description

Parameter	Parameter Description
time	Notification interval. The unit is second. The default value is 1s.

Default Value

1s

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to configure the notification interval.

```
switch(config)#mac address-table notify interval ? <0-60> -- Notifiy interval in seconds(default 1)
```

Chapter 18 Network Management Configuration Commands

18.1 SNMP Commands

SNMP commands are listed below:

- snmp-server community
- snmp-server contact
- snmp-server host
- snmp-server location
- snmp-server user
- snmp-server view
- snmp-server enable
- show snmp

18.1.1 snmp-server community

Syntax

The following command is used to set the community access string of the accessible SNMP protocol in global configuration mode. To delete the specified community character string, use the no form of this command.

snmp-server community *string* [**ro | rw**] [**view** *view-name*]

no snmp-server community *string*

Parameter Description

Parameter	Parameter Description
string	Means the community string of the accessible SNMP protocol, which is similar to the password.
view view-name	(optional) stands for the previously defined view's name. In this view, the MIB objects are defined, which are effective to the community.
ro	(Optional) Designates the read-only permission. Those authorized workstations can only read the MIB objects.
rw	(Optional) Designates the read-write permission. Those authorized workstations can read and modify the MIB objects.

Default Value

By default, the SNMP community string allows read-only permission to all objects.

Command Mode

Global Configuration Mode

Usage Guidelines

The following command shows how to delete a designated community.

no snmp-server community *string*

Command Mode

Global EXEC mode

Example

The following example shows how to distribute the "mgr" string to SNMP, allow to read and write access to the objects in the Restricted view.

```
Switch(config)#snmp-server community mgr rw view restricted
```

The following example shows how to delete the "comaccess" community.

```
Switch(config)#no snmp-server community comaccess
```

18.1.2 snmp-server contact

Syntax

To use the Global Configuration Mode command snmp-server contact to set the contact information (sysContact) of the management node, run snmp-server contact text. To remove the contact information, use the no form of this command.

snmp-server contact *text*

no snmp-server contact

Parameter Description

Parameter	Parameter Description
text	Means the string of the information about the contact person.

Default Value

The information about contact person is not set.

Command Mode

Global Configuration Mode

Usage Guidelines

It corresponds to the sysContact of the MIB variable in the System group.

Example

The following example shows the information about the contact person in a node.

```
Switch(config)#snmp-server contact Dial_System_Operator_at_beeper_\#_27345
```

18.1.3 snmp-server host

Syntax

To specify the receiver of SNMP trap operation, run the first of the following commands in global configuration mode. To cancel this designated host, run the following second command.

snmp-server host *host* **version** [**v1**|**v2c**] *community-string* [**informs**|**trap**]

no snmp-server host *host* **version** [**v1**|**v2c**] *community-string* [**informs**|**trap**]

Parameter Description

Parameter	Parameter Description
host	Means the host's name or the address of the Internet. Uses bipv4 address in host
[**v1**|**v2c**]	(Optional) Means the version ID of the SNMP protocol, which is used to transmit traps.
[**informs** | **traps**]	(Optional) Specifies the type of trap for version V2C. Informs: means the type of trap is "informs". Traps: means the type of trap is "traps".
community-string	Means a community string in version 1 and version 2c which is similar to the password sent with the trap operations.

Default Value

This command is invalid in default settings. No trap will be sent by default. If no command with any key word is entered, all traps with v1 standard are not sent by default.

Command Mode

Global Configuration Mode

Usage Guidelines

If this command is not entered, the traps will not be sent. In order to enable a switch to send the SNMP traps, you must run snmp-server host. If the keyword "trap-type" is not contained in this command, all kinds of traps of this host will be activated. If the keyword "trap-type" is contained in this command, all trap types related with this keyword are activated. You can specify multiple trap types in this command for each host.

If you designate multiple snmp-server host commands on the same host, the SNMP trap messages that are sent to the host will be decided by the community string and the trap type filtration in this command. (Only one trap type can be configured for a same host and a same community string).

The availability of the trap-type option depends on the device type and the attributes of routing software, which is supported by this device.

Example

The following example shows how to transmit SNMP traps to host 10.20.30.40. The community string is defined as `comaccess`.

```
Switch(config)#snmp-server host 10.20.30.40 version v2c comaccess traps
```

18.1.4 snmp-server location

Syntax

To set the location string of a node, run the first one of the following two commands in global configuration mode. To cancel this designated host, run the following second command.

snmp-server location *text*

no snmp-server location

Parameter Description

Parameter	Parameter Description
text	A string describing the location of the node

Default Value

The location string of a node is not set by default.

Command Mode

Global Configuration Mode

Usage Guidelines

It corresponds to the sysLocation of the MIB variable in the System group.

Example

The following example shows how to define the actual location of a device.

```
Switch(config)#snmp-server location Building_3/Room_214
```

Related Command

```
Switch(config)#snmp-server contact
```

18.1.5 snmp-server user

Syntax

To create or update **snmp user** in global configuration mode, run the following first command; To cancel this SNMP user, run the following second command.

If the remote parameter is designated, a remote user will be configured; when a remote user is configured, the SNMP engine ID that corresponds to the IP address of this management station must exist. Format of the command is as follows:

snmp-server user *username* {**ro**|**rw**} {**noauthnopriv** | **authnopriv** | **authpriv**} [**view** *view_name*] [**authtype**] [**MD5** *KEY* **privacytype** *KEY* ***DES*** *KEY*|***AES*** *KEY* **view** *view_name*]|[**SHA** *KEY*

privacytype DES|**AES** *KEY* **view** *view_name*]

Parameter Description

Parameter	Parameter Description
username	Stands for the name of the created or modified SNMP user.
{**ro**|**rw**}	Stands for User Permissions
{**noauthnopriv** | **authnopriv** | **authpriv**}	Encryption Type
[**MD5**|**SHA**]	The method of encryption authentication.
KEY	The authentication password of the user
view_name	SNMP MIB view name
DES	Data encryption protocol
AES	Advanced encryption protocol

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to set the username and the password.

Example

In the following example, an SNMP user is created, whose name is set-user,writable permissions, the security level is authentication and encryption, the password is 12345678, and MD5 is used as the harsh algorithm.

```
Switch(config)#snmp-server user set-user rw authpriv md5 12345678
```

18.1.6 snmp-server view

Syntax

To create or update a MIB view, run the first one of the following two commands in global configuration mode. To cancel a view in the SNMP server, run the second one of the following two commands.

snmp-server view *view-name oid-tree* {**included** | **excluded**} **no snmp-server view** *view-name*

Parameter Description

Parameter	Parameter Description
view- name	Updates or creates the label of a view.
oid-tree	The object IDs of the ASN.1 sub-tree must be contained or excepted from a view. The identifier sub-tree is used to designate a numeral-contained string, e.g., 1.3.6.2.4 or a system sub-tree. The sub-tree name can be found in all MIB trees.
{**included** | **excluded**}	the view type. The parameter included or excluded must be specified.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

If other SNMP commands need a view as a parameter, you can use this command to create a view as the parameter of these SNMP commands. By default, you need not define the view, and you can see all the views, equivalent to Cisco-predefined views. The command is used to define objects that can be seen in the view.

Example

The following example shows how to create the views of all objects in the MIB-II sub-tree.

```
Switch(config)#snmp-server view mib2 mib-2 included
```

The following example shows how to create the views of all objects, including those objects in the system group.

```
Switch(config)#snmp-server view phred system included
```

The following example shows how to create the views of all objects that includes the objects in the system groups but excludes the objects in system7(sysServices.7) and interface 1.

```
Switch(config)#snmp-server view agon system included  Switch(config)#snmp-server view agon system.7 excluded
```

Related Command

```
snmp-server community
```

18.1.7 snmp-server enable

Syntax

The following command is used to enable/disable snmp service.

[**no**] **snmp-server enable**

Parameter Description

None

Default Value

Snmp service is disabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to enable snmp service.

18.1.8 show snmp

Syntax

The following commands are used to display SNMP related information.

show snmp [**community** |**contact** | **location** | **source** |**mibs** | **state** | **user** | **trap**]

Parameter Description

Parameter	Parameter Description
community	Display community string entries
contact	Display SNMP MIB node contact information
location	Display SNMP MIB node location information
source	Display information about global SNMP restricted sources.
mibs	Display SNMP MIB registration information
state	Display SNMP service status information
user	Display SNMP user information
trap	Display SNMP trap information

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

The command **show snmp community** is used to display community string entries.

The command **show snmp contact** is used to display SNMP MIB node contact information.

The command **show snmp location** is used to display node location information.

The command **show snmp source** is used to display information about global SNMP restricted sources.

The command **show snmp mibs** is used to display SNMP MIB registration information.

The command **show snmp state** is used to display SNMP service status information.

The command **show snmp user** is used to display SNMP user information.

The command **show snmp trap** is used to display SNMP trap information.

Example

The following example shows how to display SNMP community information.

```
Switch(config)#show snmp community community planet rw
```

The following example shows how to display SNMP trap information.

```
Switch(config)#show snmp trap

192.168.25.62 version v2c planet traps
```

18.2 RMON Configuration Commands

18.2.1 rmon alarm

Syntax

rmon alarm *index variable interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**repeat**] [**owner** *string*]

To configure a rmon alarm entry, run the above command.

Parameter Description

Parameter	Parameter Description
index	Stands for the index of the event table Value range: 1-65535
variable	Stands for the object needs to be monitored. Value range: oid of the monitored object.
interval	Stands for the sampling interval Value range: 1~ 2147483647 seconds.
absolute	Take the absolute value
delta	Take relative value
value	Stands for the alarm threshold Value range: -1~ 2147483647.
eventnumber	Stands for the event index generated after reaching the threshold. Value range: 1~65535.
repeat	Stands for the repeat trigger event.
string	Stands for the owner description information Value range: the length of the character string is 1~31.

Default Value

eventnumber is not set by default.

repeat is not set by default.

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to monitor the value of specified object. The certain event will be triggered when the value exceeds the threshold.

Example

The following example shows how to set an alarm entry to monitor the object ifInOctets.2 and the sampling interval is 10. When the sampling interval increases more than 15, event 1 will be triggered. When the sampling interval decreases more than 25, event 2 will be triggered.

```
Switch(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.10.2 10 absolute rising-threshold 15 1
falling-thr
```

18.2.2 rmon event

Syntax

rmon event *index* [**description** *des-string*] [**log**] [**owner** *owner-string*] [**trap** *community*] [**ifctrl** *interface*]

To configure a rmon event entry, run the above command.

Parameter Description

Parameter	Parameter Description
index	Stands for the index of the event table Value range: 1-65535
des-string	Stands for the event description character string. Value range: 1~127.
owner-string	Stands for the owner character string. Value range: 1~31.
community	Stands for the community name when generating trap. Value range: 1~31.
interface	Stands for the shutdown port that the event controls.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to set a rmon event entry for alarm.

Example

The following example shows setting one rmon event entry with an index of 6 and the description character string to example. When an event is triggered, an entry is added to the log table and a trap is generated with public as the community's name.

```
Switch(config)#rmon event 6 log trap public description example owner switch
```

18.2.3 show rmon

Syntax

show rmon [**alarm**] [**event**]

To show rmon configuration, run the above command.

Parameter Description

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

To show rmon configuration, run the above command.

Example

To show rmon configuration, run the following command.

```
Switch(config)#show rmon
alarm Index 1(status is valid) Variable 1.3.6.1.4.1.10456.1.1670.0 Interval 5 Type absolute riseThr alarm Index 2(status is valid) Variable 1.3.6.1.4.1.10456.1.1670.0 Interval 4 Type absolute riseThr event Index 1(status is valid) log owner aa
event Index 2(status is valid) trap planet owner sc
```

Chapter 19 NTP Configuration Commands

19.1 ntpd enable

Syntax

ntpd enable

To enable the ntp function, run the command.

no ntpd enable

To disable the ntp function, run the command.

Parameter

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After **ntpd** is enabled, both the client and the server are enabled.

Example

```
Switch(config)#ntpd enable
Switch(config)#no ntpd enable
```

Related Command

ntpd server

19.1.1 ntpd server

Syntax

ntpd server *A.B.C.D* [**poll** *poll*]

To add a remote ntp server configuration, run the command.

no ntpd server [*A.B.C.D*]

To delete a remote ntp server configuration, run the command.

Parameter

Parameter	Parameter Description
A.B.C.D	The address of the ntp server, which can be an IP address or a domain name
poll	The time interval between client requests is valid for 2 seconds.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to set the address of the ntp server. Only supports configuring a single ntp clock source.

Example

```
Switch(config)#ntpd server 1.1.1.1
```

Related Command

ntpd enable

19.1.2 ntpd broadcast

Syntax

ntpd broadcast client-enable

To enable the device to receive broadcast clock sources, run the command.

no ntpd broadcast client-enable

To enable the device to reject broadcast clock sources, run the command.

ntpd broadcast server-enable

To provide broadcast clock source service, run the command.

no ntpd broadcast server-enable

To disable the broadcast clock source service of the device, run the command.

Parameter

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

When setting the broadcast clock source server, you need to configure the port route of the broadcast address 255.255.255.255 or specify the default route.

Example

The following command is used to configure the broadcast clock source server.

```
Switch(config)#ntpd broadcast server-enable Switch(config)#ip route default 1.1.1.1
```

The following command is used to configure the broadcast clock source client.

```
Switch(config)#ntpd broadcast client-enable
```

Related Command

ntpd server

19.1.3 ntpd ntpq

Syntax

ntpd ntpq

To view the detailed status of the ntp peer, run the command.

Parameter

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to view the ntpd peer status. The relevant instructions are as follows:

Field Name	Definition
remote	The IP address of the ntpd server
refid	The reference source of the server clock
st	Clock hierarchy
t	Type, u represents unicast mode, b represents broadcast mode, and m represents multicast mode
when	The time (in seconds) since the last message was received from the server
poll	The time interval between two NTP messages sending.
reach	Octal number, the status of the last eight messages, used to update poll.
delay	The sending delay between the client and the server (in milliseconds)
offset	Time deviation from the server (in milliseconds)
jitter	(Deprecated) The volatility of the data

Example

```
Switch(config)#ntpd ntpq
```

Related Command

ntpd server

19.1.4 show ntpd

Syntax

show ntpd

To display the relevant information of ntp configuration, run the command.

Parameter

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to display the current status of ntp.

Example

```
Switch(config)#show ntpd state:   enable
server:  120.25.115.20
```

Chapter 20 OAM Configuration Commands

20.1 OAM Configuration Commands

20.1.1 ethernet oam

Syntax

[**no**] **ethernet oam**

The command is used to enable or disable OAM.

Parameter Description

None

Default Value

ethernet oam disable

Command Mode

Port Configuration Mode

Usage Guidelines

None

Example

The following command enable OAM on port tg0/0/2.

```
Switch#
Switch#config
Switch(config)#interface tg0/0/2
Switch(config-tg0/0/2)#ethernet oam
```

20.1.2 ethernet oam {max-rate | min-rate | mode | timeout}

Syntax

[**no**] **ethernet oam** {**max-rate** *value1* | **min-rate** *value2* | **mode** {**active** | **passive**} | **timeout** *value3*}

ethernet oam max-rate *value1*

The command is used to set the maximum sending rate of OAM packets.

ethernet oam min-rate *value2*

The command is to specify the slowest transmission rate of OAM packets.

ethernet oam mode {**active** | **passive**}

The command is used to set OAM mode.

ethernet oam timeout *value3*

The command is used to set the timeout period for an OAM connection.

Parameter Description

Parameter	Parameter Description
value1	The fastest send rate, value range: 1-10, unit: packets/second
value2	The slowest send rate, in the range of 1 to 10, in seconds
value3	The timeout period of an OAM connection, which can range from 2 to 30 in seconds

Default Value

max-rate has a value of 10;

The value of min-rate is 1 ; The value of timeout is 5 ; mode is active.

Command Mode

Port Configuration Mode

Usage Guidelines

This command configure some optional parameters for establishing an OAM connection.

Example

The following command sets the fastest connection rate of OAM on tg0/0/2 to 5 packets/second, the slowest connection rate to send a packet in 5 seconds, the connection timeout period to 10 seconds, and sets the OAM mode to passive.

```
Switch(config)#
Switch(config)#interface tg0/0/2
Switch(config-tg0/0/2)# ethernet oam max-rate 5  Switch(config-tg0/0/2)#ethernet oam min-rate 5   Switch(config-tg0/0/2)#ethernet oam timeout 10   Switch(config-tg0/0/2)#ethernet oam mode passive
```

20.1.3 ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action

Syntax

ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault** } **action error-disable- interface**

no ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault** } **action**

The command is used to trigger action after receiving a remote fault indication.

Parameter Description

None

Default Value

There is no triggering action after receiving a remote fault indication.

Command Mode

Port Configuration Mode

Usage Guidelines

PLANET's Switch cannot generate Link Fault and Critical Event packets, but these packets are processed when received from the remote end. The PLANET Switch supports sending and receiving Dying Gasp packets. When a local port enters the errdisabled state, or the local port is manually disabled by the administrator, or the OAM function on the local port is manually disabled by the administrator, a Dying Gasp packet is sent to the remote port connected to the local port .

Example

Configure the action error-disable-interface after receiving a remote link fault indication on tg0/0/1:

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#ethernet oam remote-failure link-fault action error-disable-interface
```

20.1.4 ethernet oam remote-loopback {supported | timeout}

Syntax

ethernet oam remote-loopback supported

The command is used to configure whether the remote loopback is supported.

ethernet oam remote-loopback timeout *value*

The command is used to configure the remote loopback timeout period.

Parameter Description

Parameter	Parameter Description
value3	The timeout period of an OAM connection, in the range of 1 to 10, in seconds

Default Value

2 seconds

Command Mode

Port Configuration Mode

Usage Guidelines

This timer is valid only for the master side of the loopback, if the master side does not receive a response from the slave side within the specified timeout period after making a start or stop request, the master side will automatically exit the loopback mode.

Example

Configure the timeout period of loopback on tg0/0/2 to be 5 seconds.

```
Switch(config-tg0/0/2)#ethernet oam remote-loopback timeout 5
```

20.1.5 ethernet oam link-monitor {symbol-period | frame | frame- period | frame-seconds | receive-crc} threshold high

Syntax

[**no**] **ethernet oam link-monitor** {**symbol-period** | **frame** | **frame-period** | **frame-seconds** | **receive- crc**} **threshold high** {**none** | *value*}

The command is used to configure high thresholds for link monitoring (Error Signal Periodic Event, Error Frame Event, Error Frame Periodic Event, Error Frame Seconds Event, Error CRC Event).

Parameter Description

Parameter	Parameter Description
Value	For the error signal periodic, the value range: 1-65535, unit: number of signals; For error frame events, the value range: 1-65535, unit: number of frames; For the wrong frame period event, the value range: 1-65535, unit: number of frames; For the error frame number of seconds event, the value range: 1-900, unit: seconds; For incorrect CRC events, the value range: 1-65535, unit: number of frames.

Default Value

For all kinds of general link events, the default value is none;

Command Mode

Port Configuration Mode

Usage Guidelines

When a high threshold for an event is configured, and the ethernet oam link-monitor high-threshold action error-disable-interface is configured, the locally received event will enter the errdisabled state if the event exceeds the high threshold.

Example

The high threshold for configuring the Wrong Frame Cycle event on port tg0/0/2 is 10.

```
Switch(config-tg0/0/2)#ethernet oam link-monitor symbol-period threshold high 10
```

20.1.6 ethernet oam link-monitor {symbol-period | frame | frame- period | frame-seconds | receive-crc} threshold low

Syntax

[**no**] **ethernet oam link-monitor** {**symbol-period** | **frame** | **frame-period** | **frame-seconds** | **receive- crc**} **threshold low** {**none** | *value*}

The command is used to configure low thresholds for link monitoring (Error Signal Cycle Event, Error Frame Event, Error Frame Cycle Event, Error Frame Seconds Event, Error CRC Event).

Parameter Description

Parameter	Parameter Description
Value	For the error signal periodic event, the value range: 0-65535, unit: number of signals; For error frame events, the value range: 0-65535, unit: number of frames; For the error frame period event, the value range: 0-65535, unit: number of frames; For the error frame number of seconds event, the value range: 0-900, unit: seconds; For incorrect CRC events, the value range: 0-65535, unit: number of frames.

Default Value

For the error signal period event, the Default Value value is 1; For error frame events, the Default Value value is 1;
For the error frame period event, the Default Value value is 1; For the error frame second event, the Default Value value is 1; For incorrect CRC events, the Default Value value is 10.

Command Mode

Port Configuration Mode

Usage Guidelines

If a low threshold is configured for an event, the event received locally exceeds the low threshold, and the event notification OAM packet is used to report to the peer.

Example

Configure a low threshold of 10 for the error signal cycle event on port tg0/0/2.

```
Switch(config-tg0/0/2)#ethernet oam link-monitor symbol-period threshold low 10
```

20.1.7 ethernet oam link-monitor {symbol-period | frame | frame- period | frame-seconds | receive-crc} window

Syntax

ethernet oam link-monitor {**symbol-period** | **frame** | **frame-period** | **frame-seconds** | **receive-crc**} **window** *value*

The command is used to configure the polling window size for link monitoring (Error Signal Periodic Event, Error Frame Event, Error Frame Periodic Event, Error Frame Seconds Event, Bad CRC Event).

Parameter Description

Parameter	Parameter Description
Value	For the error signal periodic event, the value range is 10-600 on GigaEthernet and 1-60 on FastEthernet, and the unit is 100M signals. For error frame events, the value range: 1-60, unit: seconds; For the error frame period event, the value range is 100-6000 on GigaEthernet and 10-600 on FastEthernet, and the value range is 14881 frames. For the error frame number of seconds event, the value range: 10-900, unit: seconds; For erroneous CRC events, the value ranges from 1 to 180 in seconds.

Default Value

For the error signal periodic event, the Default Value value is 10 on GigaEthernet and 1 on FastEthernet. For error frame events, the default value is 1;

For the error frame period event, the Default Value value is 100 on GigaEthernet and 10 on FastEthernet. For error frame seconds events, the default value is 60;

For incorrect CRC events, the default value is 1.

Command Mode

Port Configuration Mode

Usage Guidelines

None

Example

Configure the window for the error signal cycle event on port tg0/0/2 to 50.

```
Switch(config-tg0/0/2)#ethernet oam link-monitor symbol-period window 50
```

20.1.8 ethernet oam link-monitor high-threshold action

Syntax

ethernet oam link-monitor high-threshold action error-disable-interface

[**no**] **ethernet oam link-monitor high-threshold action**

The command is used to configure the trigger event for link monitoring high thresholds.

Parameter Description

None

Default Value

There are no high-threshold triggering events.

Command Mode

Port Configuration Mode

Usage Guidelines

When a high threshold for an event is configured, and the Ethernet OAM link-monitor high-threshold action error-disable-interface is configured, the locally received event will enter the **errdisabled s**tate if the event exceeds the high threshold.

Example

Set the high-threshold trigger event to **error-disable-interface** on port tg0/0/2.

```
Switch(config-tg0/0/2)#ethernet oam link-monitor high-threshold action error-disable-interface
```

20.1.9 ethernet oam link-monitor negotiation-supported

Syntax

[**no**] **ethernet oam link-monitor negotiation-supported**

The command used to configure whether link monitoring negotiation is supported.

Parameter Description

None

Default Value

Support negotiation

Command Mode

Port Configuration Mode

Usage Guidelines

Negotiation is supported by default, our device supports link monitoring function, but if the third-party device does not support the link monitoring function, our device will automatically not support link monitoring during OAM Discovery, so that OAM connection can be established through the third-party device; Otherwise, when the configuration is not negotiated, our device will force support the link monitoring function, and if the third-party device does not support it, it may not be able to establish an OAM connection.

Example

The link monitoring function is not supported on port tg0/0/2.

```
Switch(config-tg0/0/2)#no ethernet oam link-monitor negotiation-supported
```

20.1.10 ethernet oam remote-loopback {start | stop}

Syntax

ethernet oam remote-loopback {**start** | **stop**} **interface** *intf-id*

The command is used to actively start or stop OAM remote loopback.

Parameter Description

Parameter	Parameter Description
intf-id	Specify the port.

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The OAM remote loopback on a physical port that is an aggregation port is not allowed.

Example

An OAM remote loopback is initiated on port tg0/0/2.

```
Switch#ethernet oam remote-loopback start interface tg0/0/2
```

20.1.11 clear ethernet oam statistics

Syntax

clear ethernet oam statistics [**interface** *intf-id*]

The command is used to clear OAM statistics.

Parameter Description

Parameter	Parameter Description
intf-id	Specify the port. If no ports are specified, OAM statistics are cleared on all ports.

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

When you run this command, the packet count information classified by packet type, general link event statistics, and remote fault statistics are cleared at the same time.

Example

Clear the OAM statistics on port tg0/0/2.

```
Switch#clear ethernet oam statistics interface tg0/0/2
```

20.1.12 show ethernet oam discovery

Syntax

show ethernet oam discovery [**interface** *intf-id*]

The command is used to display OAM discovery information on all ports or on a specified port, including the loopback status of the local DTE port and the information about the local information TLV and remote information TLV in OAM Information packets.

Parameter Description

Parameter	Parameter Description
intf- id	Displays the discovery information of the specified port, otherwise displays the discovery information of all ports where protocol up and OAM is enabled.

Default Value

None

Usage Guidelines

None

Example

OAM discovery information is displayed on port tg0/0/2.

```
Switch(config-tg0/0/2)#show ethernet oam discovery interface tg0/0/2 tg0/0/2
Local Info TLV
  --------------
PDU revision:      1

Loopback status:    LB_DISABLED

OAM configurations field:
Mode             : active
Unidirection       : not supported
Remote loopback    : supported
Link Events        : supported
Variable retrieval: not supported

Mtu size:          1500

OUI:               00e00f

Remote Info TLV
```

```
---------------
MAC address:         001b.0d9c.e703

PDU revision:      0

OAM configurations field:
Mode              : active
Unidirection      : not supported
Remote loopback   : not supported
Link Events       : supported
Variable retrieval: not supported

Mtu size:          1500

OUI:               00000c
```

20.1.13 show ethernet oam statistics {pdu | link-monitor | remote-failure}

Syntax

show ethernet oam statistics {**pdu** | **link-monitor** | **remote-failure**} [**interface** *intf-id*]

The command is used to display OAM configuration information on all ports or on a specified port.

Parameter Description

Parameter	Parameter Description
intf-id	Displays the configuration information of the specified port, otherwise the configuration information of all protocol up ports with OAM enabled is displayed.

Default Value

None

Usage Guidelines

None

Example

Display OAM configuration information on ports tg0/0/2.

```
Switch#show ethernet oam statistics pdu interface tg0/0/2
tg0/0/2   Counters:
---------
Information OAMPDU Tx                : 59
Information OAMPDU Rx                : 56
Unique Event Notification OAMPDU Tx   : 0
Unique Event Notification OAMPDU Rx   : 0
Duplicate Event Notification OAMPDU TX: 0 Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU Tx            : 0
Loopback Control OAMPDU Rx           : 0
Variable Request OAMPDU Tx            : 0
Variable Request OAMPDU Rx            : 0
Variable Response OAMPDU Tx           : 0
Variable Response OAMPDU Rx           : 0
Organization Specific OAMPDU Tx       : 0
Organization Specific OAMPDU Rx       : 0
Unsupported OAMPDU Tx                : 0
Unsupported OAMPDU Rx                : 0
Frames Lost due to OAM                : 0
```

20.1.14 show ethernet oam configuration

Syntax

show ethernet oam configuration [**interface** *intf-id*]

The command is used to display OAM runtime information on all ports or on a specified port, including the values of some protocol internal control variables, and the last 10 state transitions of the discovery state.

Parameter Description

Parameter	Parameter Description
intf-id	Displays the runtime information of the specified port, otherwise the runtime information of all protocol up and OAM enabled ports is displayed.

Default Value

None

Usage Guidelines

None

Example

Display OAM runtime information on port tg0/0/2.

