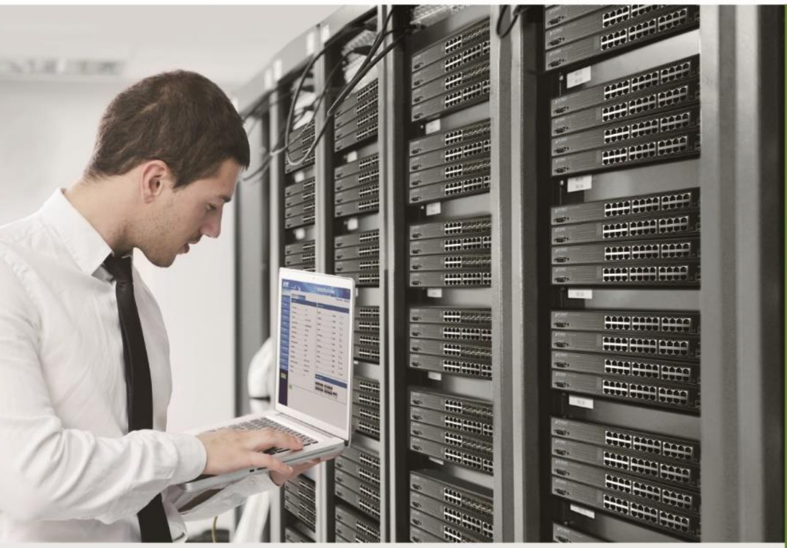
User’s Manual

PLANET Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch

- ► GS-6311 Series
- ► MGS-6311 Series
- ► XGS-6311 Series



www.PLANET.com.tw

Trademarks

Contents are subject to revision without prior notice.
PLANET is a registered trademark of PLANET Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

WEEE