```
Switch#show ethernet oam configuration interface tg0/0/2 tg0/0/2
General
-------
Admin state          : enabled
Mode                : active
PDU max rate         : 10 packets/second
PDU min rate         : 1 seconds/packet
Link timeout         : 1 seconds
High threshold action: no action

Remote Failure
--------------
Link fault action     : no action
Dying gasp action     : no action Critical event action: no action

 Remote Loopback
---------------
 Is supported       : supported
 Loopback timeout   : 2
```

```
 Link Monitoring
 ---------------
 Negotiation        : supported
 Status             : on

Errored Symbol Period Event

 Window              : 10 * 100M symbols
 Low threshold       : 1 error symbol(s)
 High threshold      : none

 Errored Frame Event
 Window
 Low       threshold  : 1 seconds
 High threshold       :      1      error
                      frame(s) : none

Errored  Frame Period  Event
Window               : 100 * 14881 frames
Low threshold        : 1 error frame(s)
High threshold       : none

Errored Frame Seconds Summary Event

Window
Low threshold  High threshold

: 60 seconds
: 1 error second(s) : none

Errored CRC  Frames  Event
Window              : 1 seconds
Low threshold        : 10 error frame(s)
High threshold       : none
```

20.1.15 show ethernet oam runtime

Syntax

show ethernet oam runtime [**interface** *intf-id*]

The command is used to display OAM runtime information on all ports or on a specified port, including the values of some protocol internal control variables, and the last 10 state transitions of the discovery state.

Parameter Description

Parameter	Parameter Description
intf- id	Displays the runtime information of the specified port, otherwise the runtime information of all protocol up and OAM enabled ports is displayed.

Default Value

None

Usage Guidelines

None

Example

Display OAM runtime information on port tg0/0/2.

```
Switch#show ethernet oam runtime interface tg0/0/2

 tg0/0/2
 Runtime
 Settings:
-----------------
 local_pdu         :        NOT
                  WORKING
 local_mux         : FWD
 local_par         : FWD
 local_link_stat   : OK
 us
 local_satisfied   : FALSE
 local_stable      : FALSE
 pdu_cnt           : 10
 pdu_timer         : stopped
 lost_link_timer   : stopped
remote_state_valid: FALSE
remote_stable      : FALSE
remote_evaluating  : FALSE Discovery State Machine:
Last 10 state transition recorded: INACTIVE -> FAULT -> ACTIVE_SEND_LOCAL -> SEN D__LOCAL
REMOTE -> SEND_LOCAL_REMOTE_OK -> SEND_ANY -> INACTIVE

------------------------
```

Chapter 21 Port Mirroring Configuration Commands

21.1 Port Mirroring Configuration Commands

21.1.1 mirror

Syntax

[**no**] **mirror session** *session_number* { {**destination interface** *interface-id* { **rspan** *vid*} } | {**source**

interface *interface-id* [, | -] {**rx** | **tx** | **both**} }

To Configure port mirror, run this command.

Parameter Description

Parameter	Parameter Description
session_number	Number of port mirroring Value range: 1-4
destination	Information about destination port mirroring
vid	Remote mirror tag vid
source	Mirroring source of port information
rx / tx / both	Data flow that will be mirrored. Rx means that only the input data is mirrored. tx means that only the output data is mirrored. both means both the input data and the output data are mirrored.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

The unknown unicast packets including the unknown unicast and the broadcast take the source whose mirroring number is 1 as the source port in output mirroring.

Example

Local mirror: The following example shows how to set port tg0/0/2 as the output mirroring of port tg0/0/1.

```
Switch(config)# mirror session 1 destination interface tg0/0/2 Switch(config)# mirror session 1 source interface tg0/0/1 tx
```

Remote mirroring: The following example shows how to set port tg0/0/2 as the local output mirror port of port tg0/0/1, and the remote mirroring VLAN is 100.

```
Switch(config)# mirror session 1 destination interface tg0/0/2 rspan 100 Switch(config)# mirror session 1 source interface tg0/0/1 tx
```

21.1.2 show mirror

Syntax

show mirror [**session** *session_number*]

To display the configuration information about port mirroring, run this command.

Parameter Description

Parameter	Parameter Description
session_number	Number of port mirroring Value range: 1-4

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

This command can be used to display information about port mirroring.

Example

The following example shows how to display the information of port mirroring on port 1.

```
Switch(config)#show mirror session 1 Session 1

Destination Ports: None Source Ports:

RX Only: None

TX Only: None

Both: None
```

Chapter 22 SSH Configuration Commands

22.1 SSH Configuration Commands

22.1.1 ip sshd enable

Syntax

[**no**] **ip sshd enable**

Parameter Description

None

Default Value

ip sshd is disabled by default.

Usage Guidelines

After this configuration command is enabled, it starts Monitoring connections to the ssh server.

Command Mode

Global Configuration Mode

Example

The following example shows how to enable the ssh service.

```
Switch(config)#ip sshd enable
```

22.1.2 ip sshd connections

Syntax

ip sshd connections *maxConnections*

no ip sshd connections

Parameter Description

Parameter	Parameter Description
maxConnections	The maximum number of ssh connections accepted locally, the value range is 1-64.

Default Value

64

Usage Guidelines

To prevent too many users from occupying connection resources, you can configure the maximum number of connections to limit the upper limit of connections.

Command Mode

Global Configuration Mode

Example

The following example shows how to set the maximum number of connections to 10.

```
Switch(config)# ip sshd connections 10
```

22.1.3 ip sshd port

Syntax

ip sshd port *listen-port* **no ip sshd port**

Parameter Description

Parameter	Parameter Description
listen-port	The listen-port number specified by the user is in the range of 1025-65535.

Default Value

22

Usage Guidelines

This command is used to modify the listen-port number of the sshd service.

Command Mode

Global Configuration Mode

Example

The following example shows how to change the listen-port number to 3040:

```
Switch(config)# ip sshd port 3040
```

22.1.4 ip sshd passwordauth

Syntax

[**no**] **ip sshd passwordauth enable**

Parameter Description

None

Default Value

ip sshd passwordauth is disabled by default.

Usage Guidelines

This command is used to enable the password authentication function of the sshd service.

Command Mode

Global Configuration Mode

Example

The following example shows how to enable the password authentication function of the sshd service.

```
Switch(config)# ip sshd passwordauth enable
```

22.1.5 ip sshd pubkeyauth

Syntax

[**no**] **ip sshd pubkeyauth enable**

Parameter Description

None

Default Value

ip sshd pubkeyauth is disabled by default.

Usage Guidelines

This command is used to enable the public key authentication function of the sshd service.

Command Mode

Global Configuration Mode

Example

The following example shows how to enable the public key authentication function of the sshd service.

```
Switch(config)# ip sshd pubkeyauth enable
```

22.1.6 ssh

Syntax

ssh *destIP* **user** *userid* [**port** *port*]

Parameter Description

Parameter	Parameter Description
destIP	Destination IP in dotted decimal notation
userid	User ID on the server
port	The listen-port number, the default value is 22.

Default Value

None

Usage Guidelines

This command is used to establish a connection with a remote ssh server.

Command Mode

EXEC mode, Global Configuration Mode

Example

The following example shows how to establish a connection with the ssh server whose IP address is 192.168.20.41, and the user ID is zmz.

```
Switch#ssh 192.168.20.41 user zmz
```

22.1.7 show ip sshd

Syntax

show ip sshd

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to display the current status of the ssh server on this device.

Command Mode

EXEC mode, Global Configuration Mode

Example

The following example shows how to display the current status of the ssh server on this device.

```
Switch#show ip sshd state: enable

connections: 64 port: 22

PasswordAuthentication: enable PubkeyAuthentication: enable
```

Chapter 23 STP Configuration Commands

23.1 SSTP Configuration Commands

23.1.1 spanning-tree

Syntax

spanning-tree

no spanning-tree

To enable the default spanning-tree protocol mode, run the first one of the above commands.

To disable the spanning tree protocol, run the no form of the first command.

In port configuration mode, the above commands enable or disable STP of the port.

Parameter Description

None

Default Value

RSTP mode is enabled.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Physical port, aggregation port configuration mode.

Example

None

23.1.2 spanning-tree mode sstp

Syntax

spanning-tree mode sstp

no spanning-tree mode

To configure the operating mode of the spanning-tree to be SSTP, run **spanning-tree mode sstp**.

To return to the default setting, use the no form of this command.

Parameter Description

None

Default Value

The default STP mode is RSTP.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command enables SSTP mode.

```
Switch(config)# spanning-tree mode sstp Switch(config)#
```

23.1.3 spanning-tree sstp priority

Syntax

spanning-tree sstp priority *value*

no spanning-tree sstp priority

To configure the SSTP bridge priority, run **spanning-tree sstp priority** *value*.

To return to the default setting, use the no form of the command.

Parameter Description

Parameter	Parameter Description
value	Weight. Value is from 0 to 61440.

Default Value

32768

Usage Guidelines

The device becomes the root of the whole network spanning-tree when configured the priority value. You can set the bridge priority in increments of 4096 only. When you set the priority, valid values are 0, 4096, 8192, 3*4096, 4*4096, ……, 15*4096.

Command Mode

Global Configuration Mode

Example

The following command configures the SSTP priority to be 4096.

```
Switch(config)# spanning-tree sstp priority 4096 Switch(config)#
```

23.1.4 spanning-tree sstp hello-time

Syntax

spanning-tree sstp hello-time *time*

no spanning-tree sstp hello-time

To configure the hello-time delay timer, run **spanning-tree sstp hello-time**.

To return to the default settings, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time	Update time interval. The value is from 1s to 10s.

Default Value

2s

Usage Guidelines

The hello-time configured by the local device is valid only when the local device is the root device.

Command Mode

Global Configuration Mode

Example

The following command configures the BPDU forwarding interval of SSTP is 8s.

```
Switch(config)# spanning-tree sstp hello-time 8 Switch(config)#
```

23.1.5 spanning-tree sstp max-age

Syntax

spanning-tree sstp max-age *time*

no spanning-tree sstp max-age

To configure the SSTP BPDU max-age timer, run **spanning-tree sstp max-age *time.***

To return to the default settings, use the no form of this command.

Parameter Description

Parameter	Parameter Description
seconds	BPDU max survival time. The value is from 6 to 40s.

Default Value

20s

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command configures the max survival time of SSTP to be 24 seconds.

```
Switch(config)# spanning-tree sstp max-age 24 Switch(config)#
```

23.1.6 spanning-tree sstp forward-time

Syntax

spanning-tree sstp forward-time *time*

no spanning-tree sstp forward-time

To set the forward-delay timer, run **spanning-tree sstp forward-time** *time* command.

To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time	The forwarding time delay. The value is from 4 seconds to 30 seconds.

Default Value

15 seconds

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the forward delay timer of SSTP to be 20s.

```
Switch(config)# spanning-tree sstp forward-time 20 Switch(config)#
```

23.1.7 spanning-tree sstp cost

Syntax

spanning-tree sstp cost *value*

no spanning-tree sstp cost

To set the path cost of the interface for SSTP calculations, run **spanning-tree sstp cost** *value* command in interface configuration mode. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
value	Path cost. The values is 1 to 65535.

Default Value

10M Ethernet:100

100M Ethernet: 19

1000M Ethernet: 4

2.5G Ethernet: 2

10G Ethernet: 2

40G Ethernet: 2

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command configures SSTP path cost on port G0/0/1 to be 100:

```
Switch(config-g0/0/1)#spanning-tree sstp cost 100 Switch(config-g0/0/1)#
```

23.1.8 spanning-tree cost

Syntax

spanning-tree cost *value*

no spanning-tree cost

To configure the path cost of the interface for Spanning Tree Protocol (STP) calculations, run **spanning-tree cost *value*** command in interface configuration mode. To return to the default setting, use the ne form of this command.

Parameter Description

Parameter	Parameter Description
value	Path cost. The value is from 1 to 200000000.

Default Value

The default path cost is computed based on the port rate of the interface.

Usage Guidelines

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the path cost of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the path cost of all spanning-tree examples will be updated.

However, the configuration result of the command will not influence the independent configuration in various modes. For example, the switch respectively configured with the spanning-treesstp cost 100 and the spanning-tree cost 110 in SSTP mode, the port path cost will be 100.

Command Mode

Port configuration mode

Example

The following command configures the path cost of g0/0/1 to be 24.

```
Switch(config-g0/0/1)# spanning-tree cost 24 Switch(config-g0/0/1)#
```

23.1.9 spanning-tree sstp port-priority

Syntax

spanning-tree sstp port-priority *value*

no spanning-tree sstp port-priority

To set the priority value in SSTP mode, run **spanning-tree sstp port-priority** *value*. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
value	Port priority. Value is from 0 to 240.

Default Value

128 (0x80)

Usage Guidelines

The port priority must be set in increments of 16 only.

Command Mode

Port configuration mode

Example

The following command sets 32 as the priority value on port g0/0/1:

```
Switch(config-g0/0/1)# spanning-tree sstp port-priority 32 Switch(config-g0/0/1)#
```

23.1.10 spanning-tree port-priority

Syntax

spanning-tree port-priority *value*

no spanning-tree port-priority

To configure the priority of the port in all spanning-tree modes, run **spanning-tree port-priority**. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
value	Port priority. The value is from 0 to 240. The step is 16.

Default Value

Port priority value is 128

Usage Guidelines

The configuration result of this command is valid to all spanning-tree modes. In STP mode, the priority of all VLAN spanning-trees on the interface will be updated. In MSTP mode, the priority of all spanning-tree examples will be updated.

But the configuration result of the command will not influence the independent configuration in various modes. For example, the switch respectively configured with the spanning-treesstp port-priority 128 and the spanning-tree port-priority 48 in SSTP mode, the port priority will be 128.

Command Mode

Port Configuration Mode

Example

The command shows set the priority in all spanning-tree modes on port g0/0/1 to be 16:

```
Switch(config-g0/0/1)#spanning-tree port-priority 16 Switch(config-g0/0/1)#
```

23.1.11 spanning-tree management trap

Syntax

[**no**] **spanning-tree management trap** [**newroot**|**topologychange**]

To enable STP Trap, run the command. To disable STP Trap, use the no form of this command.

Parameter Description

Parameter	Parameter Description
newroot	newRoot Trap type
topologychange	topologyChange Trap type

Default Value

STP Trap is not enabled.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

None

23.2 VLAN STP Configuration Commands

23.2.1 spanning-tree mode pvst

Syntax

spanning-tree mode pvst

no spanning-tree mode

To enable VLAN distribution based STP mode, run **spanning-tree mode pvst.**

To disable the STP mode, use the no form of the command.

Parameter Description

None

Default Value

RSTP

Usage Guidelines

Note: PVST can create 63 instances at most.

Command Mode

Global Configuration Mode

Example

The following command enables PVST on the device.

```
Switch(config)# spanning-tree mode pvst Switch(config)#
```

23.2.2 spanning-tree vlan

Syntax

[**no**] **spanning-tree vlan** *vlan-list*

To designate VLAN distribution spanning-tree instance, run the command.

To delete the designated VLAN spanning-tree, use the no form of this command.

Parameter Description

Parameter	Parameter Description
vlan-list	VLAN list, such as 1,2,3-10,15. The value is from 1 to 4094.

Default Value

OLT can only distribute spanning-tree instances for a certain number of VLAN. By default, the VLAN exceeding the number limit will be automatically add to the STP disabled list.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command first deletes the spanning tree of VLAN10, 11, 15-19 and then distribute the spanning tree for VLAN 40-50:

```
Switch(config)#no spanning-tree vlan 10,11,15-19 Switch(config)#spanning-tree vlan 40-50
Switch(config)#
```

23.2.3 spanning-tree vlan priority

Syntax

spanning-tree vlan *vlan-list* **priority** *value*

no spanning-tree vlan *vlan-list* **priority**

To configure the network bridge priority value of the designated VLAN, run **spanning-tree vlan** *vlan-list* **priority** *value* command.

Parameter Description

Parameter	Parameter Description
vlan-list	VLAN list, such as 1,2,3-10,15. The value is from 1 to 4094.
value	The priority value. The range is 0 to 61440. The step is 4096.

Default Value

By default, the bridge priority of each VLAN spanning tree is 32768 plus the VLAN number.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command configures VLAN1-3. The network bridge priority for 5-10 is 4096.

```
Switch(config)#spanning-tree vlan 1-3,5-10 priority 4096 Switch(config)#
```

23.2.4 spanning-tree vlan forward-time

Syntax

spanning-tree vlan *vlan-list* **forward-time** *value*

no spanning-tree vlan *vlan-list* **forward-time**

To configure the Forward Delay parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan** *vlan-list* **forward-time** *value*.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15
value	Value of the forward-delay parameter. Value range: 4-30 seconds□ Default value: 15 seconds

Default Value

The value of the forward-delay parameter of all VLANs is 15 seconds.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following example shows how to set the forward delay parameter of VLAN 1-3, 5-10 to 19 seconds.

```
Switch(config)#spanning-tree vlan 1-3,5-10 forward-time 19 Switch(config)#
```

23.2.5 spanning-tree vlan max-age

Syntax

spanning-tree vlan *vlan-list* **max-age** *value*

no spanning-tree vlan *vlan-list* **max-age**

To configure the Max Age parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan** *vlan-list* **max-age** *value* . To return to the default value, run **no spanning-tree vlan** *vlan-list* **max-age**.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15. The range is from 1 to 4094.
value	Value of the max-age parameter. Value range: 6-40 seconds Default value: 20 seconds

Default Value

The default value of the max-age parameter for all VLANs is 20 seconds.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the max age parameter of VLAN 1-3, 5-10 to 20 seconds.

```
Switch(config)#spanning-tree vlan 1-3,5-10 max-age 19 Switch(config)#
```

23.2.6 spanning-tree vlan hello-time

Syntax

spanning-tree vlan *vlan-list* **hello-time** *value*

no spanning-tree vlan *vlan-list* **hello-time**

To set the hello time parameter of the spanning tree in the designated VLAN, run **spanning-tree vlan** *vlan-list* **hello-time** *value* . To return to the default setting, run **no spanning-tree vlan** *vlan-list* **hello-time**.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15. The value is from 1 to 4094.
value	Value of the hello time parameter. Value range: 1-10 seconds Default value: 2 seconds

Default Value

The default value of the Hello-Time parameter for all VLANs is 2 seconds.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the Hello Time parameter of VLAN 1-3, 5-10 to 9 seconds.

```
Switch(config)#spanning-tree vlan 1-3,5-10 hello-time 9 Switch(config)#
```

23.2.7 spanning-tree vlan cost

Syntax

spanning-tree vlan *vlan-list* **cost** *value*

no spanning-tree vlan *vlan-list* **cost**

To set the path cost of the spanning tree in the designated VLAN, run **spanning-tree vlan** *vlan-list* **cost** *value*. To return to the default value, run **no spanning-tree vlan** *vlan-list* **cost**.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15. The value is from 1 to 4094.
value	The port path cost. The value is from 1 to 65535.

Default Value

The path cost of a port depends on the port rate.

The value of the path cost of the 10M Ethernet is 100.

The value of the path cost of the 100M Ethernet is 19.

The value of the path cost of the 1000M Ethernet is 1.

The value of the path cost of the 2.5G Ethernet is 2.

The value of the path cost of the 10G Ethernet is 2.

The value of the path cost of the 40G Ethernet is 2.

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command shows how to set the path cost of port G0/0/1 VLAN1-3,5-10 to 100.

```
Switch(config-g0/0/1)#spanning-tree vlan 1-3,5-10 cost 100 Switch(config-g0/0/1)#
```

23.2.8 spanning-tree vlan port-priority

Syntax

spanning-tree vlan *vlan-list* **port-priority** *value*

no spanning-tree vlan *vlan-list* **port-priority**

To set the priority level of the spanning tree in the designated VLAN, run s **spanning-tree vlan** *vlan-list* **port-priority** *value* . To return to the default setting, run **no spanning-tree vlan** *vlan-list* **port-priority**.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15. The value is 1 to 4094.
value	Priority level of a port, which ranges between 0 and 240 and the step is 16.

Default Value

128

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command configures how to set the priority level of port g0/0/1 VLAN1-3,5-10 to 32.

```
Switch(config-g0/0/1)#spanning-tree vlan 1-3,5-10 port-priority 32 Switch(config-g0/0/1)#
```

Chapter 24 RSTP Configuration Commands

24.1 RSTP Configuration Commands

24.1.1 spanning-tree mode rstp

Syntax

spanning-tree mode rstp

no spanning-tree mode

To enable the RSTP function, run **spanning-tree mode rstp**.

To disable the STP, run no spanning-tree mode.

Parameter Description

None

Default Value

RSTP is enabled.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to enable RSTP on the switch.

```
Switch(config)# spanning-tree mode rstp Switch(config)#
```

24.1.2 spanning-tree rstp forward-time

Syntax

spanning-tree rstp forward-time *time*

no spanning-tree rstp forward-time

To configure the forwarding delay of RSTP, run **spanning-tree rstp forward-time** *time* . To resume the default forwarding delay of RSTP, run **no spanning-tree rstp forward-time**.

Parameter Description

Parameter	Parameter Description
time	Time of the forwarding delay. Range: 4-30 seconds

Default Value

15 seconds

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the forwarding delay of RSTP to 20 seconds.

```
Switch(config)# spanning-tree rstp forward-time 20 Switch(config)#
```

24.1.3 spanning-tree rstp hello-time

Syntax

spanning-tree rstp hello-time *time*

no spanning-tree rstp hello-time

To configure the update interval of RSTP, run **spanning-tree rstp hello-time** *time* . To resume the default update interval of RSTP, run **no spanning-tree rstp hello-time**.

Parameter Description

Parameter	Parameter Description
time	Updates the interval. Range: 1-10 seconds

Default Value

2 seconds

Usage Guidelines

The Hello-Time configured on the local switch validates only when the local switch runs as a root switch.

Command Mode

Global Configuration Mode

Example

The following command shows how to set the update interval of RSTP to 8 seconds.

```
Switch(config)# spanning-tree rstp hello-time 8 Switch(config)#
```

24.1.4 spanning-tree rstp max-age

Syntax

spanning-tree rstp max-age *time*

no spanning-tree rstp max-age

To configure the maximum lifespan of the SSTP BPDU, run **spanning-tree rstp max-age** *time*. To resume the default interval time, run **no spanning-tree rstp max-age**.

Parameter Description

Parameter	Parameter Description
time	Maximum interval of the lifespan Range: 6-40 seconds

Default Value

20 seconds

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the maximum lifespan of RSTP to 24 seconds.

```
Switch(config)# spanning-tree rstp max-age 24 Switch(config)#
```

24.1.5 spanning-tree rstp priority

Syntax

spanning-tree rstp priority *value*

no spanning-tree rstp priority

To configure the RSTP priority value, run **spanning-tree rstp priority** *value*. To resume the default value of the RSTP priority value, run **no spanning-tree rstp priority**.

Parameter Description

Parameter	Parameter Description
value	Priority level of the bridge. Value range: 0-61440 Step: 4096

Default Value

None

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the bridge priority of RSTP to 4096.

```
Switch(config)# spanning-tree rstp priority 4096 Switch(config)#
```

24.1.6 spanning-tree rstp cost

Syntax

spanning-tree rstp cost *value*

no spanning-tree rstp cost

To configure the path cost of a port, run **spanning-tree rstp cost** *value* . To resume the default value, run **no spanning-tree rstp cost**.

Parameter Description

Parameter	Parameter Description
value	Value of the path cost. Value range: 1-200000000

Default Value

The path cost depends on the connection rate of the port.

100 Mbps: 200000

1000 Mbps: 20000 2500Mbps:8000

10Gbps:2000 40Gbps:500

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command shows how to set the path cost of port g0/1 to 24:

```
Switch(config-g0/0/1)# spanning-tree rstp cost 24 Switch(config-g0/0/1)#
```

24.1.7 spanning-tree rstp port-priority

Syntax

spanning-tree rstp port-priority *value*

no spanning-tree rstp port-priority

To configure the priority level of a port, run **spanning-tree rstp port-priority** *value*. To resume the default value, run **no spanning-tree rstp port-priority**.

Parameter Description

Parameter	Parameter Description
value	Priority level of a port. Value range: 0-240□ Step: 16

Default Value

128

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command shows how to set the priority level of port g0/0/1 to 16:

```
Switch(config-g0/0/1)# spanning-tree rstp port-priority 16 Switch(config-g0/0/1)#
```

24.1.8 spanning-tree rstp edge

Syntax

spanning-tree rstp edge

no spanning-tree rstp edge

To configure the port to be the edge port, run this command. To return to the default settting, run the no form of this command.

Parameter Description

None

Default Value

Auto-detection

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

None

24.1.9 spanning-tree rstp point-to-point

Syntax

spanning-tree rstp point-to-point {**force-true**|**force-false**|**auto**}

no spanning-tree rstp point-to-point {**force-true**|**force-false**|**auto**}

To set the point-to-point connection of a port to force-truce, force-false or auto, run this command.

Parameter Description

Parameter	Parameter Description
force-true	Sets the point-to-point connection to be forcedly effective.
force-false	Sets the point-to-point connection to be forcedly ineffective.
auto	Sets the point-to-point connection to be automatic check (default).

Default Value

Auto-detection

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

None

24.1.10 spanning-tree rstp migration-check

Syntax

spanning-tree rstp migration-check

To restart checking protocol transfer of RSTP, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

This command is used to restart the protocol transfer check on a port and to change the port in STP-compatible mode to the RSTP mode, enabling RSTP BPDU to be transmitted.

Command Mode

Global and Port Configuration Mode

Example

The following command shows how to check protocol transfer on port g0/0/1.

```
Switch(config-g0/0/1)#spanning-tree rstp migration-check Switch(config-g0/0/1)#
```

Chapter 25 MSTP Configuration Commands

25.1 MSTP Configuration Commands

25.1.1 spanning-tree mode mstp

Syntax

spanning-tree mode mstp

no spanning-tree mode

To set the operation mode of the spanning tree to MSTP, run **spanning-tree mode mstp**. To return to the default set, run **no spanning-tree mode**.

Parameter Description

None

Default Value

MSTP is disabled, while SSTP is enabled.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to enable MSTP on a switch.

```
Switch(config)# spanning-tree mode mstp Switch(config)#
```

25.1.2 spanning-tree mstp name

Syntax

spanning-tree mstp name *string*

no spanning-tree mstp name

To configure the MSTP name, run **spanning-tree mstp name** *string*. To resume the default name, run **no spanning-tree mstp name**.

Parameter Description

Parameter	Parameter Description
string	A character string to configure the name, which contains up to 32 characters and is capital sensitive. Its default value is the MAC address of a switch.

Default Value

Its default value is the MAC address of a switch.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the name of MSTP for a switch to reg-01.

```
Switch(config)# spanning-tree mstp name reg-01 Switch(config)#
```

25.1.3 spanning-tree mstp revision

Syntax

spanning-tree mstp revision *value*

no spanning-tree mstp revision

To configure the MSTP revision number, run **spanning-tree mstp revision** *value* . To resume the default revision number, run **no spanning-tree mstp revision**.

Parameter Description

Parameter	Parameter Description
value	Revision number, which ranges between 0 and 65535 and the default value is 0.

Default Value

The default value of the revision number is 0.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the revision number of MSTP to 100.

```
Switch(config)# spanning-tree mstp revision 100 Switch(config)#
```

25.1.4 spanning-tree mstp instance

Syntax

spanning-tree mstp instance *instance-id* **vlan** *vlan-list*

no spanning-tree mstp instance *instance-id*

To map VLAN to MSTI, run **spanning-tree mstp instance** *instance-id* **vlan** *vlan-list* . To remap VLAN to CIST, run **no spanning-tree mstp instance** *instance-id*.

Parameter Description

Parameter	Parameter Description
instance-id	Instance ID of the spanning-tree, which stands for an MSTI. Value range: 1-63
vlan-list	A VLAN list which is mapped to a spanning tree. Value range: 1-4094

Default Value

All VLANs are mapped to CIST (MST00).

Usage Guidelines

Instance ID is an independent value which stands for an STP instance.

The vlan-list parameter can stand for a VLAN group, such as VLANs 1,2 and3, VLANs 1-5 or VLANs 1,2,5-10.

Command Mode

Global Configuration Mode

Example

The following command shows how to map VLAN2 to STP instance 1, and VLANs 5, 7, 10-20 to STP instance 2 and then remap these VLANs to MST00.

```
Switch(config)# spanning-tree mstp instance 1 vlan 2

Switch(config)# spanning-tree mstp instance 2 vlan 5,7,10-20 Switch(config)# no spanning-tree mstp instance 1

Switch(config)# no spanning-tree mstp instance 2
```

25.1.5 spanning-tree mstp root

Syntax

spanning-tree mstp *instance-id* **root** {**primary**|**secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mstp *instance-id* **root**

To set a designated STP instance to a primary or secondary root, run **spanning-tree mstp** *instance-id* **root** {**primary**|**secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]. To resume the default value of the bridge priority of an STP instance, run **no spanning-tree mstp** *instance-id* **root**.

The diameter command and the hello time command are allowed to modify the network diameter and the hello-time parameter.

Parameter Description

Parameter	Parameter Description
instance-id	Number of the STP instance, which ranges between 0 and 63.
primary	Sets an STP instance to a primary root.
secondary	Sets an STP instance to a secondary root.
net-diameter	An optional parameter which presents the network diameter. When instance-id is 0, net-diameter ranges between 2 and 7.
seconds	An optional parameter standing for the value of the Hello Time parameter, which ranges between 1 and 10 seconds

Default Value

The default value of bridge priority for all STP instances is 32768. The network diameter is 7, while Hello Time is 2 seconds.

Usage Guidelines

The diameter command and the hello-time command validate only when the instance-id parameter is 0.

In general, after the command to set the primary root is executed, the protocol automatically check the bridge ID of the current network's root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance. If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as the secondary root.

Command Mode

Global Configuration Mode

Example

The following command shows how to set a device to the primary root in CIST, and how to recalculate the time parameter of STP through diameter 3 and hello-time 3, and then set the switch to the secondary root in MST01.

```
Switch(config)# spanning-tree mstp 0 root primary diameter 3 hello-time 3 Switch(config)# spanning-tree mstp 1 root secondary
```

25.1.6 spanning-tree mstp priority

Syntax

spanning-tree mstp *instance-id* **priority** *value*

no spanning-tree mstp *instance-id* **priority**

To configure the value of the bridge priority of a designated STP instance, run **spanning-tree mstp** *instance-id* **priority** *value*. To resume the default value of the bridge priority, run **no spanning-tree mstp** *instance-id* **priority**.

Parameter Description

Parameter	Parameter Description
instance- id	Number of the STP instance, which ranges between 0 and 63
value	Value of the bridge priority, which can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440,

Default Value

The default value of the bridge priority for all STP instances is 32768.

Usage Guidelines

The priority values in each STP instance are independent and can be configured independently.

Command Mode

Global Configuration Mode

Example

The following command shows how to set the priority values of a switch in CIST and MST01 to 4096 and 8192 respectively.

```
Switch(config)# spanning-tree mstp 0 priority 4096 Switch(config)# spanning-tree mstp 1 priority 8192
```

25.1.7 spanning-tree mstp hello-time

Syntax

spanning-tree mstp hello-time *seconds*

no spanning-tree mstp hello-time

To configure the Hello Time of MSTP, run **spanning-tree mstp hello-time** *seconds* . To resume the default value of the Hello Time of MSTP, run **no spanning-tree mstp hello-time**.

Parameter Description

Parameter	Parameter Description
seconds	Value range: 1-10 seconds □Default value: 2 seconds

Default Value

2 seconds

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the Hello Time parameter of MSTP to 10.

```
Switch(config)# spanning-tree mstp hello-time 10 Switch(config)# no spanning-tree mstp hello-time
```

25.1.8 spanning-tree mstp forward-time

Syntax

spanning-tree mstp forward-time *seconds*

no spanning-tree mstp forward-time

To configure the forward delay parameter of MSTP, run **spanning-tree mstp forward-time** *seconds*.To resume the default value of the forward delay parameter of MSTP, run **no spanning-tree mstp forward-time**.

Parameter Description

Parameter	Parameter Description
seconds	Value range: 4-30 seconds□. Default value: 15 seconds

Default Value

15 seconds

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the Forward Delay parameter of MSTP to 10.

```
Switch(config)# spanning-tree mstp forward-time 10 Switch(config)# no spanning-tree mstp forward-time
```

25.1.9 spanning-tree mstp max-age

Syntax

spanning-tree mstp max-age *seconds*

no spanning-tree mstp max-age

To configure the max age parameter of MSTP, run **spanning-tree mstp max-age** *seconds* .To resume the default value of the forward delay parameter of MSTP, run **no spanning-tree mstp max-age**.

Parameter Description

Parameter	Parameter Description
seconds	Value range: 6-40 seconds □Default value: 20 seconds

Default Value

20s

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following example shows how to set the max age parameter of MSTP to 10.

```
Switch(config)# spanning-tree mstp max-age 10 Switch(config)# no spanning-tree mstp max-age
```

25.1.10 spanning-tree mstp diameter

Syntax

spanning-tree mstp diameter *net-diameter*

no spanning-tree mstp diameter

To configure the network diameter of MSTP, run **spanning-tree mstp diameter** *net-diameter* . To resume the default value of the network diameter, run **no spanning-tree mstp diameter**.

Parameter Description

Parameter	Parameter Description
net-diameter	Value range: 2-7□ Default value: 7

Default Value

The default value of the network diameter is 7.

Usage Guidelines

The net-diameter parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved. The net-diameter parameter is effective only to CIST. After configuration, the three time parameters of STP are automatically updated to a prior value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the reasonability of the time parameter.

Command Mode

Global Configuration Mode

Example

The following command shows how to set the network diameter of MSTP to 5 and then resume its default value.

```
Switch(config)# spanning-tree mstp diameter 5
Switch(config)# no spanning-tree mstp diameter
```

25.1.11 spanning-tree mstp max-hops

Syntax

spanning-tree mstp max-hops*hop-count*

no spanning-tree mstp max-hops

To set the maximum hops of MSTP BPDU, run **spanning-tree mstp max-hops***hop-count* . To resume the default settings, run **no spanning-tree mstp max-hops**.

Parameter Description

Parameter	Parameter Description
hop-count	Value range: 1-40□ Default value: 20

Default Value

The default value of the maximum hops is 20.

Usage Guidelines

None

Command Mode

Global Configuration Mode

Example

The following command shows how to set the maximum hops of MSTP BPDU to 6 and then resume the default value.

```
Switch(config)# spanning-tree mstp max-hops 6
Switch(config)# no spanning-tree mstp max-hops
```

25.1.12 spanning-tree mstp port-priority

Syntax

spanning-tree mstp *instance-id* **port-priority** *value*

no spanning-tree *instance-id* **port-priority**

To configure the port priority in the designated spanning-tree instance, run **spanning-tree mstp** *instance-id* **port-priority** *value*. To resume the port priority to the default settings, run **no spanning-tree** *instance-id* **port-priority**.

Parameter Description

Parameter	Parameter Description
instance- id	Number of the STP instance, which ranges between 0 and 63.
value	Value of the port priority, which can be one of the following values 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240,

Default Value

The port priority in all STP instances is 128 by default.

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following example shows how to set the priority value of port g0/0/1 in CIST to 16 and then resume the default value.

```
Switch(config-g0/0/1)# spanning-tree mstp 0 port-priority 16
Switch(config-g0/0/1)# no spanning-tree mstp 0 port-priority
```

25.1.13 spanning-tree mstp cost

Syntax

spanning-tree mstp *instance-id* **cost** value

no spanning-tree mstp *instance-id* **cost**

To set the path cost of the spanning tree in the designated STP instance, run **spanning-tree mstp** *instance-id* **cost** value. To resume the default value, run **no spanning-tree mstp** *instance-id* **cost**.

Parameter Description

Parameter	Parameter Description
instance-id	Number of the STP instance, which ranges between 0 and 63
value	Path cost of a port, which ranges between 1 and 200,000,000

Default Value

The path cost depends on the connection rate of the port.

100 Mbps: 200000

1000 Mbps: 20000

2500Mbps:8000

10Gbps:2000

40Gbps:500

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command shows how to set the path cost of port g0/0/1 to 200 in CIST.

```
Switch(config-g0/0/1)# spanning-tree mstp 1 cost 200 Switch(config-g0/0/1)#
```

25.1.14 spanning-tree mstp edge

Syntax

spanning-tree mstp edge

no spanning-tree mstp edge

To configure the MSTP edge of a port, run **spanning-tree mstp edge**.

To resume the connection type to be automatic check, run **no spanning-tree mstp edge**.

Parameter Description

None

Default Value

MSTP will automatically check the edge port by default.

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

None

25.1.15 spanning-tree mstp point-to-point

Syntax

spanning-tree mstp point-to-point {**force-true**|**force-false**|**auto**}

no spanning-tree mstp point-to-point {**force-true**|**force-false**|**auto**}

To configure the connection type of a port, run **spanning-tree mstp point-to-point** {**force-true**|**force-false**|**auto**}. To resume the connection type to auto-check, run **no spanning-tree mstp point-to-point** {**force-true**|**force-false**|**auto**}.

Parameter Description

Parameter	Parameter Description
force-true	Sets the port connection mode to point-to-point.
force-false	Sets the port connection mode to sharing.
auto	Sets the port connection mode to auto-check (the default mode).

Default Value

MSTP will automatically check the port connection mode by default.

Usage Guidelines

None

Command Mode

Port Configuration Mode

Example

The following command shows how to set the connection mode of port g0/0/1 to sharing.

```
Switch(config-g0/0/1)# spanning-tree mstp point-to-point force-false Switch(config-g0/0/1)#
```

25.1.16 spanning-tree mstp mst-compatible

Syntax

[**no**] **spanning-tree mstp mst-compatible**

To enable or disable multiple spanning tree compatible mode, run this command in global configuration mode.

spanning-tree mstp mst-compatible [**enable**|**disable**]

To enable or disable multiple spanning tree compatible mode, run this command in port configuration mode.

Parameter Description

None

Default Value

The compatible mode is not activated by default and the switch cannot establish an area with other switches which transmit BPDU in compatible mode.

Usage Guidelines

After the compatible mode is enabled, you are recommended to set a connected switch which runs other MSTP to the root of CIST, securing that the switch can enter the compatible mode through receiving packets.

Command Mode

Global Configuration Mode，Port Configuration Mode

Example

The following command shows how to activate the MST-compatible mode of a switch in global configuration mode.

```
Switch(config)#spanning-tree mstp mst-compatible
```

The following command shows how to activate the MST-compatible mode of a switch in the port configuration mode.

```
Switch(config-g0/0/1)#spanning-tree mstp mst-compatible enable
```

25.1.17 spanning-tree mstp migration-check

Syntax

spanning-tree mstp migration-check

To remove the STP information which is checked on a port and then restart the protocol transform process, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

Global Configuration Mode，Port Configuration Mode

Example

The following commands shows how to conduct the protocol transfer check on all ports and then conduct the second protocol transfer check on port g0/0/1.

```
Switch(config)# spanning-tree mstp migration-check Switch(config)# interface g0/0/1
Switch(config-g0/0/1)# spanning-tree mstp migration-check
```

25.1.18 spanning-tree mstp restricted-role

Syntax

[**no**] **spanning-tree mstp restricted-role**

To eanble/disable the restricted-role of the port, run the command.

Parameter Description

None

Default Value

Diable the restricted-role of the port.

Usage Guidelines

Enable the restricted-role to enable the port not be selected as the root port.

Command Mode

Port Configuration Mode

Example

None

25.1.19 spanning-tree mstp restricted-tcn

Syntax

[**no**] **spanning-tree mstp restricted-tcn**

To enable/disable TCN restrict of the port, run the command.

Parameter Description

None

Default Value

TCN restrict of the port is disabled.

Usage Guidelines

Enabling TCN restriction on a port prevents the port from propagating topology changes to other ports.

Command Mode

Port Configuration Mode

Example

None

Chapter 26 Check STP Information

26.1 STP Display Information Commands

26.1.1 show spanning-tree

Syntax

show spanning-tree

To display spanning-tree information, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

The command is used to display spanning-tree status. The command is available no matter the whatever mode the spanning-tree is.

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
Switch(config)#show spanning-tree  Spanning tree enabled protocol SSTP SSTP
Root ID Priority 32768  Address 00E0.0FCC.F775  This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32768
Address 00E0.0FCC.F775
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Pri.Nbr Type
 ---------------- ---- --- --------- ------- --------------------------------
G0/0/1 Desg FWD 19 128.16 P2p Switch(config)#
```

26.1.2 show spanning-tree detail

Syntax

show spanning-tree detail

To display the details of the current operating spanning-tree status, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
  Switch(config)#show spanning-tree detail SSTP (running)
Bridge priority 32768, address BC60.6B45.D701(sysid 4095) Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not Set, detected flag not Set Number of topology changes 0
Times:  hold 1, topology change 35, notification 4 hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (g0/0/1) of SSTP is Desg Forwarding
Port path cost 2, Port priority 128, Port Identifier 128.1   Designated root has priority 32768, address BC60.6B45.E001   Designated bridge has priority 32768, address BC60.6B45.E001
Designated port id is 128.1, designated path cost 0
Timers: message age 0, forward delay 15, hold 1 Number of transitions to forwarding state: 1
  last transitions occurred 00:00:02 ago BPDU: sent 17, received 1
```

26.1.3 show spanning-tree interface

Syntax

show spanning-tree interface *intf-i*

To show the spanning-tree of the port, run the command.

Parameter Description

Parameter	Parameter Description
intf-i	Port name. For example, G0/0/1.

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

Switch(config)#show spanning-tree interface tg0/0/1

```
Port 1 (tg0/0/1) of SSTP is Desg Forwarding

Port path cost 2, Port priority 128, Port Identifier 128.1  Designated root has priority 32768, address BC60.6B45.E001  Designated bridge has priority 32768, address BC60.6B45.E001
Designated port id is 128.1, designated path cost 0

Timers: message age 0, forward delay 15, hold 1 Number of transitions to forwarding state: 1

  last transitions occurred 00:00:02 ago BPDU: sent 17, received 1
```

26.1.4 show spanning-tree diag-interface

Syntax

show spanning-tree diag-interface *intf-i*

To display the spanning-tree port diagnosis information, run the command.

Parameter Description

Parameter	Parameter Description
intf-i	Port name, for example tg0/0/1.

Default Value

None

Usage Guidelines

Port diagonosis information (only as a reference to the R&D)

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
Switch(config)#show spanning-tree diag-interface tg0/0/1
tg0/0/1, Flags (0x00030000), State (1, 1, 0) VLANs: 1
```

26.1.5 show spanning-tree state

Syntax

show spanning-tree state

To show the diagnois information of the spanning-tree current operating status, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

Global diagonois information (only as a reference to the R&D)

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
Switch(config)#show spanning-tree state
SpanningTree Protocol Version 0.0.1

State: active, Running Time: 00:24:17 (1457 seconds) Global Words:
  Control: 0x04081001(0x18C6170), Lock: 0 Current Mode: 802.1D Spanning Tree
Ports:
  Allocated: 54, LinkUp: 2 Mode Changed: 3
SSTP 1, PVST 0, RSTP 1, MSTP 0, NONE 1
  ( R S ) BPDU:
Total-received: 691, Task-forwarded: 0 Error-discarded: 0, Terminated: 0
Transmited: 697 (PVST 0), Received: 691 (PVST 0)
  Forwarded: 0  System Control:
  Port-Stat: 283 (0, idle), Topo-Chg: 5, Vlan-Mapping: 5 VLAN Maps:
System: 1-2,10 SSTP: 1-4094
Send: 1-2,10
Hotswap: 0, State: halte
```

26.1.6 show spanning-tree statistics

Syntax

show spanning-tree statistics

To show the statistics information of the spanning-tree operating status, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
Switch(config)#show spanning-tree statistics SpanningTree Protocol Statistics
Running Time: 00:20:39 (1239 seconds) Current Mode: 802.1D Spanning Tree
Ports:
  Allocated: 54, LinkUp: 2 Mode Changed: 3
SSTP 1, PVST 0, RSTP 1, MSTP 0, NONE 1 ( R S )
BPDU:
Total-received: 582, Task-forwarded: 0 Error-discarded: 0, Terminated: 0
Transmited: 588 (PVST 0), Received: 582 (PVST 0)
Forwarded: 0
System Control:
Port-Stat: 283 (0) Topo-Chg: 5, Vlan-Mapping: 5
```

26.1.7 show spanning-tree vlan

Syntax

show spanning-tree vlan *vlan-list* [**detail**]

To check the state of the spanning tree in the designated VLAN, run the command.

Parameter Description

Parameter	Parameter Description
vlan-list	List of the VLAN numbers, such as 1,2,3-10,15. The range is 1 to 4094.
detail	Optional parameter, display the detailed information about the state of the spanning tree.

Default Value

None

Usage Guidelines

In the spanning-tree mode besides pvst, it shows none.

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
The following commands show how to check the spanning tree of VLAN 1-2.

Switch(config)#show spanning-tree vlan 1-2 Spanning tree enabled protocol PVST

VLAN0001

Root ID Priority 32769  Address 00E0.0FCC.F775  This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 Address 00E0.0FCC.F775

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Pri.Nbr Type

---------------- ---- --- --------- ------- --------------------------------
```

```
G0/0/1 Desg FWD 19 128.1 P2p VLAN0002

Root ID Priority 32770  Address 00E0.0FCC.F775  This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32770

Address 00E0.0FCC.F775

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Pri.Nbr Type

---------------- ---- --- --------- ------- --------------------------------

G0/0/1 Desg FWD 19 128.1 P2p Switch(config)#
```

26.1.8 show spanning-tree pvst

Syntax

show spanning-tree pvst {*instance-list*}

To display pvst information, run the command.

Parameter Description

Parameter	Parameter Description
instance-list	(compulsory parameter) Displays pvst instances and vlan corresponding information

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

```
Switch(config)#show spanning-tree pvst instance-list PVST Instance List:

Instance     VLAN ID(s)
 ------------     ------------

Forbided(0) 1 2 3 4 5 6 7 8 9

10



1

2

3
```

4

5

6

7

8

9

10

26.1.9 show spanning-tree mstp

Syntax

show spanning-tree mstp [**instance** *instance-id*]

To check MSTP information, and display all spanning tree instance information withou the instance sub-command, run the command.

Parameter Description

Parameter	Parameter Description
instance-id	Spanning tree instance number, ranges from 0 to 63.

Default Value

None

Usage Guidelines

The command can be used in monitor mode, global configuration mode, and port mode.

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

The following commands show how to check the example of spanning tree instance, among which "MST00" means CIST and "Type" means the connection type corresponding to the port.

```
Switch\#show spanning-tree mstp MST00 Vlans Mapped: 1,4-4094

Bridge Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0) Root This bridge is the CIST and regional root

Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20 Root Times Hello Time 2, Forward Delay 15, Max Age 20

Interface Role Sts Cost Pri.Nbr Type

 ---------------- ---- --- --------- ------- --------------------------------

G0/0/1 Desg FWD 200000 128.1 P2p  G0/0/2 Desg FWD 200000 128.2 Edge MST01 Vlans Mapped: 2

Bridge Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1) Root This bridge for MST01

Interface Role Sts Cost Pri.Nbr Type
```

```
---------------- ---- --- --------- ------- --------------------------------

G0/0/1 Desg FWD 200000 128.1 P2p MST02 Vlans Mapped: 3

Bridge Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2) Root This bridge for MST02

Interface Role Sts Cost Pri.Nbr Type

---------------- ---- --- --------- ------- --------------------------------

G0/0/1 Desg FWD 200000 128.1 P2p
```

26.1.10 show spanning-tree mstp region

Syntax

show spanning-tree mstp region

To check the domain configuration information of the MSTP protocol, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

The "MST Config Table" below shows the correspondig relationship between VLAN and STP.

```
Switch(config)# show spanning-tree mstp region MST Region:
Name: [reg01] Revision:[0]  Role: [Root]

MST Config Table: Instance VLAN IDs
 ---------- ----------
0 1,4-4094
1 2
2 3
```

26.1.11 show spanning-tree mstp region config-digest

Syntax

show spanning-tree mstp region config-digest

To check the domain configuration abstract information of MSTP, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

As shown below, "Format selector" is the fixed field, stands for adopting the configuration tag format specified by the MSTP protocol; " Revision level" is the domain revision number (see 3.13 for details).

```
switch(config)#show spanning-tree mstp region config-digest Format selector:  0
Config name     :  reg01 Revision level  :  0
Config digest   :  B41829F9030A054FB74EF7A8587FF58D
```

26.1.12 show spanning-tree mstp detail

Syntax

show spanning-tree mstp detail

To check the details of MSTP, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

The following example shows how to check the details of STP and list the connection type of the port and the optional characteristics.

```
Switch\#show spanning-tree mstp detail MST00 Vlans Mapped: 1,4-4094

Bridge Address 00E0.0F64.8365 Priority 32768 (32768 mst-id 0) Root This bridge is the CIST and regional root

Configured Hello Time 2, Forward Delay 15, Max Age 20, Max Hops 20

Root Times Hello Time 2, Forward Delay 15, Max Age 20 GigaEthernet0/0/1 of MST00 is designated forwarding  Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.1 Edge Port: disabled Link Type: point-to-point (auto)
```

Bpdu Guard: disabled (default) Root Guard: disabled (default) Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec Number of transitions to forwarding state: 1

Bpdu sent 335, received 5

GigaEthernet0/0/2 of MST00 is designated forwarding Port Info Port ID 128.47 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0

CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0

Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.2 Edge Port: enabled (auto) Link Type: point-to-point (auto)

Bpdu Guard: disabled (default) Root Guard: disabled (default) Loop Guard: disabled (default)

Timers: message expires in 0 sec, forward delay 0 sec, up time 1485 sec Number of transitions to forwarding state: 1

Bpdu sent 744, received 0 MST01 Vlans Mapped: 2

Bridge Address 00E0.0F64.8365 Priority 32769 (32768 mst-id 1) Root This bridge for MST01

GigaEthernet0/0/1 of MST01 is designated forwarding Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32769 Port ID 128.1 Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1 MST Config Message transmitted 335, received 0 MST02 Vlans Mapped: 3

Bridge Address 00E0.0F64.8365 Priority 32770 (32768 mst-id 2) Root This bridge for MST02

GigaEthernet0/0/1 of MST02 is designated forwarding Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32770 Port ID 128.1 Timers: message expires in 0 sec, forward delay 0 sec, up time 662 sec

Number of transitions to forwarding state: 1 MST Config Message transmitted 335, received 0

26.1.13 show spanning-tree mstp interface

Syntax

show spanning-tree mstp interface *interface-id*

To check MSTP protocol port information, run the command.

Parameter Description

Parameter	Parameter Description
interface-id	Port name, such as "G0/0/1" and "GigaEthernet0/0/2".

Default Value

None

Usage Guidelines

None

Command Mode

EXEC Mode, Global Configuration Mode, Port Configuration Mode

Example

The following example shows how to check the G0/0/1 information with the command.

```
Switch\#show spanning-tree mstp interface g0/0/1
GigaEthernet0/0/1 of MST00 is designated forwarding Port Info Port ID 128.1 Priority 128 Cost 200000
Designated Root Address 00E0.0F64.8365 Priority 32768 Cost 0
CIST Regional Root Address 00E0.0F64.8365 Priority 32768 Cost 0
Designated Bridge Address 00E0.0F64.8365 Priority 32768 Port ID 128.1 Edge Port: disabled Link Type: point-to-point (auto)
Bpdu Guard: disabled (default) Root Guard: disabled (default) Loop Guard: disabled (default)
```

Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec Number of transitions to forwarding state: 1

Bpdu sent 430, received 5

GigaEthernet0/0/1 of MST01 is designated forwarding Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32769 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32769 Port ID 128.1 Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1

MST Config Message transmitted 430, received 0

GigaEthernet0/0/1 of MST02 is designated forwarding Port Info Port ID 128.1 Priority 128 Cost 200000

Designated Root Address 00E0.0F64.8365 Priority 32770 Cost 0

Desingated Bridge Address 00E0.0F64.8365 Priority 32770 Port ID 128.1 Timers: message expires in 0 sec, forward delay 0 sec, up time 851 sec

Number of transitions to forwarding state: 1 MST Config Message transmitted 430, received 0 Instance Role Sts Cost Pri.Nbr Vlans Mapped

-------- ---- --- --------- ------- --------------------

0 Desg FWD 200000 128.1 1,4-4094

1 Desg FWD 200000 128.1 2

2 Desg FWD 200000 128.1 3

26.1.14 show spanning-tree mstp protocol-migration

Syntax

show spanning-tree mstp protocol-migration

To check the protocol transfer information of the MSTP port, run the command.

Parameter Description

None

Default Value

None

Usage Guidelines

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Example

The following example shows how to check port protocol transfer with the command, among which port G0/0/1 has been transferred to 802.1D STP mode.

```
Switch\#show spanning-tree mstp protocol-migration

MSTP Port Protocol Migration Interface Protocol

 ---------------- ---------- ------------

G0/0/1 802.1D
```

Chapter 27 DHCP Sever Configuration Commands

27.1 DHCPD Configuration Commands

27.1.1 ip dhcpd pool

Syntax

ip dhcpd pool *name*

Parameter Description

Parameter	Parameter Description
name	The name of the DHCP address pool

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

You can use this command to increase the DHCP address pool named name and enter the DHCP address pool configuration mode.

Example

The following command adds a DHCP address pool named test123 and enters the DHCP address pool configuration mode:

```
ip dhcpd pool test123
```

27.1.2 ip dhcpd enable

Syntax

ip dhcpd enable

Parameter Description

None

Default Value

If the Default Value is used, the DHCP service is disabled.

Command Mode

Global Configuration Mode

Usage Guidelines

Users can use this command to enable the DHCP service.

Note that DHCP Server and DHCP Relay share the same UDP 67 port for sending and receiving, so you need to choose one of the two functions.

Example

The following command enables the DHCP Server service:

```
ip dhcpd enable
```

Related Command

ip dhcpd pool *name*

27.1.3 ip dhcpd export

Syntax

ip dhcpd export

Parameter Description

The current DHCP server configuration is displayed.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Used to display the current DHCP server configuration.

Example

None

Related Command

None

27.1.4 ip dhcpdip-bind

Syntax

ip dhcpdip-bind *ip-addr* **mac** *mac-addr*

no ip dhcpdip-bind {*ip-addr*|*all*}

Parameter

Parameter	Parameter Description
ip-addr	IP address
mac-addr	Client hardware address
all	All records are bound and used only for the no command.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Users can use this command to configure the binding relationship between IP address and MAC address. If the IP address is not in all address pools, the binding is invalid.

Example

The following command sets the address of IP 192.168.11.2 to be bound to the client hardware address, and its MAC address is AA:BB:CC:DD:EE:FF:

```
ip dhcpd ip-bind 192.168.11.2 mac aa:bb:cc:dd:ee:ff
```

27.2 DHCPD Address Pool Configuration Commands

Note: Each address pool needs to be configured with five basic configuration commands: network, range, gateway, DNS, and lease, and the address pool is in the enable state.

27.2.1 network

Syntax

network *ip-addr netmask*

Parameter Description

Parameter	Parameter Description
ip-addr	The network address of the address pool used for automatic assignment.
netmask	Subnet mask

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

Users can use this command to configure the network address for the address pool to be used for auto-assignment, and this command is only used for the auto-assignment mode.

When you run this command, make sure that the network number of the IP address of the interface on the interface receiving DHCP packets is the same as the network number of the network address in the pool network. Otherwise, the address pool does not take effect.

Example

Set the network number address of the DHCP address pool to 192.168.20.0 and the subnet mask to 255.255.255.0 in the DHCP address pool.

```
network 192.168.20.0 255.255.255.0
```

27.2.2 range

Syntax

range *lowaddr-highaddr* [,*lowaddr-highaddr*,[*lowaddr-highaddr*...]]

Parameter Description

Parameter	Parameter Description
lowaddr	The starting address used to automatically assign an address zone.
highaddr	A termination address for the automatic assignment of address zones.
Note: A maximum of 10 CIDR blocks can be configured	

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

Users can use this command to configure address zones for auto-allocation, each address pool can have up to 10 address ranges, separated by commas, and each range must be within the network range and do not coincide with each other. This command is only used for auto-assignment methods.

Example

Run the following command to set the address allocation region of the DHCP address pool from 192.168.20.210 to 192.168.20.219:

```
range 192.168.20.210-192.168.20.219
```

The following command configures the multiple address allocation zones of the DHCP address pool as 192.168.20.210-192.168.20.219 and 192.168.20.110-192.168.20.119.

```
range 192.168.20.210-192.168.20.219,192.168.20.110-192.168.20.119
```

27.2.3 gateway

Syntax

gateway *ipaddr* [,*ipaddr*]

Parameter Description

Parameter	Parameter Description
ipaddr	The Default Value route assigned to the client, which is the gateway address.
Note: A maximum of 2 gateway addresses can be configured.	

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to configure the Default Value routes assigned to the client, up to 2 Default Value routes, separated by commas.

Example

The following command configures the Default Value route assigned to the DHCP client to 192.168.20.1.

```
gateway 192.168.20.1
```

The following command configures multiple Default Value routes assigned to the DHCP client as 192.168.20.1 and 192.168.20.2.

```
gateway 192.168.20.1,192.168.20.2
```

27.2.4 dns

Syntax

dns *ipaddr* [,*ip-addr*]

Parameter Description

Parameter	Parameter Description
ipaddr	The DNS server address assigned to the client.
Note: You can configure up to 2 DNS server addresses.	

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to configure the DNS server addresses assigned to the client, up to 2 DNS servers, separated by commas.

Example

The following command sets the DNS server address assigned to the client 192.168.1.3.

```
dns 192.168.1.3
```

The following command configures the multiple DNS server addresses assigned to the client as 192.168.1.3 and 8.8.8.8

```
dns 192.168.1.3,8.8.8.8
```

27.2.5 domain

Syntax

domain *name*

Parameter Description

Parameter	Parameter Description
name	The domain name assigned to the client.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to configure the domain name assigned to the client.

Example

The following command sets the domain name assigned to the client test.domain:

```
domain test.domain
```

27.2.6 lease

Syntax

lease {*days hours minutes*|*infinite*}

Parameter Description

Parameter	Parameter Description
days	The number of days the address is allocated
hours	The number of hours assigned by the address
minutes	The number of minutes assigned by the address
infinite	Addresses are permanently assigned
Note: lease 0 0 0 is configured for None.	

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to configure the lease time for an address assigned to a client.

Example

The following command sets the time limit for assigning an address to a client of 2 days and 12 hours.

```
Lease 2 12 0
```

27.2.7 specificInfo

Syntax

specificInfo *cisco ipaddr* [*ipaddr*]

Parameter Description

Parameter	Parameter Description
cisco	Configure option 43 in Cisco format, deliver AC addresses.
ipaddr	A maximum of two IP addresses can be delivered from Option 43.

Default Value

None

Command Mode

DHCP address pool configuration mode

Usage Guidelines

The DHCP Server reply packet contains option 43, which is the IP address of the AC in the AC/AP environment.

Example

Command the following command to deliver the AC address 192.168.111.112 to the client:

```
specificInfo cisco 192.168.111.112
```

27.2.8 enable

Syntax

enable

Parameter Description

None

Default Value

enable

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to enable the address pool and make it valid.

Example

None

27.2.9 disable

Syntax

disable

Parameter Description

None

Default Value

Enable

Command Mode

DHCP address pool configuration mode

Usage Guidelines

You can use this command to shut down the address pool and invalidate it.

Example

None

27.3 DHCPD Management Commands

27.3.1 show ip dhcpd pool

Syntax

show ip dhcpd pool

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to display all address pool information for DHCPD.

Example

None

27.3.2 show ip dhcpd pool-conf

Syntax

show ip dhcpd pool-conf

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to display the address pool configuration for DHCPD.

Example

None

27.3.3 show ip dhcpdip-bind

Syntax

show ip dhcpdip-bind

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to display the configuration of the IP address binding for DHCPD.

Example

None

27.3.4 show ip dhcpd state

Syntax

show ip dhcpd state

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to display the operational status of DHCPD.

Example

None

27.3.5 show ip dhcpd leases

Syntax

show ip dhcpd leases

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to display the status of the leases that DHCPD has been assigned.

Example

None

27.3.6 show ip dhcpd statistic

Syntax

show ip dhcpd statistic

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

You can use this command to display statistics on packets sent and received by the DHCP server.

Example

None

27.3.7 Debug dhcpd error

Syntax

debug dhcpd error

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to enable the foreground to display the debug information of the DHCP server.

Example

None

Chapter 28 DHCP Relay Configuration Commands

28.1 DHCP Relay Configuration Commands

28.1.1 ip dhcpr enable serverIP

Syntax

ip dhcpr enable serverIP *ipaddr*

Parameter Description

Parameter	Parameter Description
ipaddr	The IP address of the uplink DHCP server

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Enable the DHCP relay function and specify the IP address of the uplink DHCP server.

Note: DHCP Relay and DHCP Server on the device use the same communication port UDP 67, so you can choose one of the two functions and cannot use them at the same time.

Example

The device uses the DHCP Relay function and specifies the IP address of the DHCP server on the uplink port as 192.168.2.1.

```
Ip dhcpr enable serverIP 192.168.2.1
```

28.1.2 ip dhcpr export

Syntax

ip dhcpr export

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to display the current DHCP Relay configuration.

Example

None

28.1.3 show ip dhcpr

Syntax

show ip dhcpr

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The configured DHCP trunk configuration that can be displayed using this command can be output in json format.

Example

None

28.1.4 debug dhcpr error

Syntax

debug dhcpr error

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

Users can use this command to enable the foreground to output the debug information of DHCP Relay.

Example

None

Chapter 29 ERPS Configuration Commands

29.1 Global Configuration Commands

29.1.1 erps

Syntax

To set an instance of ring and enter the node mode, run the following command:

erps *id*

To cancel an instance of ring, run the following command:

no erps *id*

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

By default, the ring node instance is not configured.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)# erps 1 Switch(config_ring1)#
```

Related Command

None

29.1.2 control-vlan

Syntax

To set the control vlan value of the local node, run the following command:

control-vlan *value*

Parameter Description

Parameter	Parameter Description
value	The value ranges from 1 to 4094.

Default Value

vlan 1

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

The command is the compulsory option for the node configuration. The node cannot be modified after it works well.

Example

```
Switch(config)# erps 1 Switch(config_ring1)#
Switch(config_ring1)# control-vlan 2
```

Related Command

None

29.1.3 wtr-time

Syntax

To configure the timeout time of the WTR timer, run the following command:

wtr-time *value*

Parameter Description

Parameter	Parameter Description
value	The timeout time of WTR is 20s by default. The value ranges from 10 to 720s.

Default Value

The timeout time of WTR is 20s by default.

Command Mode

Ethernet ring node configuration mode

Usage Guidelines

None

Example

```
Switch(config)# erps 1 Switch(config_ring1)#
Switch(config_ring1)# wtr-time 15
```

Related Command

None

29.1.4 guard-time

Syntax

To configure the timeout time of the Guard timer, run the following command:

guard-time *value*

Parameter Description

Parameter	Parameter Description
value	The timeout time of the Guard timer. Unit: 1ms. The default is 500. The value ranges from 10 to 2000.

Default Value

The timeout time of the Guard timer is 500 milliseconds by default.

Command Mode

Node configuration mode for the Ethernet ring.

Usage Guidelines

When a port is recovered from an invalid state, the Guard timer is forbidden to handle the received protocol packets to avoid outdated packets from generating inaccurate protocols.

Example

```
Switch(config)# erps 1
Switch(config_ring1)# guard-time 60
```

Related Command

None

29.1.5 send-time

Syntax

To set the interval of transmission of the protocol packets, run the following command:

send-time *value*

Parameter Description

Parameter	Parameter Description
value	The timeout time of the timer. The default value is 5 seconds. The value ranges from 1 to 10 seconds.

Default Value

By default, ERPS PDU is transmitted every five seconds.

Command Mode

Node configuration mode for the Ethernet ring

Usage Guidelines

None

Example

```
Switch(config_ring1)# wtr-time 15

Switch(config_ring1)# send-time 5
```

Related Command

None

29.2 Port Configuration Commands

29.2.1 erps ring-port

Syntax

To set a port to be a common ring port, run the following command:

erps *id* **ring-port**

To delete the common ring port or the ring configuration on the RPL port, run the following command:

no erps *id* **ring-port**

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

ERPS can set a physical or aggregation port to be a ring port. However, the physical port where link aggregation, 802.1X or port security has been configured can not be set to be an ERPS ring port.

The default VLAN for each ring port must be configured to be consistent so that ERPS packets can be normally forwarded.

Example

```
Switch(config)# interface tg0/0/1
Switch(config-tg0/0/1)# erps 1 ring-port
```

Related Command

None

29.2.2 erps rpl

Syntax

To set a port to be a RPL (ring protection link) port of ERPS, run the following command:

erps *id***rpl**

To delete the RPL port and retain its role as a common ring port, run the following command:

no erps *id***rpl**

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

In case of automatic discovery, the function of the erps rpl command is as same as the priority value is modified to 0.

If you want to delete the ring settings of the port, run the following command.

```
no erps id ring-port
```

Example

```
Switch(config)# interface tg0/0/3
Switch(config-tg0/0/3)# erps 1 rpl
```

Related Command

None

29.2.3 erps neighbour

Syntax

If you want to delete the ring settings of the port, run the following command.

erps *id* **neighbour**

To return to the default setting, use the no form of this command.

no erps *id* **neighbour**

Parameter Description

Parameter	Parameter Description
id	ID of the node

Default Value

None

Command Mode

Configuration mode of the switching port (physical port or aggregation port)

Usage Guidelines

Set a port to be RPL of a designated node. Meanwhile, the port must be connected to the RPL port and become the RPL neighbor port.

Example

```
Switch(config)# interface tg0/0/3
Switch(config-tg0/0/3)# erps 1 neighbour
```

Related Command

None

29.3 Control Commands

29.3.1 erps [ForcedSwitch | ManualSwitch | Clear]

Syntax

To force the node switch to the interface *interface-type interface-number*, run the following command:

erps *id* **ForcedSwitch interface** *interface-type interface-number*

To force the node switch to the interface *interface-type interface-number* manually, run the following command:

erps *id* **ManualSwitch interface** *interface-type interface-number*

To clear the switch command of the node, run the following command:

erps *id* **Clear**

Parameter Description

Parameter	Parameter Description
id	ID of the node
interface-type	Type of the interface
interface-number	Number of the interface

Default Value

None

Command Mode

Monitor mode

Usage Guidelines

None

Example

None

Related Command

None

29.4 Show Configuration Commands

29.4.1 show erps

Syntax

To show the abstract information of the ERPS, run the following command:

show erps [*id*]

To show the detailed information of the Ethernet ring node, run the following command:

show erps *id* **detail**

To show the information of the Ethernet interface, run the following command:

show erps interface *intf-name*

Parameter Description

Parameter	Parameter Description
id	ID of the node
intf-name	Interface name

Default Value

None

Command Mode

Monitor mode, global configuration mode, node configuration mode or port configuration mode

Usage Guidelines

None

Example

None

Related Command

None

Chapter 30 IGMP-SNOOPING Configuration Commands

IGMP-SNOOPING configuration commands include：

- ipigmp-snooping
- ipigmp-snooping immediate-leave
- ipigmp-snooping mrouter-multi-vlan
- ipigmp-snooping mrouter interface multi-vlan
- ipigmp-snooping mc-vlan
- ipigmp-snooping proxy enable
- ipigmp-snooping proxy last-member-query
- ipigmp-snooping dlf-drop
- ipigmp-snooping router age
- ipigmp-snooping response time
- ipigmp-snooping querier
- ipigmp-snooping querier timer
- show ipigmp-snooping
- show ipigmp-snooping timer
- show ipigmp-snooping group
- show ipigmp-snooping group interface
- show ipigmp-snooping statistics
- show ipigmp-snooping mc-vlan-xlate
- show ipigmp-snooping vlan
- debug ipigmp-snooping packet
- debug ipigmp-snooping timer
- debug ipigmp-snooping event
- debug ipigmp-snooping error
- debug ipigmp-snooping

30.1 igmp-snooping

Syntax

ipigmp-snooping { [vlan *vlan_id* **] | [enable] }**

no ipigmp-snooping { [vlan vlan_id] | [enable] }

To enable the IGMP-snooping of VLAN, use the ip igmp-snooping command. Use the no form of this command to restore the default.

Parameter Description

Parameter	Parameter Description
vlanid	VLAN identity. Value ranges from 1 to 4094.

Default Value

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

If not specified the vlan parameter, this command enable or disable all vlans in the system (IGMP-snooping currently can be ran on 16 vlans at most at the same time.)

Example

The following command enables IGMP snooping of VLAN 1:

```
Switch(config)# ipigmp-snooping vlan 1
Switch(config)#
```

30.1.1 igmp-snooping immediate-leave

Syntax 1

In the global configuration mode:

ipigmp-snooping vlan *vlan_id* **immediate-leave**

no ipigmp-snooping vlan *vlan_id* **immediate-leave**

To configure the immediate-leave characteristic of vlan, use the ip igmp-snooping vlan command. Use the no form of this command to restore the default value.

Parameter Description

Parameter	Parameter Description
vlanid	VLAN ID. Value ranges from 1 to 4094.

Default Value

Disabled

Command Mode

Global Configuration Mode

Syntax 2

In the port configuration mode:

ipigmp-snooping immediate-leave

no ipigmp-snooping immediate-leave

To configure the immediate-leave characteristic of vlan, use the **ipigmp-snooping immediate-leave** command. Use the no form of this command to restore the default value.

Parameter Description

None

Default Value

Disabled

Command Mode

Port Configuration Mode

Usage Guidelines

Configuring the immediate-leave feature of a VLAN or port allows the switch to delete the port from the port list of the corresponding multicast group immediately after receiving the leave packet on the port, instead of enabling the timer to wait for another host to join the multicast. If other hosts on the same port also belong to the group but do not want to leave, the multicast communication of these users may be affected and the immediate-leave function should not be enabled. The immediate-leave configuration on the port and the immediate-leave configuration in VLAN will take effect simultaneously.

Example

The following command enables the immediate-leave characteristics of VLAN 1.

```
Switch(config)# ipigmp-snooping vlan 1 immediate-leave Switch(config)#
```

The following command enables the immediate-leave of port g0/0/8.

```
Switch(config)_g0/0/8#ip igmp-snooping immediate-leave
```

30.1.2 igmp-snooping mrouter-multi-vlan

Syntax

ipigmp-snooping mrouter-multi-vlan *vlan_id*

no ipigmp-snooping mrouter-multi-vlan *vlan_id*

Parameter

Parameter	Parameter Description
vlanid	VLAN ID. Value ranges from 1 to 4094.

Default Value

None

Usage Guidelines

Must be uplink port

The command is used to configure the static multi-vlan of IGMP-snooping.

Example

The following command configures vlan2000 to IGMP-snooping multi vlan.

```
Switch(config)# ipigmp-snooping mrouter-multi-vlan 2000
Switch(config)#
```

30.1.3 igmp-snooping mrouter interface multi-vlan

Syntax

ipigmp-snooping mrouter interface *intf* **multi-vlan** *vlan_id*

no ipigmp-snooping mrouter interface *intf* **multi-vlan** *vlan_id*

Parameter

Parameter	Parameter Description
vlanid	VLAN ID. Value ranges from 1 to 4094.
intf	interface

Default Value

None

Usage Guidelines

Must be uplink port

The command is used to configure the VALN static route port. Use the no form of this command to delete the route port.

You can configure static routing ports only for existing VLANs.

Example

The following command configure G0/0/1 as IGMP-snooping static multicast router port.

```
Switch(config)# ipigmp-snooping mrouter interface g0/0/1 multi-vlan 2000 Switch(config)#
```

30.1.4 igmp-snooping mc-vlan

Syntax

ipigmp-snooping mc-vlan *vlan_id* **range** *A.B.C.D &<1-n>*

no ipigmp-snooping mc-vlan *vlan_id* **range** *A.B.C.D &<1-n>*

no ipigmp-snooping mc-vlan *vlan_id* Parameter

Parameter	Parameter Description
vlanid	VLAN ID. Value ranges from 1 to 4094.
A.B.C.D	Multicast IP address.

Default Value

None

Usuage Guidelines

This command has two functions: first, only the destination IP address has been added to the report and leave packets of a multicast VLAN can be received by the IGMP snooping protocol. Second, to convert the VLAN tag of the downstream multicast service flow to the multicast VLAN tag. A multicast VLAN can contain multiple consecutive or non-contiguous multicast IP addresses, and a multicast IP address can belong to only one multicast VLAN.

Example

The following command is to add muticast group 225.1.1.1 to the multicast VLAN 2.

```
Switch(config)# ipigmp-snooping mc-vlan 2 range 225.1.1.1
Switch(config)#
```

Note:

224.0.0.0-224.0.0.255 is the non-routable multicast address and cannot be registered on each port.

30.1.5 igmp-snooping proxy enable

Syntax

ipigmp-snooping proxy enable

no ipigmp-snooping proxy enable

To enable the IGMP-snooping proxy, run the above command. To return to the default setting, run the no form of the command.

Parameter

None

Default Value

Disabled

Usage Guidelines

Before enable IGMP-snooping proxy, ensure to enable ipigmp-snooping querier.

Example

The following command enable IGMP-snooping proxy:

```
Switch(config)# ipigmp-snooping proxy enable Switch(config)#
```

30.1.6 igmp-snooping proxy last-member-query count

Syntax

ipigmp-snooping proxy last-member-query [**count** *value1* | **interval** *value2*]

noipigmp-snooping proxy last-member-query ** {count** | **interval**}

Parameter

Parameter	Parameter Description
value1	querier times, 1 to 5.
value2	Query interval, 1 to 60 seconds.

Default Value

Value 1 is 2 by default, and value 2 is 1 by default.

Usage Guidelines

None

Example

The following command confgures last-member-query count to 3 and last-member-query interval to 2.

```
Switch(config)# ipigmp-snooping proxy last-member-query count 3    Switch(config)#ip igmp-snooping proxy last-member-query interval 2 Switch(config)#
```

30.1.7 igmp-snooping dlf-drop

Syntax

ipigmp-snooping dlf-drop

no ipigmp-snooping dlf-drop

Parameter Description

Parameter	Parameter Description
	The command is used to filter the unregistered address group packet.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the switch to filter multicast packets that are not registered with the destination multicast address and restore to the default setting (intra-VLAN broadcasting) with the no form of this command.

Example

The following example shows how to drop the multicast packets with unregistered destination addresses in all VLANs.

```
Switch(config)# ipigmp-snooping dlf-drop
Switch(config)#
```

30.1.8 igmp-snooping router age

Syntax

ipigmp-snooping timer router-age *timer_value*

no ipigmp-snooping timer router-age

Parameter Description

Parameter	Parameter Description
time value	Queries the time of the timer. Value range: 10-2147483647

Default Value

260 seconds

Command Mode

Global Configuration Mode

Usage Guidelines

This command is used to query the time of the timer of IGMP-Snooping. The negative form of this command is used to resume the default value.

Example

The following example shows how to set the query time of the router to 300 seconds.

```
Switch(config)# ipigmp-snooping timer router-age 300 Switch(config)#
```

30.1.9 igmp-snooping response time

Syntax

ipigmp-snooping timer response-time *timer_value*

no ipigmp-snooping timer response-time

To configure the maximum response time of IGMP snooping, run **ipigmp-snooping timer response-time** *timer_value.* To resume the default value of IGMP snooping, run no form of the command.

Parameter Description

Parameter	Parameter Description
time value	Queries the time of the timer. Value range: 1-2147483647

Default Value

15 seconds

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following command shows how to set the query response time of IGMP snooping to 20 seconds.

```
Switch(config)# ipigmp-snooping timer response-time 20 Switch(config)#
```

30.1.10 igmp-snooping querier

Syntax

ipigmp-snooping querier [**address** <*ip_addr*>]

no ipigmp-snooping querier [**address**]

To activate the IGMP-snooping querier mechanism, or set the source IP address of the automatic query packet, run ip igmp-snooping querier [address <ip_addr>]. To resume the default value, run no form of the command.

Parameter Description

Parameter	Parameter Description
ip_addr	IP address of a normal unicast

Default Value

By default, the querier function is not enabled and the source IP address is 10.0.0.200.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following command shows how to activate IGMP Querier to serve as a multicast router if no multicast router is working.

```
Switch(config)# ipigmp-snooping querier
Switch(config)#
```

30.1.11 igmp-snooping querier querier-timer

Syntax

ipigmp-snooping querier querier-timer *time_value*

no ipigmp-snooping querier querier-timer

To configure the forward interval of forwarding query packets by the local querier, run the first one of the above commands. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
time_value	local querier interval

Default Value

When enabling Querier, the time interval is 200s by default.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following command shows how to configure the query period of the local querier to 140s.

```
Switch(config)# ipigmp-snooping querier querier-timer 140 Switch(config)#
```

30.1.12 show ipigmp-snooping

Syntax

show ipigmp-snooping

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is used to display the information about IGMP-snooping configuration.

Example

The following command shows how to display the information of each VLAN where IGMP-snooping is running.

```
Switch(config)# show ipigmp-snooping Global IGMP snooping configuration:


--------------------------------

VLAN nodes : 1-4094 IGMP version : V3

Max src-rec num : 32

Dlf-drop VLAN nodes : 1-4094 Sensitive : Disabled

Querier : Disabled

Querier address : 10.0.0.200 Querier interval : 200s

Router age : 260s

Response time : 15s   Pull-stream : Disabled

Pull-stream address : 10.0.0.200 Report suppression : Disabled

Proxy leave : Disabled IPMC work mode : L2

vlan_id Immediate-leave Ports Router Ports
```

```
------------------------------------------------------------------

1  Disabled 5-10 SWITCH(querier);

50 Disabled 1-4 SWITCH(querier);

100 Disabled NULL SWITCH(querier);G0/0/1(static);

200 Disabled NULL SWITCH(querier);

400 Disabled NULL SWITCH(querier);

500 Disabled NULL SWITCH(querier);

Switch(config)#
```

30.1.13 show ipigmp-snooping timer

Syntax

show ipigmp-snooping timer

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is used to display the information about the IGMP-snooping timer.

Example

The following example shows how to display the information about the IGMP-snooping timer.

```
Switch(config)# show ipigmp-snooping timer
vlan 1 mrouter on port 3 : 251
Switch(config)#
```

30.1.14 show ipigmp-snooping group

Syntax

show ipigmp-snooping group

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is used to display the information about the multicast group of IGMP-snooping.

Example

The following example shows how to display the information about the multicast group of IGMP-snooping.

```
Switch(config)# show ipigmp-snooping group
Total number of groups: 1 Vlan Group Type Port(s)
1000 225.0.0.1 IGMP gpon0/0/2:7 Switch(config)#
```

30.1.15 show ipigmp-snooping group interface

Syntax

show ipigmp-snooping group interface *intf*

Parameter

Parameter	Parameter Description
intf	interface

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to display the IGMP-snooping mutlicast group information of the port.

Example

The following command displays the port gpon0/0/2:7 added igmp-snooping mulicats group information.

```
Switch#show ipigmp-snooping group interface gpon0/0/2:7
Number of joined groups: 1

Vlan Group  Mode Source Num


---- --------------- ------- ----------

1000 225.0.0.1 IGMP gpon0/0/2:7 Switch#
```

30.1.16 show ipigmp-snooping statistics

Syntax

show ipigmp-snooping statistics [message|packet|hardware|vlan *vlanid*]

Parameter Description

Parameter	Parameter Description
vlanid	When the command has the keyword "VLAN", specifiy the VLAN ID.

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to display statistics for IGMP-snooping. Keywords: messge, packet, hardware, and VLAN are optional. If an optional keyword is displayed, the statistics of messages received, packets received, hardware operations, and VLANs of the IGMP-Snooping task are displayed. If there are no optional keywords, the global statistics of messages, packets, and hardware operations are displayed. If you want to use a keyword VLAN, you need to specify the parameter vlanid to display statistics under the VLAN.

Example

The following example shows how to display the information about IGMP-snooping statistics.

```
Switch#show ipigmp-snooping statistics IGMP Snooping Message Statistics

-----------------------------------

L2 main messages sent OK : 305 L2 main messages sent failed : 0 L2 packets received : 302
L2 packets sent : 302
L2 packets sent failed : 0
L2 link-status messages : 3
```

IGMP Snooping messages received: 313

IGMP packet messages received : 302

IGMP Snooping Packet Statistics

Received packets : 302

IGMP packets : 259

M-routing protocol packets : 0

Other packets : 43

Received IGMP general queries : 0

Received IGMPv2 specific queries : 0

Received IGMPv3 g specific queries : 0 Received IGMPv3 gs specific queries: 0 Received IGMPv1 reports : 0

Received IGMPv2 reports : 230

Received IGMP leaves : 0

Received IGMPv3 reports : 29

Flooded queries : 0

Forwarded and proxy-sent reports : 0

Forwarded and proxy-sent leaves : 0

IGMP Snooping Hardware Operation Statistics

Total : 9

Succeeded : 9

Failed : 0

Report/leave processing: 5

Response timer expiring: 4 Group creating/updating: 7

Group deleting : 2

30.1.17 show ipigmp-snooping mc-vlan-xlate

Syntax

show ipigmp-snooping mc-vlan-xlate

Parameter

None

Default Value

None

Usage Guidelines

The command is used to display the IGMP-snooping translation table information.

Example

The following command is to display the IGMP-snooping translation table information.

```
Switch(config)#show ipigmp-snooping mc-vlan-xlate
Total Multicast VLAN XLATE Entry Number : 512  Current Multicast VLAN XLATE Entry Number: 12
index interface router-pvid MC-VLAN ID Multicast-IP mask

0 tg0/0/1  1 45 225.0.0.1 255.255.255.255
1 tg0/0/1  1 45 225.0.0.2 255.255.255.254
2 tg0/0/1  1 45 225.0.0.4 255.255.255.252
3 tg0/0/1  1 45 225.0.0.8 255.255.255.248
4 tg0/0/1  1 45 225.0.0.16 255.255.255.240
5 tg0/0/1  1 45 225.0.0.32 255.255.255.224
6 tg0/0/1  1 45 225.0.0.64 255.255.255.192
7 tg0/0/1  1 45 225.0.0.128 255.255.255.128
8 tg0/0/1  1 45 225.0.1.0 255.255.255.0
9 tg0/0/1  1 45 225.0.2.0 255.255.254.0
10 tg0/0/1  1 45 225.0.4.0 255.255.252.0
11 tg0/0/1  1 45 225.0.8.0 255.255.255.255

Switch(config)#
```

30.1.18 show ipigmp-snooping vlan

Syntax

show ipigmp-snooping vlan *vlan-id*

Parameter Description

Parameter	Parameter Description
vlan	1-4094

Default Value

None

Command Mode

EXEC Mode

Usage Guidelines

The command is used to display IGMP-snooping VLAN information.

Example

The following command is to display the igmp-snooping vlan information.

```
Switch(config)#show ipigmp-snooping vlan
vlan_id Immediate-leave Ports Router Ports

---------------------------------------------------------------

1 Disabled SWITCH(querier);
333 Disabled SWITCH(querier);
1000 Disabled SWITCH(querier);
2000 Disabled SWITCH(querier);tg0/0/4(static);
```

30.1.19 debug ipigmp-snooping packet

Syntax

debug ipigmp-snooping packet

no debug ipigmp-snooping packet

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable IGMP-snooping packet debug switch.

Example

The following command shows how to enable the packet debugging switch of IGMP-snooping.

```
switch# debug ipigmp-snooping packet
switch#
```

30.1.20 debug ipigmp-snooping timer

Syntax

debug ipigmp-snooping timer

no debug ipigmp-snooping timer

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

This command is used to enable or disable the timer debugging switch of IGMP-snooping.

Example

The following example shows how to enable the timer debugging switch of IGMP-snooping.

```
switch# debug ipigmp-snooping timer
switch#
```

30.1.21 debug ipigmp-snooping event

Syntax

debug ipigmp-snooping event

no debug ipigmp-snooping event

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable the event debug switch of igmp-snooping.

Example

The following command enable the event debug switch of igmp-snooping.

```
Switch#debug ipigmp-snooping event Switch#
```

30.1.22 debug ipigmp-snooping error

Syntax

debug ipigmp-snooping error

no debug ipigmp-snooping error

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable the error debug switch of igmp-snooping.

Example

The following command enable the error debug switch of igmp-snooping.

```
Switch#debug ipigmp-snooping error
Switch#
```

30.1.23 debug ipigmp-snooping

Syntax

debug ipigmp-snooping

no debug ipigmp-snooping

Parameter Description

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to enable/disable all debug switches of igmp-snnoping.

Example

The following command enable all debug switches of igmp-snooping.

```
Switch#debug ipigmp-snooping
IGMP-snooping packet debugging is on
IGMP-snooping timer debugging is on
IGMP-snooping event debugging is on
IGMP-snooping error debugging is on
Switch#
```

Chapter 31 Syslog Configuration Commands

31.1 Syslog Configuration Commands

31.1.1 logging

Syntax

Use the logging command to configure the logging host level of the logging server.

logging *host level*

Parameter Description

Parameter	Parameter Description
host	Configure the log server address to receive logs.
level	Configure the log server port number to receive logs. The value ranges from emergencies, alerts, critical, error, warnings, and notificationsinformational、debugging

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After this function is enabled, logs generated by the device at a level greater than or equal to the specified level will be sent to the specified log server.

Example

```
Switch(config)#logging 1.1.1.1 informational
```

31.1.2 terminal monitor

Syntax

To display the debug output and system error messages on the current terminal, use the terminal monitor command. Disable monitoring with the no form of this command.

[no] terminal monitor

Parameter Description

No parameter or key words

Default Value

The default value of the console port is enabled, and the default value of other terminals is disabled.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is only valid for the current terminal, and when the dialog ends, the terminal properties are also lost.

Example

```
switch#terminal monitor
```

Chapter 32 Telnet Configuration Commands

This document describes telnet and its associated configuration and management commands. telnet is used to establish a telnet session with a remote server, and telnet is generally used to remotely log in to and from Unix systems. Option negotiation is required. telnet does not provide login authentication. Therefore, the biggest difference with Rlogin is that it does not provide password verification on its own.

32.1 ip telnetd enable

Syntax

[**no**] **ip telnetd enable**

Parameter Description

None

Default Value

Enable

Usage Guidelines

This command is used to enable the telnetd service and listen for telnet connections.

Command Mode

Global Configuration Mode

Example

The following command disables the telnetd service.

```
Switch(config)#no ip telnetd enable
```

32.2 ip telnetd connections

Syntax

ip telnetd connections *maxConnections* **no ip telnetd connections**

Parameter Description

Parameter	Parameter Description
maxConnections	The maximum number of locally accepted telnet connections, the value ranges from 1 to 16

Default Value

16

Usage Guidelines

To prevent too many users from occupying connection resources, you can configure the maximum number of connections.

Command Mode

Global Configuration Mode

Example

The following command sets the maximum number of connections to 10:

```
Switch(config)# ip telnetd connections 10
```

32.3 ip telnetd port

Syntax

ip telnetd port *listen-port* **no ip telnetd port**

Parameter Description

Parameter	Parameter Description
listen-port	The value of the listening port specified by the user ranges from 1025 to 65535

Default Value

23

Usage Guidelines

This command can modify the listening port number of the telnetd service.

Command Mode

Global Configuration Mode

Example

The following command changes the listening port number to 3030:

```
Switch(config)# ip telnetd port 3030
```

32.4 telnet

Syntax

telnet {*A.B.C.D*|*X:X:X:X::X*|*WORD*} [**port** *port_num*|**debug**|**local** *src_ip*]*

Parameter Description

Parameter	Parameter Description
A.B.C.D	The user needs the telnet destination IPv4 address
X:X:X:X::X	The user needs the telnet destination IPv6 address
WORD	The user needs the destination remote host name of the telnet
port	The user needs to configure the destination port of telnet
debug	Whether the debug flag is enabled for telnet
local	Configure the local source port of the telnet
port_num	The port number of the destination address, ranging from 1025 to 65535
src_ip	A local IPv4 address of telnet is required

Default Value

None

Usage Guidelines

This command is used to telnet as a client to establish a telnet session with a remote server. To exit the remote telnet, press CTRL+SHIFT+6 at the same time, and then enter the quit command.

Command Mode

Global Configuration Mode、EXEC mode

Example

The following command will attempt to establish a session with 10.25.153.153 via telnet:

```
Switch#telnet 10.25.153.153
Note: Please hold down 'CTRL+SHIFT+6' simultaneously, and then input 'quit' to exit telnet!
Telnet escape character is '^^'.
Trying 10.25.153.153...
```

Chapter 33 VLAN Configuration Commands

33.1 VLAN Configuration Commands

33.1.1 vlan

Syntax

[no] vlan *vlan-id*

To add a VLAN, run vlan vlan-id. To delete a VLAN, run [no] vlan vlan-id.

Parameter Description

Parameter	Parameter Description
vlan-id	Defines the ID of the VLAN. Value range: 1-4094.

Default Value

The default value is 1.

Command Mode

Global Configuration Mode

Usage Guidelines

Use this command to create vlan.

Example

The following example shows how to add the VLAN whose ID is 2-10:

```
Switch(config)#
Switch(config)#vlan 2-10
```

33.1.2 vlan-view

Syntax

vlan-view *vlan-id*

To enter VLAN Configuration Mode, run the above command.

Parameter Description

Parameter	Parameter Description
vlan-id	Defines the ID of the VLAN. Value range: 1-4094.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

After you run this command, you can enter the VLAN Configuration Mode, and you can change some properties of the vlan after entering the mode. If a VLAN has not yet been created, the VLAN is created first, and then it enters VLAN mode.

Example

The following example shows how to add the VLAN whose ID is 2:

```
Switch(config)#
Switch(config)#vlan-view 2  Switch(config-vlanid2)#exit
Switch(config)#
```

33.1.3 name

Syntax

[no] name *str*

To name a VLAN, run name str. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
str	Defines the name of the VLAN. Value range: 1-32 characters.

Default Value

The default VLAN name is 'Default'. Other VLAN's name is VLANxxxx (xxxx is 4-digit stack ID)

Command Mode

VLAN Configuration Mode

Usage Guidelines

This command can be used to modify the VLAN name to symbolize a specific VLAN.

Example

The following example shows how to set the name of VLAN200 to main405:

```
Switch(config)#
Switch(config)#vlan-view 200
Switch(config-vlanid200)#name main405 Switch(config-vlanid200)#
```

33.1.4 dot1q-tunnel

Syntax

[no] dot1q-tunnel

To enable or disable the global Dot1q Tunnel, run the above command.

Parameter Description

None

Default Value

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

After a Dot1Q tunnel is enabled globally, all ports are connected to the Dot1Q tunnel by default, and an SPVLAN tag is forcibly added to incoming packets.

Example

Configure enable Dot1q Tunnel globally.

```
Switch(config)#dot1q-tunnel
```

33.1.5 switchport pvid

Syntax

switchport pvid *vlan-id* no switchport pvid

To configure VLAN of the access-mode port, run switchport pvid vlan-id. To return to the default setting, use the no form of this command.

Parameter Description

Parameter	Parameter Description
vlan-id	VLAN ID which the port belongs to. Value range: 1-4094

Default Value

All ports belong to VLAN 1.

Command Mode

Port Configuration Mode

Usage Guidelines

The port can be access mode or relay mode. If there is no VLAN, the VLAN will be created.

Example

The following example shows how to set port g0/1 to the access port of VLAN10:

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport pvid 10
```

33.1.6 switchport mode

Syntax

switchport mode{access | trunk | dot1q-tunnel-uplink [*tpid*] | dot1q-translating-tunnel}

no switchport mode

To configure the port mode, run the above commands.

Parameter Description

Parameter	Parameter Description
access	Access mode
trunk	Relay mode
dot1q-tunnel-uplink	VLAN tunnel uplink mode
tpid	Tpid is the field value of VLAN tag
dot1q-translating-tunnel	VLAN translating tunnel mode

Default Value

Switch port dot1q-tunnel-uplink，GPON port access mode

Command Mode

Port Configuration Mode

Usage Guidelines

The switch port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

The relay mode indicates that the port connects other OLTs and the tagged Ethernet frame can be transmitted and received.

The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the OLT omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.
The port mode collides with the 802.1X protocol. The 802.1X protocol cannot be configured in relay mode (including the VLAN translating tunnel mode and the VLAN tunnel uplink mode); the port on which the 802.1X protocol is configured cannot be set to the relay mode. That is to say, the 802.1X protocol can be effective only on the access-mode port (including the VLAN tunnel mode).
The 802.1X standard does not support authentication on the trunk port. The reason is that the authentication object regulated in the standard is not the port. As to port multiplexing, if user authentication is approved in one VLAN, all other VLAN users who multiplex this port are also authorized correspondingly, therefore, the trunk port does not support authentication.
GPON port does not support dot1q-tunnel-uplink.

Example

The following example shows how to set the port to the VLAN tunnel uplink mode and how to set the TPID of the unlink port to 0x9100:

```
Switch(config-tg0/0/1)#switchport mode dot1q-tunnel-uplink 0x9100
```

33.1.7 switchport trunk

Syntax

[no] switchport trunk {vlan-allowed {*vlan-list*|none|add *vlan-list*|remove *vlan-list*|except *vlan-list*|all}

| vlan-untagged {*vlan-list*|none|add *vlan-list*|remove *vlan-list*|except *vlan-list*|all} }

To configure the relay port characterisitcs, run the above commands.

Parameter Description

Parameter	Parameter Description
vlan-allowed	VLAN ID which can be received and transmitted by the port Value range: 1-4094
vlan-untagged	Frame that will be transmitted without adding the VLAN tag Value range: 1-4094
vlan-list	VLAN list
none	No VLAN ID
add	Add VLAN ID to the existed list
remove	Remove VLAN ID from the existed list
except	All VLAN ID except the ones listed below
all	All VLAN ID

Default Value

The native VLAN ID of all relay ports is 1. The allowable value for all VLANs ranges between 1 and 4094.

Command Mode

Port Configuration Mode

Usage Guidelines

No matter the port is in access mode or in relay mode, you can run this command on the port. However, the port is in relay mode when this command functions.

The vlan-allowed parameter is used to control theVLANrange of the port; the vlan-untagged parameter is used to decide which packets need be added with theVLANtag when a port transmits these packets.

When the vlan list is used, you can add, remove or set (none, all, except) the lists of the existingVLAN. The entered lists are separated by the comma or the hyphen. For example, "1, 3, 5, 7" stands for "vlan 1, vlan 3, vlan 5, vlan 7", while "1, 3-5, 7" stands for "vlan 1, vlan 3, vlan 4, vlan -5, vlan 7".

Example

The following example shows how to set the allowable VLAN range to 1-10, and the untagged VLAN range to 2-1000.

```
Switch(config-tg0/0/1)#switchport trunk vlan-allowed 1-10
Switch(config-tg0/0/1)#switchport trunk vlan-untagged 2-1000
```

33.1.8 switchport dot1q-translating-tunnel

Syntax

switchport dot1q-translating-tunnel mode QinQ translate {oldvlanid | oldvlanlist }*newvlanid* [*priority*]

no switchport dot1q-translating-tunnel mode QinQ translate {oldvlanid| oldvlanlist}

switchport dot1q-translating-tunnel mode flat translate {1to1|nto1} {oldvlanid | oldvlanlist}*newvlanid* [*priority*]

no switchport dot1q-translating-tunnel mode flat translate{1to1|nto1}{oldvlanid | oldvlanlist}

switchport dot1q-translating-tunnel mode mix translate{oldvlanid | oldvlanlist}*newvlanid addvlanid* [*priority*]

no switchport dot1q-translating-tunnel mode mix translate{oldvlanid | oldvlanlist}

To configure the attributes of a port in VLAN translating tunnel mode, run the above command:

Parameter Description

Parameter	Parameter Description
1to1 | nto1	The translation mode of Flat is 1:1 or n:1.
oldvlanid | oldvlanlist	The VLAN translation entries of VLAN translation tunnel ports. The value range of oldvlanlist and oldvlanid is 1 to 4094.
flat | QinQ| mix	VLAN translation mode of a VLAN translation tunnel port
newvlanid	The vlan ID after translation. The value ranges from 1 to 4094.
addvlanid	The vlan serial number needs to add after translation. The value ranges from 1 to 4094.
priority	Priority level. The value ranges from 0 to 7.

Default Value

The VLAN translating mode of the VLAN translating tunnel port is QinQ and no VLAN translating items exists.

Command Mode

Port Configuration Mode

Usage Guidelines

Both the VLAN translating mode and the VLAN translating items validate in dot1q-translating-tunnel mode after they are configured. The translation modes fall into two kinds: the Flat mode and the QinQ mode. In Flat mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list. The CVLAN will be replaced by detected SPVLANs; when the packets are forwarded out of the port, the SPVLAN will then be replaced by CVLAN. In QinQ mode, the CLAN tag of packets which are received by the dot1q-translating-tunnel downlink port will be used as an index to look up the VLAN translating list and then the detected SPVLANs will form into SPVLAN tag to be added to the outside of CVLAN tag; when the packets are forwarded out of the port, the SPVLAN tag will then be removed.

When the VLAN translating items are configured on a port, the mapping between CVLAN and multiple SPVLANs can be configured in QinQ mode. To configure the mapping between CVLAN and multiple SPVLANs in flat mode, you have to configure QoS and then the correct transformation from SPVLAN to CVLAN can be conducted when packets are transmitted out from this port.

Example

The following example shows how to add the translation items to g0/1, translate CVLAN 1000 into SPVLAN 100 and set the VLAN translation mode of the translation items to Flat.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport dot1q-translating-tunnel mode flat translate 1000 100
```

33.1.9 mac-vlan mac-address

Syntax

mac-vlan mac-address *mac-addr*vlan *vlan-id* [*priority*]

no mac-vlan mac-address *mac-addr*

To add or delete VLAN entry based on MAC, run the above command.

Parameter Description

Parameter	Parameter Description
mac-addr	The MAC address corresponding to the MAC VLAN entry
vlan-id	The VLAN ID corresponding to the MAC VLAN entry. The value ranges from 1 to 4094.
priority	The priority corresponding to MAC VLAN entry. The value ranges from 0 to 7.

Default Value

No VLAN entry based on MAC.

Command Mode

Global Configuration Mode

Usage Guidelines

None

33.1.10 switchport mac-vlan

Syntax

[no] switchport mac-vlan

To enable/disable VLAN based on MAC, run the above command.

Parameter Description

None

Default Value

Disable MAC-based VLAN

Command Mode

Port Configuration Mode

Usage Guidelines

If the port mode is set to access, if the VLAN that matches the VLAN through the MAC VLAN entry is not the PVID of the port, the packet is discarded. Therefore, do not configure the port mode with MAC VLAN enabled as access unless required.

33.1.11 subnet

Syntax

subnet any

no subnet any

[no] subnet *ip-addr mask*

To add/delete IP subnet based VLAN, run the above command.

Parameter Description

Parameter	Parameter Description
any	If the source IP address is any IP address, the VLAN corresponding to the entry is matched.
ip-addr mask	The entry corresponding IP address and subnet mask

Default Value

No IP subnet based VLAN entry.

Command Mode

VLAN Configuration Mode

Usage Guidelines

None

Example

Configure the VLAN classification of the network segment with IP address 192.168.100.3 and mask 255.255.255.0 as VLAN 100, and allow the use of all slots in the key for all slots in place on the current wired card.

```
Switch(config)#vlan-view 100
Switch(config-vlanid100)#subnet 192.168.100.3 255.255.255.0 Switch(config-vlanid100)#exit
Switch(config)#
```

33.1.12 switchport vlan-subnet enable

Syntax

[no] switchport vlan-subnet enable

To enable/disable IP subnet based VLAN, run the above command.

Parameter Description

None

Default Value

Disable IP subnet based VLAN.

Command Mode

Port Configuration Mode

Usage Guidelines

If the port mode is set to access, if the incoming packet matches the PVID of the port through the subnet VLAN entries, the packet is discarded. Therefore, do not configure the port mode with Subnet VLAN enabled as access unless required.

Example

On port tg0/0/1 enable IP subnet based VLAN function:

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport vlan-subnet enable
```

33.1.13 protocol-vlan

Syntax

protocol-vlan ether-type *etype-id* vlan *vlan-id*

no protocol-vlan ether-type *etype-id*

To add/delete the protocol template, run the above commands.

Parameter Description

Parameter	Parameter Description
etype-id	*Stands for the Ethernet type of the incoming packets.*
vlan-id	Stands for the corresponding VLAN ID, which ranges from 1 to 4094.

Default Value

No protocol template

Command Mode

Global Configuration Mode

Usage Guidelines

The configuration commands may vary with different switches.

33.1.14 switchport protocol-vlan

Syntax

switchport protocol-vlan *protocol_index* vlan *vlan-id*

no switchport protocol-vlan *protocol_index*

To enable or disable the protocol-based VLAN, run the above commands.

Parameter Description

Parameter	Parameter Description
protocol_index	Stands for the protocol template type (only applicable to the model with this function)
vlan-id	Stands for the corresponding VLAN ID, which ranges from 1 to 4094 (only applicable to the model with this function).

Default Value

The port does not associate with any protocol template.

Command Mode

Port Configuration Mode

Usage Guidelines

In port access mode, an incoming packet will be dropped if its VLAN, which is obtained through the matchup of protocol-based VLAN entry, is not PVID of the port. Hence, if not necessary, do not set the port mode, which is to enable protocol-based VLAN to access.

33.1.15 show vlan

Syntax

show vlan [id *vlan-id* | interface *intf-id* | dot1q-tunnel [interface *intf-id*] | mac-vlan | subnet | protocol-vlan | debug | run-config [interface *intf-id*]]

To display relative information about all VLANs, run the above command.

Parameter Description

Parameter	Parameter Description
vlan-id	Displays the designated VLAN. Value range: 1-4094
intf-id	Displays the designated port.
dot1q- tunnel	Displays the global information and statistics information about Dot1Q tunnel, or displays the detailed information about Dot1Q tunnel of the designated port.
mac-vlan	Displays the configured MAC VLAN entries.
subnet	Displays the configured IP-subnet VLAN entries.
protocol- vlan	Displays the configured protocol VLAN template or entry.

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

None

Example

Display all VLAN information.

```
Switch(config)#show vlan
VLAN Status Name Ports


---- ------- -------------------------------- --------------------------------
```

```
1 Static Default tg0/0/1, tg0/0/2, tg0/0/3, tg0/0/4, tg0/0/5, tg0/0/6, tg0/0/7, tg0/0/8,
cg0/0/1
```

The status parameter stands for the VLAN generation source; the static parameter means that VLAN is generated through configuration; the dynamic parameter means that VLAN is generated dynamically through the GVRP protocol.

Switch(config)#show vlanid 2 VLAN id: 2, Name: VLAN0002

Mode: Static, Total Ports: 2 Interface Attributes

g0/0/2 Trunk, Tagged g0/0/3 Trunk, Tagged

The following example shows relative information about a VLAN on a port:

Switch(config)#show vlan interface g0/0/3 Interface VLAN

Name Property PVID Vlan-Map uTagg-Vlan-Map

g0/0/3 Trunk 1 1-10,200 1 Switch(config)#

33.1.16 show interface vlan

Syntax

show interface vlan intf-id

To display the VLAN interface information, run the above command.

Parameter Description

|Parameter|Parameter Description|value range| |---|---|---|

|*intf-id*|dispaly the given port|

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

None

Example

Display the information of interface VLAN 1:

```
Switch(config)#show interface vlan1
vlan1 is up, line protocol is up Ifindex is 449
Encapsulation ARPA

Peak input rate 0 pps, output 0 pps
3383 packets input, 1047691 bytes

Received 3383 broadcasts, 0 multicasts

0 mplsunicasts, 0 mpls multicasts, 0 mpls input discards
0 input errors, 0 discards, 0 protocol unknown

0 packets output, 0 bytes
Transmited 0 broadcasts, 0 multicasts

0 mplsunicasts, 0 mpls multicasts, 0 mpls output discards

0 output errors, 0 discards
```

The statistics values are explained as follows:
Packets input means the input of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all packets.
Broadcasts means received broadcast packets.
Broadcasts means received broadcast packets.
Input errors means received error packets.
Input discards means that the received packets are dropped, such as the received packets when the interface protocol is down.

Packets output means the output of all packets, including broadcast packets, multicast packets and unicast packets.
Bytes means the byte volume of all transmitted packets.
Broadcasts means transmitted broadcast packets.
Multicasts means transmitted multicast packets.
Output errors means transmitting error packets.
Output discards means that the transmitted packets are dropped, such as the transmitted packets when the interface protocol is down.

Chapter 34 AAA Configuration Commands

This Chapter describes the AAA configuration commands. AAA configuration commands can be classified into authentication, authorization, accounting and local account policy configuration commands. Learn more in the following sections.

34.1 Authentication Configuration Commands

This section describes the commands for configuring authentication methods. Authentication identifies the access right of the users before they are allowed to access the network and network services.

Authentication Configuration Commands include:

- aaa authentication dot1x
- aaa authentication login
- aaa authentication ssh
- aaa authentication enable

34.1.1 aaa authentication dot1x

Syntax

To set do1x access authentication, run command aaa authentication dot1x in global configuration mode. To disable dot1x authentication, use the no form of this command.

aaa authentication dot1x default {**local** | **radius**}

no aaa authentication dot1x default

Parameter Description

Parameter	Parameter Description
local	It uses local username database for authentication.
radius	It uses RADIUS for authentication.

Default Value

Dot1x access authentication check is disable by default.

Command Mode

Global Configuration Mode

Usage Guidelines

The aaa authentication dot1x command will be referenced by the dot1x application to authenticate dot1x users who have accessed.

Example

The following example shows how to use a RADIUS server to authenticate dot1x access:

```
Switch(config)#aaa authentication dot1x default radius
```

Related Command

- dot1x enable
- dot1x port-control

34.1.2 aaa authentication login

Syntax

For console and telnet login authentication, use the global configuration command aaa authentication login. Use the no form of this command to disable aaa authentication login.

aaa authentication login default {**local** | **radius**}

no aaa authentication login default

Parameter Description

Parameter	Parameter Description
local	It uses local username database for authentication.
radius	It uses RADIUS for authentication.

Default Value

No authentication check is enabled for console and telnet logins by default.

Command Mode

Global Configuration Mode

Usage Guidelines

aaa authentication login command is used to configure console and telnet login authentication.

Example

The following example shows how to use a RADIUS server to authenticate console and telnet logins:

```
Switch(config)#aaa authentication login default radius
```

Related Command

None

34.1.3 aaa authentication ssh

Syntax

The global configuration command aaa authentication ssh is used for SSH login authentication. Use the no form of this command to disable SSH authentication.

aaa authentication ssh default {**local** | **radius**}

no aaa authentication ssh default

Parameter Description

Parameter	Parameter Description
local	It uses local username database for authentication.
radius	It uses RADIUS for authentication.

Default Value

ssh login authentication check is disabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

The aaa authentication ssh command is used to configure console and telnet login authentication.

Example

The following example shows how to use a RADIUS server to authenticate ssh logins:

```
Switch(config)#aaa authentication ssh default radius
```

Related Command

None

34.1.4 aaa authentication enable

Syntax

The global configuration command aaa authentication enable is used for enabling permission authentication. Use the no form of this command to disable the enable permission.

aaa authentication enable default local

no aaa authentication enable default

Parameter Description

Parameter	Parameter Description
local	It uses local username database for authentication.

Default Value

Disable permission authentication check is enabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

The aaa authentication enable command is used to configure enable permission authentication.

Example

The following example shows how to use the local database to authenticate the enable permission:

```
Switch(config)#aaa authentication enable default local
```

Related Command

- enable level

34.2 Local Account Configuration Commands

This section introduces local account configuration commands. The local account is used for local authentication. Local Account Policy Configuration Commands include:

- username

34.2.1 username

Syntax

To add users in the local user database for local authentication and authorization, run this command.

To delete the corresponding user, use the no form of this command.

username *username* **password** [*encryption-type*] *password* [**privilege** *privilege-level*] [**maxdays** *maxdays*]

no username *username*

Parameter Description

Parameter	Parameter Description
username	Character string of username
encryption-type	(Optional) Password encryption type: 0 for no encryption, 6 for sha256 encryption, and if left blank, it is considered as no encryption.
password	The password string.
privilege	Specify the user level after login.
privilege-level	Specify the specific value of the user level after login, rang from 1 to 15.
maxdays	Specifies the maximum number of days after logging in that a user's password must be changed.
maxdays	Specifies the maximum number of days after logging in that a user's password must be changed, range from 1 to 90.

Default Value

No username or password by default.

Command Mode

Global Configuration Mode

Usage Guidelines

Notes: The password we configure cannot include space; the username cannot start with a number or a capital letter.

Currently, our system supports only two encryption-types. The parameters in the command are 0 and 6 respectively. 0 means no encryption. You can directly enter the plain text of the password in the encrypted password. This method has the same effect as directly entering the password parameter without adding encryption-type. 6 means using the sha256 algorithm for encryption. The plain text of the password needs to be entered in the encrypted password. The ciphertext generated can be copied from the configuration file of our company's device.

Example

The following example shows how to add a local user with the username someone and password some other:

```
Switch(config)#username someone password someother
```

The local user is added in the Example below, the username is Oscar, the password is Joan. The encryption type applied is 6, namely the encryption method, the ciphertext of the password needs to be entered. 5 is the user level after login, 4 is the maximum number of days after login that the user password needs to be changed:

```
Switch(config)#username oscar password 6 Joan privilege 5 maxdays 4
```

Related Command

- aaa authentication login
- aaa authentication ssh
- aaa authentication dot1x

34.2.2 password-policy

Syntax

The following command is used to check the password complexity on newly added or modified local user passwords.

password-policy [**min-length** *min-length*] [**min-digits** *min-digits*] [**min-upper** *min-upper*] [**min-lower** *min-lower*] [**min-other** *min-other*]

no password-policy

Parameter Description

Parameter	Parameter Description
min-length	(Optional)check the minimum length of the password.
min-length	The optional range of the minimum length is 1~75.
min-digits	(Optional) Check the minimum number of digits in the password.
min-digits	The minimum number of digits can be selected from 1 to 75.
min-upper	(Optional) Check the minimum number of capital letters in the password.
min-upper	The minimum number of capital letters can range from 1 to 75.
min-lower	(Optional) Check the minimum number of lowercase letters in the password.
min-lower	The minimum number of lowercase letters can range from 1 to 75.
min-other	(Optional) Check the minimum number of special characters in the password.
min-other	The minimum number of special characters can be selected in the range of 1 to 75.

Default Value

The password complexity check is disable by default.

Command Mode

Global Configuration Mode

Usage Guidelines

Note: This configuration will not affect the existing local user data, only the newly created users after configuration will be checked. Special characters refer to non-alphanumeric characters that can be displayed. At least one of the 5 options must be selected, and all can be selected.

Example

The following command will set the password to be at least 11 characters long, including at least 1 number, 2 uppercase letters, 3 lowercase letters and 4 special characters:

```
Switch(config)#password-policy min-length 11 min-digits 1 min-upper 2 min-lower 3 min-other 4
```

Related Command

- username
- enable level

Chapter 35 RADIUS Configuration Commands

This chapter introduces the commands for RADIUS configuration. RADIUS is a distributed client/server system capable of denying unauthorized network access.

RADIUS client is running on the switch and sends the request of authentication to the central RADIUS server containing the authentication information of all the users and the information of network service access.

35.1 RADIUS Configuration Commands

35.1.1 radius-server host

Syntax

The global configuration command "radius-server host" is used for designating IP address of RADIUS server. The "no" format of the command is used for deleting the designated RADIUS host.

radius-server host *ip-address* **key** *key* [**auth-port** *number*] [**timeout** *time*]

no radius-server host *ip-address*

Parameter Description

Parameter	Parameter Description
ip-address	the ip address of RADIUS server
key	The shared key is used between the switch and the RADIUS server.
auth-port	(optional item) Designating destination port number for authentication.
number	The configurable range of the authentication destination port number is 1 to 65535.
timeout	(Optional) Specify a timeout period.
time	The configurable range of the timeout period is 3 to 60.

Default Value

No RADIUS host is designated.

Command Mode

Global Configuration Mode

Usage Guidelines

The command "radius-server host" can be used repeatedly for designating multiple servers. The polling can be done under the order of configuration when necessary.

Example

The Example below designates RADIUS host whose IP address is 1.1.1.1. The shared key is PLANET. The default port is used for accounting and authentication.

```
Switch(config)#radius-server host 1.1.1.1 key planet
```

The following Example designates Port 12 as the destination port of authentication request on the RADIUS host whose IP address is 1.2.1.2. The shared key is planet. The authentication timeout is 3 seconds

```
Switch(config)#radius-server host 1.2.1.2 key planet auth-port 12 timeout 3
```

Related Command

- aaa authentication login
- aaa authentication ssh
- aaa authentication dot1x

Chapter 36 FAIL-LOCK Configuration Commands

This chapter introduces the configuration commands of FAIL-LOCK. Fail-lock is a method to prevent violent attacks. It protects the switch by locking out users who have failed to log in multiple times and making them unable to log in for a short period of time.

36.1 FAIL-LOCK Configuration Commands

36.1.1 failed-lock

Syntax

For users who have failed to log in a specified number of times within a certain period of time, their login will be locked in a configurable period of time. The "no" form of this command will disable this function.

failed-lock retry-times *retry-times* **failed-interval** *failed-interval* **unlock-time** *unlock-time*

no failed-lock

Parameter Description

Parameter	Parameter Description
retry-times	The number of consecutive failures is configurable from 1 to 50.
failed-interval	The unit consecutive failure time is configurable from 1 to 86400.
unlock-time	The user lock time is configurable from 1 to 86400.

Default Value

The fail-lock function to prevent brute force attacks is disabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is effective for users, so any authentication failure will increase the corresponding user's failure count, including enable authentication.

Example

The following example indicates that a user who fails to log in three times in a row within 60 seconds will be locked out for 180 seconds:

```
Switch(config)#failed-lock retry-times 3 failed-interval 60 unlock-time 180
```

Related Command

- aaa authentication login
- aaa authentication ssh
- aaa authentication dot1x
- aaa authentication enable
- username
- radius-server host
- enable level
- enable

Chapter 37 Privilege Configuration Commands

This chapter introduces the configuration commands of privilege. privilege is a command used in conjunction with user level authorization. Its effect is to set the minimum level of users who can execute each command, thereby realizing the functional authority distinction of different users.

37.1 Privilege Configuration Commands

37.1.1 privilege

Syntax

The following command is used to set the minimum level of users that can execute each command.

privilege {**exec** | **interface**} {**default** | *level*} *command*

Parameter Description

Parameter	Parameter Description
exec	Commands in the enable and config views.
interface	Commands in interface view.
default	Resume to the default minimum permissions.
level	Set the minimum permission to use, the setting range is 1~15.
command	The configured Commands

Default Value

Except for the show and debug commands, which have a default level of 0, all other commands have a default level of 15.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to set the minimum execution privilege of the ping command to 10:

```
Switch(config)#privilege exec 10 ping
```

Related Command

- enable
- change-privilege

Chapter 38 Enable Level Configuration Commands

This chapter introduces the configuration commands of ENABLE LEVEL. Enable level is the password used to configure local authentication of enable.

38.1 Enable Level Configuration Commands

38.1.1 enable level

Syntax

The following command is used to set the password for local authentication of enable. Use the no form of this command to delete the password authentication of the corresponding level.

enable level *level* **password** [*encryption-type*] *password*

no enable level *level*

Parameter Description

Parameter	Parameter Description
level	The password level needs to be configured, the value range is 1~15.
encryption-type	(Optional) Password encryption type: 0 for no encryption, 6 for sha256 encryption, and if left blank, it is considered no encryption.
password	The password is used to authenticate match.

Default Value

All levels have no passwords by default.

Command Mode

Global Configuration Mode

Usage Guidelines

Note: The password we configure cannot contain space.

Example

The following example shows how to set the permission password for level 15 to enable15:

```
Switch(config)#enable level 15 password 0 enable15
```

Related Command

- enable
- aaa authentication enable

Chapter 39 Change-privilege Configuration Commands

This chapter introduces the configuration command of CHANGE-PRIVILEGE. Change-privilege is used to set whether the logged-in user is allowed to actively change his own permissions after obtaining the permissions.

39.1 Change-privilege Configuration Commands

39.1.1 change-privilege

Syntax

This command is used to Set the logged-in user to be allowed to actively change his permissions after obtaining permissions. The no form of this command does not allow the user to change his own permissions after obtaining permissions.

change-privilege enable

no change-privilege enable

Parameter Description

None

Default Value

The command is not allowed to actively change your own permissions after obtaining permissions.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows the effect of not allowing logged-in users to actively change their own permissions after obtaining permissions:

```
Switch>enable 5  Switch#enable 10
User is denied change privilege.
```

Related Command

- enable
- aaa authentication enable
- username

Chapter 40 Port Additional Characteristics Configuration Commands

40.1 Configuring Storm Blocking Commands

Syntax

[**no**] **switchport block** {**unicast** | **multicast** | **broadcast**}

To configure a port not to forward a designated type of messages, run this command.

Parameter Description

Parameter	Parameter Description
unicast	Means that the unknown unicast frame is not forwarded on a port.
multicast	Means that the multicast frame is not forwarded on the port.
broadcast	Means that the broadcast frame is not forwarded on the port.

Default Value

All types of messages can be forwarded by default.

Command Mode

Interface configuration mode

Usage Guidelines

This command must be configured in Layer 2 interface configuration mode.

Example

The following example shows how to configure port tg0/0/1 not to forward the unknown unicast frame.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport block unicast
```

40.2 Configuring Port Isolation Commands

40.2.1 Configuring Port Isolation Group Commands

Syntax

[no] port-protected [*group-id*] [**description** *word*]

Parameter Description

Parameter	Parameter Description
group-id	Configures port isolation group id 1 to 16.
word	Description of port isolation. Single character, not a sentence.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to configure port isolation group 3 and set the description information.

```
Switch(config)#port-protected 3 description name3
```

40.2.2 Checking Port Isolation Group Commands

Syntax

This command is used to display information about all port isolation groups.

port-protected show

Parameter Description

None

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to display information about all port isolation groups.

```
Switch(config)#port-protected show port-protected group:  0
portlist
description
port-protected group:  1 portlist 41
description
port-protected group:  3 portlist
description name3
port-protected group: 12
portlist
description
```

40.2.3 Applying Port Isolation Commands

Syntax

[**no**] **switchport protected** [*group-id*]

This command is used to configure port isolation.

Parameter Description

Parameter	Parameter Description
group-id	Port isolation group id

Default Value

None

Command Mode

Interface configuration mode

Usage Guidelines

This command is used on Layer 2 ports. Data communication is disabled between isolated ports, but data packets between non-isolated ports and between isolated ports and non-isolated ports can still be forwarded normally.

Example

The following example shows how to configure port isolation on port tg0/0/1.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport protected
```

40.3 Configuring Storm Control Commands

40.3.1 storm-control

Syntax

storm-control {**broadcast** | **multicast** | **unicast**} **threshold** *count* **no storm-control** {**broadcast** | **multicast** | **unicast**} **threshold**

To configure storm control for a port, run storm-control {broadcast | multicast | unicast} threshold count.

Parameter Description

Parameter	Parameter Description
broadcast	Defines broadcast storm control.
multicast	Defines multicast storm control.
unicast	Defines unknown unicast storm control.
count	Defines the threshold flux of the storm.

Default Value

The storm control function is disabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in Layer 2 Interface configuration mode.

Example

The following example shows how to set the unknown unicast-frame storm to 20pps on port tg0/0/1.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#storm-control unicast threshold 20
```

40.3.2 storm-control mode

Syntax

storm-control mode {**kbps** | **pps**} **no storm-control mode**

This command is used to configure the storm control threshold unit of the port.

Parameter Description

Parameter	Parameter Description
kbps	Set the storm threshold in kbps. The minimum unit is 64kpbs.
pps	Set the storm threshold in pps. The minimum unit is 1pps.

Default Value

The unit is pps by default.

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in Layer 2 Interface configuration mode.

When configuring, ensure that there is no storm control function configured.

Example

The following example shows how to set the storm control unit on tg0/0/1 to kbps.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#storm-control mode kbps
```

40.3.3 storm-control action

Syntax

storm-control {**broadcast** | **multicast**} **action** {**shutdown** | **resume**}

no storm-control {**broadcast** | **multicast**} **action**

This command is used to configure the storm control action function of the port.

Parameter Description

Parameter	Parameter Description
shutdown	When the port traffic reaches the threshold, the port will shutdown.
resume	Resume ports that were shutdown due to storm control.

Default Value

Storm control action is disabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in Layer 2 Interface configuration mode.

If storm-control auto_resume is not configured, the port status will not be automatically resumed. You need to manually configure storm-control action resume to enable the port to resume packet forwarding.

Only broadcast and multicast, and when the mode is based on PPS, support storm-controlaction operation, and the corresponding storm threshold must be configured before configuration.

Example

The following example shows how to set the broadcast storm control action to disable on tg0/0/1.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#storm-control mode pps
Switch(config-tg0/0/1)#storm-control broadcast threshold 20
Switch(config-tg0/0/1)#storm-control broadcast action shutdown
```

40.3.4 storm-control auto_resume

Syntax

storm-control {**broadcast** | **multicast**} **auto_resume** [*second*]

no storm-control {**broadcast** | **multicast**} **auto_resume**

This command is used to configure the storm control auto_resume function of the port.

Parameter Description

Parameter	Parameter Description
second	The time it takes for the port to automatically recover, in seconds. If not entered, the default value is 60 seconds.

Default Value

The storm control auto_resume function is disabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in Layer 2 Interface configuration mode.

Only broadcast and multicast, and when the mode is based on pps, support the storm-control auto_resume operation, and the corresponding storm-control action must be configured before configuration.

Example

The following example shows that the automatic recovery time for broadcast storm control on tg0/0/1 is 100 seconds.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#storm-control mode pps
Switch(config-tg0/0/1)#storm-control broadcast threshold 20
Switch(config-tg0/0/1)#storm-control broadcast action shutdown Switch(config-tg0/0/1)#storm-control broadcast auto_resume 100
```

40.3.5 storm-control notify

Syntax

storm-control notify {**log** | **trap**}

no storm-control notify {**log** | **trap**}

This command is used to configure the storm control alarm reporting function of the port.

Parameter Description

Parameter	Parameter Description
log	Report alarms in syslog printing mode.
trap	Report alarms in snmp-trap mode.

Default Value

The storm control alarm reporting function is disabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

The command must be configured in Layer 2 Interface configuration mode. Both modes can be enabled at the same time.

Example

The following example shows how to enable syslog reporting alarms of storm control on tg0/0/1.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#storm-control notify log
```

40.4 Configuring Port Rate Limit Commands

Syntax

[**no**] **switchport rate-limit** {*band* | **bandwidth** *percent*} {**ingress**|**egress**} {**burst-size** [*high* | *middle* | *low*]}

This command is used to configure the traffic rate limit of the port.

Parameter Description

Parameter	Parameter Description
band	Traffic rate. Step size 64Kbps
percent	Traffic Ratio. Unit: 1%
ingress	Valid for ingress.
egress	Valid for egress.
burst-size	Port buffer size
high	Configuring large buffer
middle	Configuring Medium Buffering
low	Configuring Low Buffering

Default Value

The port has no rate limit by default.

Command Mode

Interface configuration mode

Usage Guidelines

This command must be configured in Layer 2 interface configuration mode.

Example

The following example shows how to configure the flow ingress rate limit on port tg0/0/1 to 1M.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport rate-limit 16 ingress
```

40.5 Configuring Port Loop Check Commands

Syntax

[**no**] **keepalive** *second*

This command is used to configure the interval for the port to transmit loop check messages.

Parameter Description

Parameter	Parameter Description
second	Time interval, 0-32767 seconds, default 12 seconds.

Default Value

The time interval is 12 seconds by default.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to configure the transmission interval on port tg0/0/1 to 10 seconds.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#keepalive 10
```

40.6 Configuring Port MAC Address Learning Commands

Syntax

[**no**] **switchport disable-learning**

This command is used to configure port mac address learning capability.

Parameter Description

None

Default Value

The port mac address learning capability is enabled by default.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to disable MAC address learning capability on port tg0/0/1.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switch port disable-learning
```

40.7 Configuring Port Security Commands

40.7.1 switchport port-security mode

Syntax

switchport port-security mode {**dynamic** | **static** {**accept** | **reject**} | **sticky**}

[**no**] **switchport port-security mode**

This command is used to configure the port security mode

Parameter Description

Parameter	Parameter Description
dynamic	Configure port security dynamic mode.
static {**accept**	**reject**}	Configure port static receive/reject mode.
sticky	Configure port security sticky mode.

Default Value

By default, port security is disabled.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Mutually exclusive with the **switchport dynamic maximum** *number* command.

Example

The following example shows how to configure the port tg0/0/1 to dynamic port security mode.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport port-security mode dynamic
```

40.7.2 switchport port-security dynamic

Syntax

switchport port-security dynamic maximum *dynamic_number*

[**no**] **switchport port-security dynamic maximum**

This command is used to configure the maximum number of learnable MAC addresses when the port is in dynamic security mode

Parameter Description

Parameter	Parameter Description	Value range
dynamic_number	The maximum address number that can be learned.	1-1024, default value is 1.

Default Value

The maximum number of items in MAC addresses that can be learned is 1.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to set the number of MAC addresses that can be learned on port tg0/0/1 to 10.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport port-security dynamic maximum 10
```

40.7.3 switchport port-security static mac-address

Syntax

[**no**] **switchport port-security static mac-address** *AA:BB:CC:DD:EE:FF* [**vlan** *vlanid*]

This command is used to configure a static security MAC address.

Parameter Description

Parameter	Parameter Description
AA:BB:CC:DD:EE:FF	MAC address
vlanid	The vlan-id of the message, the value is 1-4094.

Default Value

None

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to configure the mac address 00:01:00:02:00:03 to static security address.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport port-security static mac-address 00:01:00:02:00:03
```

40.7.4 switchport port-security sticky

Syntax

switchport port-security sticky { **maximum** *sticky_number* | **mac-address** *AA:BB:CC:DD:EE:FF* | **stop**}

[**no**] **switchport port-security sticky** {**maximum** | **mac-address** *AA:BB:CC:DD:EE:FF* | **stop**}

This command is used to configure port mac address sticky.

Parameter Description

Parameter	Parameter Description
sticky_number	The maximum number of addresses that can be learned on the port. Default Value is 100, Range: 1-1024
AA:BB:CC:DD:EE:FF	Mac address
stop	Stop sticky learning.

Default Value

The port mac address is not sticky by default.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to manually set mac:44:33:00:02:00:21 as the sticky mac address.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switchport port-security sticky mac-address 44:33:00:02:00:21
```

40.7.5 switchport port-security mac aging-time

Syntax

switchport port-security mac aging-time *aging_time*

no switchport port-security mac aging-time

This command is used to configure the aging time of the security address under sticky and dynamic port.

Parameter Description

Parameter	Parameter Description
aging_time	Aging time. The unit is minutes. The default value is 0, which means no aging. The range is 0-100.

Default Value

The default is no aging.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to set the aging time to 3 minutes.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)# switchport port-security mac aging-time 3
```

40.7.6 switchport port-security mac [inactivity-aging | absolute- aging]

Syntax

[no] switchport port-security mac [**inactivity-aging** | **absolute-aging**]

This command is used to configure the security address aging mode under sticky and dynamic port.

inactivity-aging: relative aging mode. absolute-aging: absolute aging mode.

Parameter Description

Parameter	Parameter Description
inactivity-aging	Relative aging mode. The aging time starts when the MAC stops hitting.
absolute-aging	Absolute aging mode. Calculate aging time according to the timeline.

Default Value

The default is relative aging mode.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to set the aging mode to absolute aging mode.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)# switchport port-security mac absolute-aging
```

40.7.7 switchport port-security mac violation

Syntax

switchport port-security mac violation {**protect** | **restrict** | **shutdown**}
no switchport port-security mac violation

To configure the port security alarm action. When the number of learned MAC addresses exceeds the port limit, an alarm will be issued.

protect ： : no warning.

restrict: alarm. If there are too many total alarms, the port shutdown will be triggered.

shutdown: The port will enable the shutdown operation and issue an alarm.

Parameter Description

Parameter	Parameter Description
protect	No alarm is triggered, the default is protect mode.
restrict	The alarm is triggered.
shutdown	Trigger an alarm and shut down the port at the same time.

Default Value

The default is protecting type.

Command Mode

Interface configuration mode

Usage Guidelines

Physical Interface configuration mode

Example

The following example shows how to set the alert mode to restrict type.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)# switchport port-security mac violation restrict
```

40.8 Configuring Port Binding Commands

Syntax

switchport port-security bind | **block** {**ip** | **ipv6** | **arp** | **vlan** | **both-arp-ip***ip-addr* | **mac** *mac-addr*}

no switchport port-security bind | **block** {**ip** | **ipv6** | **arp** | **vlan** | **both-arp-ip***ip-addr* | **mac** *mac- addr*}

This command is used to configure the port's MAC and IP address binding.

Use the NO form of the command to delete the bound addresses one by one or delete all the addresses of the port and exit the port binding state.

Parameter Description

Parameter	Parameter Description	Value range
ip-addr	IP address	A.B.C.D
Mac-addr	Mac address	AA:BB:CC:DD:EE:FF

Default Value

None

Command Mode

Interface configuration mode

Usage Guidelines

This command must be configured in Layer 2 interface configuration mode.

The switch disables the port binding function by default. However, as long as a bind address is configured, the port will work in the bind state unless the NO form of this command is used to clear all bind entries.

Example

The following example shows how to configure port tg0/0/1 to bind IP address 1.2.3.4 and MAC address 00:01:00:01:11:11 and reject IP and ARP messages from the bound address.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#switch port port-security block both-arp-ip 1.2.3.4 mac 00:01:00:01:11:11
```

40.9 Configuring vlan mac Address Learning

Syntax

[**no**] **vlan disable-learning** {**add** *word* | **remove** *word* | *word*}

This command is used to configure VLAN address learning capability.

Parameter Description

Parameter	Parameter Description
word	Vlan IDs such as (1,3,5,7) or (1,3-5,7) or (1-7)

Default Value

VLAN learning is enabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

This command must be configured in Layer 2 Global Configuration Mode.

Example

The following example shows how to configure to disable VLAN 1 learning.

Switch(config)#vlandisable-learning 1

40.10 Configuring Link Scan Commands

Syntax

link scan {**normal** | **fast**} *interval*

no link scan [**normal** | **fast**]

This command is used to configure the port scan interval.

Parameter Description

Parameter	Parameter Description
normal | **fast**	Normal stands for standard link scanning mode. Fast stands for fast link scanning mode.
interval	Scanning interval, unit 1ms, 10-1000.

Default Value

The default scanning interval for normal mode is 500ms. The default scanning interval for fast mode is 10ms.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode. Fast mode is mainly used for cooperating with the protocol, such as RSTP. Normal mode is used for finding port up/down.

Example

The following example shows how to configure the switch to scan a port every 20 milliseconds.

Switch(config)#link scan normal 20

40.11 Configuring System MTU Commands

Syntax

system mtu *mtu* **no system mtu**

This command is used to configure the system's mtu value.

Parameter Description

Parameter	Parameter Description
mtu	Configures the value of system mtu, 1518-9216.

Default Value

Default Value of mtu is 9216 bytes.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in global configuration mode.

Example

The following example shows how to configure the value of system mtu to 2000 bytes.

```
Switch#config
Switch(config)#system mtu 2000
```

40.12 Port Traffic Counter Commands

40.12.1 show counters

Syntax

show counters [**nonzero** | **interface** *interface-type interface-number*]

This command is used to display the number of ingress messages, egress messages, ingress pps, and egress pps of the port.

Parameter Description

Parameter	Parameter Description
nonzero	Filter out ports whose data is all 0.
interface-type interface-number	Specify a port to display data.

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#show counters
Switch(config)#show counters interface tg0/0/1 Switch(config)#show counters nonzero
```

40.12.2 show counters rate

Syntax

show counters rate [**nonzero** | **interface** *interface-type interface-number*]

This command is used to display the utilization of the port in the ingress and egress and display the pps and number of error messages in the ingress and egress. You can select one or all ports to display or only display ports with non-zero data.

Parameter Description

Parameter	Parameter Description
nonzero	Filter out ports whose data is all 0.
interface-type interface-number	Specify a port to display data.

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#show counters rate
Switch(config)#show counters rate interface tg0/0/1
Switch(config)#show counters rate  nonzero
```

40.12.3 show counters error

Syntax

show counters error [**nonzero** | **interface** *interface-type interface-number*]

This command is used to display the number of various error message types in the ingress and egress. You can select one or all ports to display or only display ports with non-zero data.

Parameter Description

Parameter	Parameter Description
nonzero	Filter out ports whose data is all 0.
interface-type interface-number	Specify a port to display data.

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#show counters error
Switch(config)#show counters error interface tg0/0/1
Switch(config)#show counters error nonzero
```

40.12.4 show counters change

Syntax

show counters change [**interface** *interface-type interface-number*]

This command is used to display the counters of port message changes during the time interval between the last call of this command. You can select a port to display.

Parameter Description

Parameter	Parameter Description
interface-type interface-number	Specify a port to display data.

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#show counters change
Switch(config)#show counters change interface tg0/0/1
```

40.13 Port Traffic Alarm Commands

40.13.1 Configuring Alarm Utilization

Syntax

[**no**] **traffic notify** {**ingress** | **egress**} **utility** {**high** *high_value*} [**resume** *resume_value*]

This command is used to set a threshold, and a log prompt is generated when the port traffic reaches the threshold in the ingress and egress. This allows users to discover possible problems early. You can also set a recovery threshold. When the port traffic reaches the recovery threshold for a period of time, a recovery log is generated. It indicates that the port utilization is less than the set recovery threshold. In order to avoid alarm fluctuations, the threshold and recovery threshold values should be kept as far apart as possible.

Parameter Description

Parameter	Parameter Description
high_value	Alarm log traffic threshold.
resume_value	Resume log flow threshold.

Command Mode

Interface configuration mode

Usage Guidelines

By default, the log threshold of the interface's ingress and egress bandwidth utilization is 80, and the recovery threshold is 60. To cancel the command configuration, the threshold is restored to the default value.

Example

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)#traffic notify egress utility high 80 resume 60 Switch(config-tg0/0/1)#no traffic notify egress utility high
```

40.13.2 Configuring Alarm Switches and Intervals

Syntax

[**no**] **traffic notify** [**interval** *second*] {**syslog** | **trap-snmp**}

This command is used to configure the port traffic alarm interval, as well as the alarm mode, log alarm and trap alarm.

Parameter Description

Parameter	Parameter Description
second	Alarm time interval.

Command Mode

Global Configuration Mode

Usage Guidelines

You can use the show run command to check whether this function is enabled. To cancel the interval, restore the interval to the default value of 20.

Example

```
Switch(config)#traffic notify syslog
Switch(config)#traffic notify interval 60
```

40.13.3 Check Port Traffic Alarm Configuration Information

Syntax

show traffic [**interface** *interface-type interface-number* | **nondefault**]

This command is used to display the current alarm rate of the port configuration or the current non-default alarm rate of the port configuration.

Command Mode

Global Configuration Mode

Parameter Description

Parameter	Parameter Description
interface-type interface-number	Specify a port to display data.
nondefault	Filter out the ports configured by default.

Usage Guidelines

None

Example

```
Switch(config)#show traffic interface tg0/0/1 Switch(config)#show traffic nondefault
```

40.14 Configuring Port Dynamic MAC Addresses Learning Maximum

Syntax

[**no**] **switchport dynamic maximum** *num*

This command is used to configure port dynamic MAC addresses learning maximum.

Parameter Description

Parameter	Parameter Description
num	Configuring Port Dynamic MAC Addresses Learning Maximum. The maximum value is equal to the maximum of MAC address tables of this model. The value range and integer type can be selected according to the device prompt information after typing "?".

Default Value

The default value is not limited.

Command Mode

Interface configuration mode

Usage Guidelines

This command is configured in interface configuration mode.

Note the difference with **switchport port-security dynamic maximum** *max_num*.

This command limits the Maximum of port dynamic MAC addresses learning. The address in the port security dynamic mode is still a static address. This command is mutually exclusive with the port security mode.

Example

The following example shows how to configure the maximum of dynamic MAC addresses learning on tg0/0/1 to 100.

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)# switchport dynamic maximum 100
```

40.15 Configuring Port Split

Syntax

[**no**] **switchport flex-portmode** { **seperate** | **combined** } **write vos-config**

The 100G port of the switch can be split into 4 10G ports through the split command, and the split ports can also be merged through the command. After configuring the split and merge port commands, you need to use write vos-config to save the configuration and restart to take effect.

Parameter Description

Parameter	Parameter Description
seperate	Configuring 100G Port Splitting
combined	Configuring Split Ports for Merging

Command Mode

Interface configuration mode. (Save configuration commands in EXEC mode.)

Usage Guidelines

Splitting or merging requires saving the configuration, which will take effect after restart. [**no**] **switchport flex-portmode** is used to restore the default state before splitting. Models that support this function is XGS-6350-24X2C.

Example

The following example shows how to split the ctg0/0/1 port.

```
Switch(config)#interface cg0/0/1
Switch(config-cg0/0/1)# switchport flex-portmode separate
Switch(config-cg0/0/1)# ! Switch(config)#exit
Switch#write vos-config
```

Chapter 41 Port Physical Characteristic Configuration Commands

41.1 auto-nego

Syntax

auto-nego {*enable*|*disable*}

Parameter Description

Parameter	Parameter Description
enable	Enable port auto-negotiation mode
disable	Disable port auto-negotiation mode

Default Value

By default, auto-negotiation mode is disabled.

Command Mode

Port Configuration Mode

Usage Guidelines

The auto-nego command is used to enable or disable the port auto-negotiation mode.

Example

```
auto-nego enable
```

41.2 speed

Syntax

speed {*1000*| *10000*|*40000*| *100000*}

Parameter Description

Parameter	Parameter Description
1000	To set the port speed to 1000M
10000	To set the port speed to 10G
40000	To set the port speed to 40G
100000	To set the port speed to 100G

Default Value

By default, the speed of 10G fiber optical ports is 10000, and the speed of 100G fiber optical ports is 100000.

Command Mode

Port Configuration Mode

Usage Guidelines

The speed command is used to set the port to the corresponding speed.

Example

```
speed 1000
```

41.3 duplex

Syntax

duplex *full*

Parameter Description

Parameter	Parameter Description
full	To set the port to full-duplex mode.

Default Value

The fiber optical port is in full-duplex mode.

Command Mode

Port Configuration Mode

Usage Guidelines

The duplex is used to set the port to full-duplex mode.

Example

```
duplex full
```

41.4 fiber-auto

Syntax

fiber-auto {*enable*|*disable*}

Parameter Description

Parameter	Parameter Description
enable	The fiber optical port matches the appropriate speed according to the optical module in duplex mode.
disable	The fiber optical port disables the automatically identifying the optical module to match the speed in duplex mode.

Default Value

By default, automatically identifying the optical module to match the speed in duplex mode is enabled.

Command Mode

Port Configuration Mode

Usage Guidelines

The fiber-auto command is used to enable or disable automatically identifying the optical module to match the speed in duplex mode and in the FEC mode.

Example

fiber-auto enable

41.5 training

Syntax

training {*40G*| *100G*}

Parameter Description

Parameter	Parameter Description
40G	To enable 40G link training mode.
100G	To enable 100G link training mode.

Default Value

By default, training is disabled on the optical port.

Command Mode

40G and 100G in port configuration mode.

Usage Guidelines

This command is used to optimize the transmission performance of high-speed copper cables. It is enabled when there is packet loss in the access copper cable module.

Example

```
training 40G
```

41.6 fec

Syntax

fec mode {*rs*|*none*}

Parameter Description

Parameter	Parameter Description
rs	To enable FEC RS mode.
none	To disable FEC mode.

Default Value

By default, FEC is disabled on the optical port.

Command Mode

100GPort Configuration Mode

Usage Guidelines

FEC is an error correction technology. In general, when this function is enabled, the transmission distance of the high-speed optical module will be longer than when the FEC function is not enabled.

Example

```
fec mode rs
```

Chapter 42 QoS Configuration Commands

42.1 QoS Configuration Commands

42.1.1 cos default

Syntax

cos default *cos*

no cos default

This command is used to configure the default COS value.

Parameter Description

Parameter	Parameter Description
cos	The COS value by default ranges between 0 and 7.

Default Value

The default COS value is 0.

Command Mode

Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

This command is configured in Layer 2 Interface Configuration Mode or Global Configuration Mode

Example

The following example shows how to set the CoS value of the untagged frames received on port tg0/0/1 to 4.

Switch(config)#interface tg0/0/1

Switch(config-tg0/0/1)#cos default 4

42.1.2 cos map

Syntax

cos map *quid cos1..cosn* **no cos map**

To set the CoS priority queues, use the cos map command.

Parameter Description

Parameter	Parameter Description
quid	Stands for the ID of the CoS priority queue, 1 to 8.
cos1..cosn	CoS value defined by IEEE802.1p, ranging between 0 and 7

Default Value

CoS Value	S Priority Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in Global Configuration Mode

Using this command in Global Configuration Mode will affect all port CoS priority queues.

Example

The following example shows how to map CoS 0-2 to CoS priority queue 1 and CoS 3 to CoS priority queue 2.

```
Switch(config)# cos map 1 0 1 2 Switch(config)# cos map 2 3
```

42.1.3 cos map-local-priority

Syntax

cos map-local-priority *cos-value1* {**cos** *cos-value2* | **cng** *cng-bit*} **no cos map**

To remap internal CoS priority and congestion bit based on cos value, use the **cos map-local-priority** command.

Parameter Description

Parameter	Parameter Description
cos-value1	CoS value is defined by IEEE802.1p, ranging between 0 and 7.
cos-value2	Remapped internal priority cos value, ranging between 0 and 7
cng-bit	Congestion bits of cos mapping, GREEN (0), YELLOW(3), RED(1)

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in Global Configuration Mode

Using this command in Global Configuration Mode will affect all port CoS priority queues.

Example

The following example shows how to remap CoS 1 to internal CoS priority queue 5.

```
Switch(config)#cos map-local-priority 1 cos 5
```

42.1.4 cos bandwidth

Syntax

cos bandwidth *quid min-bandwidth max-bandwidth*

no cos bandwidth *quid*

To set the minimum bandwidth or the maximum bandwidth of the port cos queue, run this command.

Parameter Description

Parameter	Parameter Description
quid	Stands for the ID of the CoS priority queue, 1 to 8.
min-bandwidth	Stands for the minimum bandwidth. The unit is 64Kbps. Range depends on port type.
max-bandwidth	Stands for the maximum bandwidth. The unit is 64Kbps. Range depends on port type.

Default Value

The minimum bandwidth of each queue is 0 and the maximum bandwidth is the maximum rate of the physical port.

Command Mode

Interface Configuration Mode

Usage Guidelines

This command is configured in layer 2 Interface Configuration Mode. The scheduling policy is effective between the minimum and the maximum bandwidth. The data flow lower than the minimum bandwidth passes through and the data flows higher than the maximum bandwidth drops.

Example

The following example shows how to set the minimum bandwidth 100 and the maximum bandwidth 1000 on port g0/1.

```
Switch(config)#int tg0/0/1
Switch(config-tg0/0/1)#cos bandwidth 1 100 1000
```

42.1.5 dscp map

Syntax

dscp map *word* {**cos** *cos-value* | **cng** *cng-bit*} **no dscp map**

To set the CoS priority queues according to dscp, use the dscp map command.

Parameter Description

Parameter	Parameter Description
word	Dscp range table, for instance, (1,3,5,7) (1 ， 3-5,7)，(1-7).
cos-value	The priority cos of Dscp mapping, 0-7.
cng-bit	Congestion bits of DSCP mapping, GREEN(0), YELLOW (3), RED(1)

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in Global Configuration Mode

Example

Switch(config)#dscp map 0-2

The following example shows how to map dscp 0-2 to CoS priority queue 1 and the congestion is 0.

cos 1 cng 0

42.1.6 scheduler weight bandwidth

Syntax

scheduler weight bandwidth *weight1...weightn*

no scheduler weight bandwidth

To set the bandwidth of the CoS priority queue, run this command.

Parameter Description

Parameter	Parameter Description
weight1 … *weight8*	Values of eight CoS priority queues weights DRR/WRR/WFQ, weight1-2 range is 1-15, weight 3-8 range is 0-15, 0 is sp mode.

Default Value

The weight value of each CoS priority queue is the same. All weight values of eight CoS priority queues are 1.

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in Global Configuration Mode

If this command is enabled, the bandwidth of all priority queues on all ports are affected. This command validates only when the queue schedule mode is configured as drr/wrr/wfq. It determines the bandwidth weight value of the CoS priority queue when the drr/wrr/wfq scheduling policy is used.

Example

The following example shows how to configure eight CoS priority queues with weights of 1, 2, 3, 4, 5, 6, 7 and 8 respectively.

```
Switch(config)# scheduler weight bandwidth 1 2 3 4 5 6 7 8
```

42.1.7 scheduler policy

Syntax

scheduler policy {**sp | wrr | wfq | drr**}

no scheduler policy

To set the queue scheduling policy, use the scheduler policy command.

Parameter Description

Parameter	Parameter Description
sp	Uses the SP scheduling policy.
wrr	Uses the WRR scheduling policy.
wfq	Uses wfq scheduling policy.
drr	Uses drr scheduling policy.

Default Value

The SP schedule policy is used by default.

Command Mode

Global Configuration Mode

Usage Guidelines

Global Configuration Mode

After this command is configured, the schedule mode of the interface is set to the designated value.

Example

The following example shows how to send transmission schedule mode to WRR.

```
Switch(config)# scheduler policy drr
```

42.1.8 policy-map

Syntax

policy-map *name*

no policy-map *name*

To set the QoS policy map, run policy-map name.

Parameter Description

Parameter	Parameter Description
name	Name of the QoS policy map, consisting of 1 to 20 characters.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Global Configuration Mode

After the command is entered, the system enters the QoS policy mapping configuration mode. In this mode, the following commands are used:

1. **classify** ：Used to set the QoS flow.

2. **description** ：Used to describe the QoS policy map.

3. **exit** ： Used to exit from the QoS policy mapping configuration mode.

4. **no** ：Used to cancel the previously entered command.

5. **action** ：Used to define the QoS action.

Example

The following example shows how to set the QoS policy map.

```
Switch(config)# policy-map myqos
```

42.1.9 classify

Syntax

classify {**any** }{| **seq** *seq* | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp***dscp-value* | **ip***ip-access-list* | **mac** *mac-access-list* | **exp** *exp* |**tag-num** *tag-num*}

no classify {**seq** *seq* |**cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **ip** | **mac** | **tag- num**}

To configure the matchup data flow of the QoS policy map, run the above command.

Parameter Description

Parameter	Parameter Description
seq *seq*	Configures the matched seq value; the range is 1 to 100.The maximum value varies on different models.
any	Matches up with any packet.
cos *cos*	Configures the matched COS value; the range is 0 to 7
icos *icos*	Configures the matched interior tag COS value; the range is 0 to 7.
vlan *vlanid*	Configures the matched VLAN; the range is 1 to 4094
ivlan *ivlanid*	Configures interior tag vlan id. 1-4094.
ethernet-type *ethernet-type*	Configures the matched packet type, 0x0600-0xFFFF
precedence *precedence-value*	The priority field in tos of ip packet (5-7 of tos), 0-7.
dscp*dscp-value*	dscp field of tos in ip packet (2 to 7 of tos), 0~63
ip*ip-access-list*	Configures the name of the matched IP access list. The name has 1 to -20 characters.
mac *mac-access-list*	Configures the name of the matched MAC access list. The name has 1 to 20 characters.
exp *exp*	Configures the matched exp value; the range is 0 to 7
tag-num *tag-num*	Configures the matched tag-num value; the range is 0 to 1

Default Value

Any packet is matched by default (match any).

Command Mode

Global Configuration Mode

Usage Guidelines

QoS policy map configuration mode.

All data flows in a QoS policy map must have the same mask value, and the port number in the ip access-list must be specific, not a range.

The permit rules in the IP access list and MAC access list used to match data flows are effective. That is, the permit rules are used to match data flows, and the deny rules are not used to configure data flows.

When the qinq mode is enabled, then the dot1q-tunnel command is configured. When the downlink port matches the VLAN or COS value of the source message, the ivlan and icos should be configured.

Example

Switch(policy-map)#classify vlan 4

42.1.10 action

Syntax

| **action** [**seq** *seqnum*] { **bandwidth** *max-band* | **copy-to-cpu** | **cir** *commit-band* **bc** *commit-burst-size* {**pir** *pir-band* **be** *peak-burst-size*} | [**eir** *excess-band*] **ebs** *excess-burst-size* [**confirm** { **forward** |

discardable { **green** | **yellow** | **red** } } | **exceed** { **forward** | **drop** | **discardable** { **green** | **yellow** | **red** } } | **violate** { **forward** | **drop** | **discardable** {**green** | **yellow** | **red**} }] [**tcm-end**] | **cos** *cos* | **drop** \ |

precedence *precedence-value* | **forward** \ | **icos** *icos* | **ivlan** *ivlanid* | **monitor** *session-value* | **queue** *queue-value* | **redirect** *interface-id* | **stat-packet** |** stat-byte** | **vlanID** *vlanid*}

no action {**bandwidth** | **copy-to-cpu**\ | **cir** | **cos** | **drop** | **precedence**\ | **forward** | **icos** | **ivlan** |

monitor | **queue** | **redirect** | **stat-packet** | **stat-byte** | **vlanID** *vlanid*}

To configure the data flow policy of a QoS policy map, run the **action** command.

Parameter Description

Parameter	Parameter Description
seq *seq*	Configure the matched seq value, 1-100. The maximum value varies on different models.
bandwidth *max-band*	Configure the maximum bandwidth allowed for data flow, 1-163840, unit is 64Kbps.
copy-to-cpu	Forward the message to CPU.

cir *commit-band* **bc** *commit-burst-size* {**pir** *pir-band* **be** *peak-burst-size*} | [**eir** *excess-band*] **ebs** *excess-burst-size* [**confirm** { **forward** | **discardable** { **green** | **yellow** | **red** } } | **exceed** { **forward** | **drop** | **discardable** { **green** | **yellow** | **red** } } | **violate** { **forward** | **drop** | **discardable** {**green** | **yellow** | **red**} }] [**tcm-end**]	Configure policing, cir commit-band to guarantee bandwidth. The value range is 0-156250. The unit is 64Kbps; **bc** *commit-burst-size* indicates the burst packet size. The value range is 0-4096, the maximum value varies depending on the model, the unit is Kb; **pir** *pir-band* pir pir-band indicates peak bandwidth. The value range is 0-156250. The unit is 64Kbps; **be** *peak-burst-size* is the peak burst size, the value range is 0-4096, the maximum value varies according to the model, the unit is Kb; **eir** *excess-band* is the increment of peak bandwidth minus guaranteed bandwidth. The value range is 0-156250. Unit is 64Kbps; **ebs** *excess-burst-size* is the burst size of the eir increment, ranging from 0 to 4096. The maximum value varies according to the model. The unit is Kb; confirm: the action when the bandwidth is less than cir; forward: no action is performed; discardable: set the discard priority; Exceed: The bandwidth is greater than cir and less than pir. Forward: No action is performed. Drop: Drop. Discardable: Set the discard priority. violate: action when bandwidth is greater than pir; forward: no action is performed; drop: discard; discardable: set discard priority; tcm-end: end policing configuration.
cos *cos*	Set the matched flow cos priority of the outer VLAN. The value range is 0 - 7.
drop	Drops the matched messages.
precedence *precedence-value*	Set the priority field of TOS in the matched flow IP message (bits 5 to 7 of TOS). The value range is 0-7.
forward	No action is taken on the matched messages.
icos *icos*	Sets inner cos field matched with the flow to cos-value 0~7
ivlan *vlanid*	Set the inner vlanid of the matched flow, the value range is 1-4094.

monitor *session-value*	Set the matched message mirroring to the specified mirroring session, the value range is 1-4.
queue *queue-value*	Set mapping queue; the range is 1-8.
redirect *interface-id*	Set matched messages to be redirected to the specified port.
stat-packet	Calculates the number of messages.
stat-byte	Calculates the number of bytes.
vlanID *vlanid*	Set the outer vlanid, the range is 1-4094.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

QoS policy map configuration mode.

Only when sending double-tag messages, ivlan and icos are effective.

dscp, redirect, precedence, queue, vlan add, ivlan add/del do not support on the egress.

Example

```
Switch(policy-map)#action redirect tg0/0/1
```

42.1.11 qos policy

Syntax

[**no**] **qos policy** *name* {**ingress**|**egress**}

To configure the QoS policy of a port globally, run this command.

Parameter Description

Parameter	Parameter Description
name	The name of QoS policy mapping
ingress	Functions on the ingress port.
egress	Functions on the egress port.

Default Value

None

Command Mode

Global Configuration Mode, Interface Configuration Mode

Usage Guidelines

Layer 2 Interface Configuration Mode or Global Configuration Mode

Example

The following example shows how to configure the pmap QoS policy on port tg0/0/1.

```
Switch(config)#inter tg0/0/1
Switch(config-tg0/0/1)# qos policy pmap ingress
```

42.1.12 show policy-map

Syntax

show policy-map {*policy-map-name* | **interface** *interface-id* | **global**}

To display all or some designated QoS policy maps, run this command.

Parameter Description

Parameter	Parameter Description
policy-map-name	The name of a QoS policy map.
interface [*interface-id*]	The policy of interface application
global	The globally applied policies

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode

Usage Guidelines

None

Example

The following example shows how to display all QoS policy maps.

Note: When in the state of classifying any, action is empty, because it is the default value, show policy-map will not display the specific classify and action.

```
Switch(config)#show policy-map policy-map    1
classify any
action redirect tg0/0/1 policy-map    11
Switch(config)#
```

42.1.13 trust

Syntax

[**no**] **qos trust** { **cos** | **dscp** | **untrust** }

To configure the trust mode, run this command.

Parameter Description

Parameter	Parameter Description
cos	The name of the trust mode.
Parameter	Parameter Description
dscp	Differentiated Services Code Point
untrust	The name of the untrusted mode.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

This command is configured in Global Configuration Mode.

Example

The following example shows how to configure the trust cos mode.

```
Switch(config)#qos trust cos
```

Chapter 43 Loopback Detection Configuration Commands

43.1 Loopback Detection Configuration Commands

43.1.1 loopback-detection

[**no**] **loopback-detection**

To enable or disable global loopback detection, run the above command.

Parameter Description

None

Default Value

By default, the loopback detection function is disabled globally.

Command Mode

Global Configuration Mode

Usage Guidelines

None

Example

```
Switch#config   Switch(config)#
Switch(config)#loopback-detection
```

43.1.2 loopback-detection enable

[**no**] **loopback-detection enable**

To enable or disable the loopback detection of the port, run the above command.

Parameter Description

None

Default Value

By default, the loopback detection function of the port is disabled.

Command Mode

Interface Configuration Mode

Usage Guidelines

This command can be used to enable or disable loopback detection on a specified port. However, this setting takes effect only after loopback detection is enabled globally.

Example

```
Switch(config)#
Switch(config)#interface g0/0/1
Switch(config-g0/0/1)#loopback-detection enable
```

43.1.3 loopback-detection hello-time

[**no**] **loopback-detection hello-time** *hello-time*

To set the transmission period of loopback detection messages, run this command.

Parameter Description

Parameter	Parameter Description
hello-time	Stands for the transmission period of loopback messages, whose unit is second. The value ranges from 1 to 65535.

Default Value

1 second

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

None

43.1.4 loopback-detection recovery-time

[**no**] **loopback-detection recovery-time** *recovery-time*

To set the recovery time of a port after being controlled, run this command.

Parameter Description

Parameter	Parameter Description
recovery-time	Stands for the recovery time of a port after being controlled, whose unit is second. The value ranges from 10 to 65535.

Default Value

10 seconds

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

None

43.1.5 loopback-detection control

[**no**] **loopback-detection control** {*block*|*learning*|*shutdown*} To set a port to be controlled, run this command.

Parameter Description

Parameter	Parameter Description
block	Configure the controlled function of the port to block
learning	Configure the controlled function of the port to learning
shutdown	Configure the controlled function of the port to shutdown

Default Value

None

Command Mode

Interface Configuration Mode

Usage Guidelines

When a port detects loopback in its network, you can perform corresponding control actions to this port by setting control functions. The controlled states of a port include block (blocking the port), learning (forbidding MAC address learning of the port) and shutdown (closing the port). When any controlled state is configured and loopback is found on a port, the trap alarm message will be transmitted. The trap is configured by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection messages and receives the previously transmitted loopback detection messages. The port is configured with the following five controlled operations:

block: This means to block the port. When loopback is detected, this port will be isolated from other ports, and the data packets entering the port cannot be forwarded to other ports. This port will be configured in protocol down state and the MAC address table ages.

learning: This means to disable the port MAC address learning. When a loopback is detected, this port will disable the port MAC address learning and at the same time age its MAC address table.

shutdown: This means to shut down the port. When a loopback is detected, this port will not only transmit the trap message and age its MAC address. At the same time this port will also be automatically shut down(err-disable) so that it cannot transmit messages until the err-disable-recover time expires.

When the port is in the block state, the messages transmitted to this port cannot be forwarded. At the same time, this port will continue to transmit loopback detection messages. When loopback disappears, the port will recover automatically. By default, Loopback is considered to have disappeared if on loopback detection messages are received within 10 seconds.

When the port is in Block state, the port protocol is down; when it is in Shutdown state, the port link is directly down.

Example

```
Switch#config

Switch(config)#interface g0/0/1

Switch(config-g0/0/1)#loopback-detection control block
```

43.1.6 loopback-detection dest-mac

[**no**] **loopback-detection dest-mac** *mac-addr*

To set the destination MAC address of loopback detection messages on the port, run this command.

Parameter Description

Parameter	Parameter Description
mac-addr	Stands for the MAC address that corresponds to a MAC VLAN entry.

Default Value

The default destination MAC address is 01-80-C2-00-00-0a.

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#interface g0/0/1
Switch(config-g0/0/1)#loopback-detection dest-mac 00:11:11:11:11:11
```

43.1.7 loopback-detection existence

[**no**] **loopback-detection existence**

To configure whether a loopback exists on the port by default when this port is enabled or in link UP state, run this command.

Parameter Description

None

Default Value

Loopback is nonexistent by default.

Command Mode

Interface Configuration Mode

Usage Guidelines

This command is mainly used to solve the loopback problem on a port when this port is up and its loopback detection function is enabled. When the controlled action of this port is configured as shutdown, it is not advisable to configure the port to loopback state, because the port will no longer forward messages in the shutdown state. There is no loopback by default.

Example

None

43.1.8 loopback-detection frames-threshold

[**no**] **loopback-detection frames-threshold** *frames-threshold*

To configure the threshold of the loopback detection frame received every second, run this command.

Parameter Description

Parameter	Parameter Description
frames-threshold	Upper limit of loopback detection frames received per second (10-200)

Default Value

The default value is 10.

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

```
Switch(config)#interface g0/0/1
Switch(config-g0/0/1)#loopback-detection frames-threshold 20
```

43.1.9 loopback-detection frames-monitor

[**no**] **loopback-detection frames-monitor**

To configure whether to enable the frame monitor, run this command.

Parameter Description

None

Default Value

The default value is to disable the frame detection function.

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

```
Switch#config

Switch(config)#interface g0/0/1

Switch(config-g0/0/1)#loopback-detection frames-monitor
```

43.1.10 loopback-detection forbid-packet

[no] loopback-detection forbid-packet

To configure whether to enable the port to forbid the forwarding of loopback detection packets, run this command.

Parameter Description

None

Default Value

The default value is to disable the function of forbidding the forwarding of loopback detection packets.

Command Mode

Interface Configuration Mode

Usage Guidelines

None

Example

```
Switch#config
Switch(config)#interface g0/0/1
Switch(config-g0/0/1)#loopback-detection forbid-packet
```

43.1.11 show loopback-detection

show loopback-detection

To display the configuration details of loopback detection, run this command.

Parameter Description

None

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode or Interface Configuration Mode.

Usage Guidelines

This command is used to display the global or port loopback detection configurations and port status.

Example

```
Switch(config)#show loopback-detection Loopback-detection is enable

Loopback-detection packet 's sys Mac address: ac12.8e6b.0081


Interface state information

Port      Status  dest MacAddress   Control   VLAN


   tg0/0/1          no-loop    0180.c200.000a     WARNING

   tg0/0/2          no-loop    0180.c200.000a     WARNING

   tg0/0/3          no-loop    0180.c200.000a     WARNING
```

tg0/0/4	no-loop	0180.c200.000a	WARNING
tg0/0/5	no-loop	0180.c200.000a	WARNING
tg0/0/6	no-loop	0180.c200.000a	WARNING
tg0/0/7	no-loop	0180.c200.000a	WARNING
tg0/0/8	no-loop	0180.c200.000a	WARNING
g0/0/1	no-loop	0180.c200.000a	WARNING
g0/0/2	no-loop	0180.c200.000a	WARNING
g0/0/3	no-loop	0180.c200.000a	WARNING
g0/0/4	no-loop	0180.c200.000a	WARNING

43.1.12 show loopback-detection interface

show loopback-detection interface *intf-id*

To display the information of loopback detection interface, run this command.

Parameter Description

Parameter	Parameter Description
Interface *Intf-id*	Show the specified interface.

Default Value

None

Command Mode

EXEC Mode, Global Configuration Mode or Interface Configuration Mode.

Usage Guidelines

This command is mainly used to display the information of the loopback detection status.

Example

```
Switch#show loopback-detection interface g0/0/1

Receive Packets :0   Transmit Packets: 20 Discard Packets:0

HelloTimeOut:10   RecoverTimeOut:26
```

Chapter 44 Static Route Configuration Commands

44.1 Static Route Configuration Commands

44.1.1 ip route default

Syntax

ip route default {*gateway*|**blackhole**|**reject**} [*distance*] [**tag** *tag*]

no ip route default {*gateway*|**blackhole**|**reject**} [*distance*] [**tag** *tag*]

Parameter Description

Parameter	Parameter Description
gateway	Used to reach the next-hop IP address of that network
blackhole	Configures blackhole routing to prevent routing loops from being generated
reject	Drops the packet and sends the destination packet to the source host.
distance	(Optional) management distance (1-255)
tag *tag*	Sets a tag, which is used for matchup and route control.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure default route and the corresponding management distance.

Use the no form of this command to cancel the configuration.

Note

1. After the default route is configured, the packet will be forwarded through the default route once the None method matches a specific subnet route or host route.
2. The next-hop address specified by a static route cannot be configured as the IP address of the local interface.
3. The blackhole route is equivalent to a standby route in the event of a failure, so you can set the priority of the static blackhole route a little lower (the distance value is larger).

Example

The following command configures a default route that points to the next hop of 192.168.1.3.

Switch(config)# ip route default 192.168.1.3

44.1.2 ip route A.B.C.D

Syntax

ip route *A.B.C.D mask* {*gateway*|**blackhole**|**reject**} [*distance*] [**tag** *tag*]

no ip route *A.B.C.D mask* {*gateway*|**blackhole**|**reject**} [*distance*] [**tag** *tag*]

Parameter Description

Parameter	Parameter Description
A.B.C.D	Stands for destination address IP route prefix
mask	Destination address prefix mask
gateway	Used to reach the next-hop IP address of that network
blackhole	Configures blackhole routing to prevent routing loops from being generated
reject	Drops the packet and sends the destination unreachable packet to the source host.
distance	(Optional) management distance (1-255)
tag *tag*	Sets a tag, which is used for matchup and route control.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

The command is used to configure the static route and the corresponding management distance.

Use the no form of this command to cancel the configuration.

Note

1. Static routes can be configured for equivalent routes.
2. The next-hop address specified by a static route cannot be configured as the IP address of the local interface.
3. The blackhole route is equivalent to a standby route in the event of a failure, so you can set the priority of the static blackhole route a little lower (the distance value is larger)

Example

The following command configures a static route that points to the next hop of 192.168.11.1.

Switch(config)# ip route 10.1.1.0 255.255.255.0 192.168.11.1

44.1.3 ip route bfd static nexthop

Syntax

To enable the reachability detection function in the ping form, run the first one of the following commands. To disable the function with the no form of this command.

ip route bfd static nexthop

no ip route bfd static nexthop

Parameter Description

None

Default Value

Disabled

Command Mode

Global Configuration Mode

Usage Guidelines

Use the ip route bfd static nexthop command to enable reachability detection in the form of ping, obtain the reachability status of the configured test items, and add/delete related route entries in the route table based on the results

Example

The following command enables ping detection.

Switch(config)#ip route bfd static nexthop

44.1.4 ip route ping

Syntax

To configure the static route with pind detection entry, run the following command.

To delete the route configuration, run the no form of this command.

ip route *prefix mask gateway* **ping** [*rmtaddr*&<1~4> [**strict-mode**]] [*distance*] [**tag** *tag*]

no ip route *prefix mask gateway*

Parameter Description

Parameter	Parameter Description
prefix	Destination IP route prefix
mask	Destination address prefix mask
gateway	The next-hop IP address to the destination address
ping	This route uses ping detection
rmtaddr	The remote address throughing next hop, configure 0~4
strict- mode	The route detection mode, can be used to determine the route reachable status
distance	Management distance. The configuration range: 1-255.
tag	Set a tag, used for match and control the route. The configuration range is 1 to 4294967295.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Use the ip route ping command to configure a route, which will use ping to check reachability.

Among them, 0~4 remote addresses of rmtaddr can be configured, and if not configured, the route is directly determined according to the next-hop reachability. When you configure a remote address, determine whether the route is reachable based on the detection mode and the reachability of the remote address.

The route detection mode can only be set when the remote address is configured, and the default loose-mode is that as long as a remote address is reachable, it is regarded as route reachable; If strict-mode is set to strict-mode, all remote addresses are reachable before the route is reached.

If the route detection result is unreachable, the route entry is deleted from the route table.

Example

The following command configures the static route with next hop as 192.168.3.3 and enable ping detection.

Switch(config)#ip route 3.3.3.3 255.255.255.0 192.168.3.3 ping

The following command configures the static route in strict-mode with reachability based on multiple remote address.

Switch(config)#ip route 3.3.3.3 255.255.255.0 192.168.3.3 ping 192.168.2.1 192.168.1.1 strict-mo

44.1.5 ip route bfd

Syntax

To configure the static route with bfd detection entry, run the following command.

To delete the route configuration, run the no form of this command.

ip route *prefix mask gateway* **bfd** [*distance*] [**tag** *tag*]

no ip route prefix mask gateway

Parameter Description

Parameter	Parameter Description
prefix	Destination IP route prefix
mask	Destination address prefix mask
gateway	The next-hop IP address to the destination address
bfd	This route uses bfd detection
distance	Management distance. The configuration range: 1-255.
tag	Set a tag, used for match and control the route. The configuration range is 1 to 4294967295.

Default Value

None

Command Mode

Global Configuration Mode

Usage Guidelines

Use the ip route bfd command to configure a route, which will use bfd to detect reachability, add standard bfd detection items, and add/delete the corresponding route entries in the route table based on the detection results.

Example

The following command configures a static route with the next hop of 192.168.3.3 and enable bfd detection.

Switch(config)#ip route 3.3.3.3 255.255.255.0 192.168.3.3 bfd

44.1.6 ip route bfd query interval

Syntax

To configure the detection time interval of pind detection, run the following command.

To delete the configuration, run the no form of this command.

ip route bfd query interval *value*

no ip route bfd query interval

Parameter Description

Parameter	Parameter Description
value	Detection internal, the configuration range: 1-65535（ *100ms ）

Default Value

The detection interval 10*100ms

Command Mode

Global Configuration Mode

Usage Guidelines

Use the command "ip route bfd query interval" to configure the detection interval of ping detection. The unit is 100ms.

Note: query interval must be greater than reply interval.

Example

The following command configures the query interval to be 2000ms.

Switch(config)#ip route bfd query interval 20

Related Command

ip route bfd reply interval

44.1.7 ip route bfd reply interval

Syntax

To configure the reply timeout interval for ping detection, run the following command.

To delete the configuration, run the no form of this command.

ip route bfd reply interval *value*

no ip route bfd reply interval

Parameter Description

Parameter	Parameter Description
value	Reply timeout internal. The configuration range: 1-65535（ *100ms ）

Default Value

The reply timeout interval is 1*100ms.

Command Mode

Global Configuration Mode

Usage Guidelines

Use the command "ip route bfd reply interval" to configure the timeout interval of receiving reply packet. The unit is 100ms.

The "query interval" must be greater than "reply interval".

Example

The following command configures the timeout interval to be 200ms.

Switch(config)#ip route bfd query interval 2

Related Command

ip route bfd query interval

44.1.8 show ip route static

Syntax

show ip route static [json]

Parameter Description

Parameter	Parameter Description
json	Displays json format result.

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Displays static route.

Note

Used for checking static route table information.

Example

The following command displays the static route:

Switch# show ip route static

44.1.9 show static-route json

Syntax

show static-route json

Parameter Description

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Display the static route in the json format.

Note:

Used to check the static routing table information.

Example

The following command shows the static route.

Switch# show route-static json

44.1.10 show ip static bfd info

Syntax

Displays the detection configuration and information about all configured detection items, including ping and BFD detection items

show ip static bfd info

Parameter Description

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Use the command "show ip static bfd info" to print the detection item information, and view the detection interval configuration, the number of configured detection items, the specific detection item configuration information (next hop, remote address, detection item type), and the detection status (outbound port, reachable status)

Example

The following commands prints the information of the detecion entries.

Switch(config)#show ip static bfd info

query interval = 5000ms reply interval = 2000ms bfd_detect_nh_counter = 3

gateway	rmaddr	type	ifname	state
192.168.2.2	192.168.2.2	ping	vlan2	unreachable

gateway	rmaddr	type	ifname	state
192.168.3.3	192.168.3.3	bfd	vlan27	reachable

gateway

192.168.2.2

rmaddr
192.168.4.2
type ping
ifname vlan2
state
unreachable

Switch(config)#

The table below shows the definition of of each domain:

Domain	Description
gateway	Next hop IP address
rmaddr	The remote IP address that passes through the next hop (the rmaddr is the same as the gateway in the next hop detection item)
type	The type of the detection entry: ping/bfd
ifname	Egress name
state	State：reachable/unreachable

44.1.11 debug staticd

Syntax

[**no**] **debug staticd** [**zebra**|**event**|**all**]

Parameter Description

Parameter	Parameter Description
no	Disable the static route monitor
zebra	Monitor the interaction between the static route and zebra
event	Monitor the static route event
all	Enable or disable debug staticd zebra and debug static event simultaneously

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The command is used to the interaction between the static route and zebra and the static route event.

Note

None

Example

The following command monitors the static route.

Switch# debug staticd zebra Switch# debug staticd event

Chapter 45 IP Address Configuration Commands

45.1 IP Address Configuration Commands

45.1.1 arp static

Syntax

To configure a static ARP mapping, the static ARP mapping will persist in the ARP table while the interface VLAN exists and cannot be deleted by the Clear command or ARP aging. To delete the configured static arp mapping, use the no arp static command. If the interface VLAN has not been created, the configuration fails.

arp static *ip-address hardware-address vlan*

no arp static *ip-address vlan*

Parameter

Parameter	Parameter Description
ip-address	The IP address of the local data link interface.
hardware-address	The physical address of the local data link interface.
vlan	The vlan port ID of the static arp [1-4094].

Default Value

None, no static ARP mapping in the ARP cache.

Command Mode

Global Configuration Mode

Usage Guidelines

Most hosts can support dynamic ARP resolution, so you don't need to configure static ARP mappings for hosts. In most cases, **no arp static** *ip_address vlan* is used to delete static ARP. If the interface VLAN port to which a static ARP belongs is deleted, the static ARP will also be deleted.

Example

The following command configures IP address in vlan 1 is 1.1.1.1. The MAC address for the host is 00:12:34:56:78:90 of the static arp.

```
Switch(config)#arp static 1.1.1.1 00:12:34:56:78:90  1
```

45.1.2 arp timeout

Syntax

To enable arp aging and enable dynamic arp mac detection, run the command.

[no] arp timeout

Parameter

None

Default Value

The aging function and the arp mac detection is enabled.

Command Mode

Global Configuration Mode

Usage Guidelines

After the ARP timeout is enabled, each dynamic ARP will have a separate aging timer, and a targeted ARP check will be sent after a certain period of time, and the ARP will be deleted if the ARP is not updated for a long time. In addition, the commands under the related arp timeout will revert to the default values when the arp timeout command is configured without enabling aging.

Example

The following command enables arp dynamic aging function.

```
Switch(config)#arp timeout
```

45.1.3 arp timeout scan_intervel

Syntax

To configure the interval at which the ARP cache actively reprobes point-to-point ARP requests, run the following command.

arp timeout scan_intervel *minutes*

no arp timeout scan_intervel

Parameter

Parameter	Parameter Description
minutes	Configures the interval at which the ARP cache actively reprobes point-to-point ARP requests (minute) [1-255].

Default Value

10 minutes

Command Mode

Global Configuration Mode

Usage Guidelines

After the ARP timeout is enabled, the dynamic ARP has an aging time, and the ARP is deleted after the aging time expires.

Example

The following command sets the interval for ARP active reprobing to be 2 minutes.

```
Switch(config)#arp timeout scan_intervel 2
```

Related Command

arp timeout stale_threshold

arp timeout pending_timeout

45.1.4 arp timeout stale_threshold

Syntax

To configure the aging detection time of dynamic ARP, run the following command.

arp timeout stale_threshold *minutes*

no arp timeout stale_threshold

Parameter

Parameter	Parameter Description
minutes	Configures the aging detection time (minutes) for dynamic ARP [1-255].

Default Value

4x the ARP timeout scan_intervel time

Command Mode

Global Configuration Mode

Usage Guidelines

This command sets the dynamic ARP aging time, and if the ARP update has not been received during this time, it will be deleted, and the default time is four times the detection time, which is modified with the change of the detection time configuration, unless it is configured.

Example

The following command configures the dynamic ARP deletion time to 10 minutes.

```
Switch(config)#arp timeout stale_threshold 10
```

Related Command

arp timeout scan_intervel

45.1.5 arp timeout pending_timeout

Syntax

To configure the deletion time of an incomplete ARP, run the following command.

arp timeout pending_timeout *minutes*

no arp timeout pending_timeout

Parameter

Parameter	Parameter Description
minutes	Configures the deletion time (minutes) of an incomplete ARP [1-255].

Default Value

2xarp timeout scan_intervel time

Command Mode

Global Configuration Mode

Usage Guidelines

The incomplete ARP deletion time is separated from the other dynamic ARP deletion time, and the default is twice the probe time, which is modified when the probe time configuration changes, unless it is configured.

Example

The following command sets the deletion time for incomplete ARP to be 3 minutes.

```
Switch(config)#arp timeout pending_timeout 3
```

Related Command

arp timeout scan_intervel

arp timeout stale_threshold

45.1.6 arp timeout dynamic_arp_mac_check_enable

Syntax

To configure whether to enable MAC address detection for dynamic ARP, run the following command.

[no] arp timeout dynamic_arp_mac_check_enable

Parameter

None

Default Value

MAC detection is enabled by default.

Command Mode

Global Configuration Mode

Usage Guidelines

By default, only MAC address detection is available for static ARP, and the physical egress of static ARP is updated according to the MAC table egress, and whether dynamic ARP detection is enabled needs to be configured, because the detection is polled for a long time and occupies a certain amount of CPU resources.

Example

The following command configures the MAC Detection to enable dynamic ARP.

```
Switch(config)#arp timeout dynamic_arp_mac_check_enable
```

Related Command

arp timeout mac_check_interval

45.1.7 arp timeout mac_check_interval

Syntax

To configure the interval between MAC checks for ARP, run the following command.

arp timeout mac_check_interval *seconds*

no arp timeout mac_check_interval

Parameter

Parameter	Parameter Description
seconds	Interval (seconds) for mac examination of ARP [1-255].

Default Value

3 seconds

Command Mode

Global Configuration Mode

Example

The following command sets the MAC check time for ARP to be 2 seconds.

```
Switch(config)#arp timeout mac_check_intervel 2
```

Related Command

arp timeout dynamic_arp_mac_check_enable

45.1.8 clear arp

Syntax

To clear the dynamic ARP cache, run the following command.

clear arp [*ip-address* { *mask* | *vlan vlanid* }]

Parameter

Parameter	Parameter Description
ip-address	IP or subnets
mask	Subnets mask
vlanid	VLAN ID

Default Value

None

Command Mode

EXEC mode

Example

The following command removes all dynamic entries from the ARP cache:

```
Switch(config)#clear arp
```

Related Command

arp static

45.1.9 ip address

Syntax

To set an IP address and mask for an interface, use the **ip address** command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast addresses and broadcast addresses cannot be used (all host sections are 1'). Other than the Ethernet, multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range ot the Ethernet interface cannot be the same as the arbitrary interfaces of other types. You should configure the primary address before configuring the secondary address. Also, you should delete all secondary addresses before deleting the primary address. IP packets generanted by the system, if the upper application does not specify the soruce address, the router will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the router will use the primary address of the sending interface.

If the ip address is not configured on an interface, it is not the unnumbered interface, and then this interface will not deal with any IP packet. To remove an IP address or disable IP processing, use the no form of this command.

ip address *ip-address mask* [**secondary**]

no ip address [*ip-address mask*]

Parameter

Parameter	Parameter Description
ip-address	IP address
mask	IP mask
secondary	(optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Default Value

No IP address is defined for the interface.

Command Mode

Port configuration mode, 3-layer vlan port

Usage Guidelines

If any OLT on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses

Example

In the following command, 202.0.0.1 is the primary address, 255.255.255.0 is the mask and 203.0.0.1 and 204.0.0.1 are secondary addresses for Ethernet interface vlan10:

```
Switch(config)#interface          vlan10
Switch(config-vlan10)#ip          address     202.0.0.1     255.255.255.0
Switch(config-vlan10)#ip          address     203.0.0.1     255.255.255.0       secondary
Switch(config-vlan10)#ip          address     204.0.0.1     255.255.255.0       secondary
```

45.1.10 show arp

Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, use the **show arp** command.

show arp

Parameter

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The display information includes:

Display	Display Description
ARP total num	Displays the overall arp amount
Address	Displays the network address that maps with the physical address. IP address, for example.
Hardware Address	Displays the physical address that corresponds to the network address. It is empty for the unanalyzed entries.
Interface	Displays the vlan, physical port, and the stacked slot number
Age	Displays the survival time. The time when the ARP entry was last updated to the present. Unit: minutes.

Example

The following command displays the ARP cache:

```
Switch#show    arp
ARP total num:1

Address             Hardware Address       Interface                  Age

2.1.1.2             00:10:94:00:00:03      v2(g1/0/18)[1]             0
```

45.1.11 show arp local

Syntax

To display the local MAC-IP mapping of all VRRP protocol settings (called local arp), run the command.

show arp local

Parameter

None

Default Value

None

Command Mode

EXEC mode

Usage Guidelines

The display information includes:

Display	Display Description
Local Arp total num	Displays the local arp amount
IP4	IPV4 network address mapped to physical address
Ethernet	Physical address: The physical address corresponding to the network address, which is blank for entries that have not yet been resolved.
Interface	Affiliated VLAN

Example

The following command displays local arp:

```
Switch(config)#show arp local Local Arp total num:1
IP4                Ethernet           Interface
1.1.1.5            00:00:5e:00:01:01  vlan1
```

45.1.12 show arp statistics

Syntax

To display ARP related statistics entry, run the following command.

show arp statistic

Parameter

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, and Port Configuration Mode

Usage Guidelines

The display information includes:

Display	Display Description
Total number	Includes amount of the overall arp, uncomplete arp, and complete arp
Total cache	Totoal cache amount
Deliver hardware entry statistics	Includes statistics on the number of issued entries and the number of returned entries

Example

The following command displays ARP statistics:

```
switch_config#show arp statistics Total ARP:1

Complete ARP:0, Incomplete ARP:1 Total cache:0

HWRT operate wait:29 HWRT operate over:29
```

45.1.13 show arp timeout

Syntax

To display the configuration information about ARP aging detection, run the following command.

show arp timeout

Parameter

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The display information includes:

Display	Display Description
current time	Time recording after power-on
Full scan interval	Time recording after power-on
Stale purge threshold	The deletion time when the ARP is not updated
Incomplete timeout	The deletion time of the incomplete ARP
Mac check on dynamic arp	Whether to perform MAC MAC detection on dynamic ARP
Mac check interval	Mac detection interval

Example

The following command displays the ARP aging detection configuration information:

```
Switch(config)#show arp timeout
IP neighbor scan enabled for IPV4 neighbors - current time is 1112893.0822 sec
Full scan interval: 1 min
Stale purge threshold: 4 min
Incomplete timeout:2 min
Mac check on dynamic arp:Enable Mac check interval: 3 sec
```

45.1.14 show ip interface

Syntax

To display the IP configuration on the interface, run the following command.

show ip interface {*intf-name* | **brief**}

Parameter

Parameter	Parameter Description
intf-name	(optional) interface name
brief	(optional) Displays the IP protocol brief of al vlan ports

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

If the interface link layer is usable, the line protocol is marked "Up." If you configure IP address on this interface, the router will add a direct route to the routing table. If the link layer protocol is marked "Down", the direct route will be deleted. This command displays the specified interface information if specified interface type and number, or IP configuration information of all interfaces will be displayed.

Example

The following command shows how to display IP configuration on interface vlan10.

```
Switch#show ip interface
vlan10 vlan10 is up
  Internet address is 1.1.1.1/24
  Broadcast address is 1.1.1.255
  Secondary address 11.1.1.1/24
  Secondary address 22.1.1.1/24
  MTU is 1500 bytes
```

Display description:

Domain	Description
vlan 10 is up	Interface status
IP address	Interface main IP address and network mask
Broadcast address	Interface broadcast address
Secondary address	Interface secondary IP address and network mask
MTU	Interface IP MTU.

The following command displays the brief of all IP interfaces.

```
Switch#show ip interface brief
Interface   IP-Address  Method  Status
vlan10      1.1.1.1     manual   UP
loopback10  10.1.1.1    manual    UP
```

Display description:

Domain	Description
Interface	Interface name
IP-Address	Interface main IP address
Method	Interface main IP address type (static or dynamic)
Status	Interface status

45.1.15 show ip cache

Syntax

To display all forwarding cache entries after the hardware entries are delivered, run the following command.

show ip cache clear arp

Parameter

None

Default Value

None

Command Mode

EXEC mode, Global Configuration Mode, Port Configuration Mode

Usage Guidelines

The IP cache clears the displayed information when the egress arp is deleted, including:

Display	Display Description
Cache total num	The overall IP cache amount
number	Serial number.
Dst ip	Address. A network address mapped to a physical address, such as an IP address.

Example

The following command displays ip cache:

```
switch#show ip cache Cache total num:0

Number          Dst ip
```

Related Command

clear arp

Chapter 46 DHCP Client Configuration Commands

46.1 DHCP Client Configuration Commands

The chapter describes the DHCP configuration commands. These commands are used to configure and monitor the DHCP running on the OLT.

46.1.1 ip address dhcp

Syntax

Run the **ip address dhcp** command to obtain an IP address for the interface through the dynamic host configuration protocol (DHCP). Run the **no ip address dhcp** command to delete the obtained IP address.

[no] ip address dhcp

Parameter

None

Default Value

None

Command Mode

Port configuration mode, 3-layer vlan port

Usage Guidelines

The ip address dhcp command allows an interface to obtain an IP address via the DHCP protocol, which is useful for dynamically connecting Internet Service Providers (ISPs) over an Ethernet interface.

If the ip address dhcp command is configured, the OLT will send a DHCPDISCOVER message to the DHCP server on the network. If the no ip address dhcp command is configured, the OLT will send a DHCPRELEASE message.

Example

The following command enables the vlan11 interface to obtain the IP address of the interface through DHCP:

Switch(config)#interface vlan11

Switch(config-vlan11)#ip address dhcp

Chapter 47 Applying IP Access List Configuration Commands

47.1 Applying IP Access List Configuration Commands

47.1.1 ip access-group

Syntax

To control access to an interface, run the ip access-group interface configuration command. To delete this specified access group, use the no form of this command.

1. Appling on the port

[**no**] **ip access-group** *name* [**egress**] [**stat-packet** | **stat-byte**]

2. Applying on the global

[**no**] **ip access-group** *name* [**vlan** {*word* | *add* | *remove*}] [**egress**] [**stat-packet** | **stat-byte**]

To apply the created IP access list to the port or global or delete the IP access list that has been applied to the port or the global IP access list, run the above command.

Parameter Description

Parameter	Parameter Description
name	The name of the access list, 1-20 characters in length.
vlan	The access list is applied to the ingress VLAN
word	vlan range table. For example, (1,3,5,7) or (1,3-5,7) or (1-7)
add	Adds a VLANID to the current configuration list
remove	Deletes the VLANID from the current configuration list
egress	The access list is applied in the egress direction.
stat-packet	Statistics based on the number of packets
stat-byte	Statistics based on newspaper sections

Command Mode

Global Configuration Mode, Port Configuration Mode

Usage Guidelines

Most of the rules in the access list are implemented through hardware, and the parts that are not supported by the hardware do not prompt errors, but have no practical effect; A small number of such as time-range are implemented by the software.

Note:

The IPv4 standard access list supports:

Field	Description
any	Any source IP address
source-addr source-mask	Source address match

IPV4 expand access list supports:

Field	Description
any	Any source IP address
Ip-protocol	IP protocol number
Ip-addrip-mask	IP address match
Interface *interface-id*	3-layer interface match
eq/gt/lt/neq/src-portrange/dst-portrange	tcp/udp port number match
totallen	IP packet length match
tos/is-fragment/not-fragment/precedence/ttl/offset-not-zero/offset-zero/donotfragment-set/ donotfragment-notset	Packet domain match, among which ttl must be set to equal a certain value.
tos	Packet tos priority match
cos	Packet cos priority match
precedence	packet precedence priority match

Example

The following example applies the access list filter on the entry of the Ethernet interface tg0/0/1:

```
Switch(config)#interface tg0/0/1
Switch(config-tg0/0/1)# ip access-group filter
```

Chapter 48 System Monitoring Commands

48.1 show temperature

Syntax

show temperature

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the temperature of each temperature node and its normal temperature range.

Example

```
show temperature
chassis0 slot0 BOARD temperature(Celsius): current: 42
high threshold: 70 low threshold: -10

chassis0 slot0 SWITCH temperature(Celsius): current: 74
high threshold: 100 low threshold: -10

chassis0 slot0 PON-MAC temperature(Celsius):
current: 57
high threshold: 100 low threshold: -10
```

48.2 show fan

Syntax

show fan

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the fan status of the host (or the chasis).

Example

```
show fan

fan1:
fan speed: 0 r/min
fan speed-precent: 27%
fan max-speed: 13500 r/min   present(yes) status(WRONG)

fan2:
fan speed: 0 r/min
fan speed-precent: 27%
fan max-speed: 13500 r/min   present(yes) status(WRONG)

fan3:
fan speed: 0 r/min
fan speed-precent: 27%
fan max-speed: 13500 r/min   present(yes) status(WRONG)

fan4:
fan speed: 0 r/min
fan speed-precent: 27%
fan max-speed: 13500 r/min   present(yes) status(WRONG)
```

48.3 show cpu

Syntax

show cpu

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the CPU utilization rate within 1 second, 1 minute, and 5 minutes.

Example

```
Switch#show cpu
chassis0 slot0 CPU utilization for one second: 3%; one minute: 6%; five minutes: 6%
Switch#
```

48.4 show memory

Syntax

show memory

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the related information of the current memory.

48.5 show power

Syntax

show power

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the host (or the chasis) power supply information.

Example

```
Switch#show power

power1:
present(yes) status(OK)

power2:
not present
```

48.6 show power-master

Syntax

show powe-master

Parameter Description

None

Default Value

None

Command Mode

EXEC and configuration mode

Usage Guidelines

The command is used to display the power supply status information of the local power chip, such as output voltage and current.

Chapter 49 Stacking (bvss) Configuration Example

49.1 2pcs Switch Stacking

Topology

Stacking Configuration

S1 Configuration:

```
S1_config#bvss
S1_config_bvss#
S1_config_bvss#bvss enable
S1_config_bvss#bvss mode normal
S1_config_bvss#bvss domain-id 1
S1_config_bvss#bvss member-id 1
S1_config_bvss#bvss priority 200
S1_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 1
S1_config_bvss#exit
S1#write bvss-config
S1#reboot
```

S2 Configuration:

```
S2_config#bvss
S2_config_bvss#
S2_config_bvss#bvss enable
S2_config_bvss#bvss mode normal
S2_config_bvss#bvss domain-id 1
S2_config_bvss#bvss member-id 2
S2_config_bvss#bvss priority 100
S2_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 2
S2_config_bvss#exit
S2#write bvss-config
S2#reboot
```

49.2 3pcs Switch Stacking

Topology

Stacking Configuration

S1 Configuration:

```
S1_config#
S1_config#bvss
S1_config_bvss#bvss enable
S1_config_bvss#bvss mode enhanced
S1_config_bvss#bvssdomain-id 1
S1_config_bvss#bvss member-id 1
S1_config_bvss#bvss priority 200
S1_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 1
S1_config_bvss#exit
S1#write bvss-config
S1#reboot
```

S2 Configuration:

```
S2_config#
S2_config#bvss
S2_config_bvss#bvss enable
S2_config_bvss#bvss mode enhanced
S2_config_bvss#bvss domain-id 1
S2_config_bvss#bvss member-id 2
S2_config_bvss#bvss priority 190
S2_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 2
S2_config_bvss#bvss interface 2 type tgigaEthernet port 2 group 1
S2_config_bvss#exit
S2#write bvss-config
S2#reboot
```

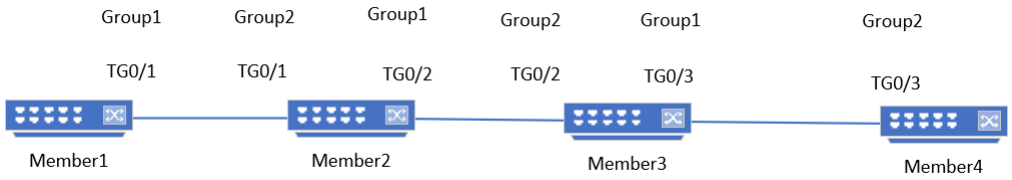
S3 Configuration:

```
S3_config_bvss#
S3_config_bvss#bvss enable
S3_config_bvss#bvss mode enhanced
S3_config_bvss#bvss domain-id 1
S3_config_bvss#bvss member-id 3
```

S3_config_bvss#bvss priority 180
S3_config_bvss#bvss interface 2 type tgigaEthernet port 2 group 2
S3_config_bvss#exit
S3#write bvss-config
S3#reboot

49.3 4pcs SWITCH Stacking

Topology



Stacking Configuration

Member 1:

Switch_config#bvss

Switch_config_bvss#bvss enable

Switch_config_bvss#bvss mode enhanced

Switch_config_bvss#bvss domain-id 1

Switch_config_bvss#bvss member-id 1

Switch_config_bvss#bvss priority 200

Switch_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 1

Switch_config_bvss#exit

Switch#write bvss-config

Switch#reboot

Member 2:

Switch_config#bvss

Switch_config_bvss#bvss enable

Switch_config_bvss#bvss mode enhanced

Switch_config_bvss#bvss domain-id 1

Switch_config_bvss#bvss member-id 2

Switch_config_bvss#bvss priority 190

Switch_config_bvss#bvss interface 1 type tgigaEthernet port 1 group 2

Switch_config_bvss#bvss interface 2 type tgigaEthernet port 2 group 1

Switch_config_bvss#exit

Switch#write bvss-config

Switch#reboot

Member 3:

Switch_config#bvss

Switch_config_bvss#bvss enable

Switch_config_bvss#bvss mode enhanced

Switch_config_bvss#bvss domain-id 1

Switch_config_bvss#bvss member-id 3

Switch_config_bvss#bvss priority 180

Switch_config_bvss#bvss interface 2 type tgigaEthernet port 2 group 2

Switch_config_bvss# bvss interface 3 type tgigaEthernet port 3 group 1

Switch_config_bvss#exit

Switch#write bvss-config

Switch#reboot

Member 4:

Switch_config#bvss

Switch_config_bvss#bvss enable

Switch_config_bvss#bvss mode enhanced

Switch_config_bvss#bvss domain-id 1

Switch_config_bvss#bvss member-id 4

Switch_config_bvss#bvss priority 170

Switch_config_bvss# bvss interface 3 type tgigaEtherne port 3 group 2

Switch_config_bvss#exit

Switch#write bvss-config

Switch#reboot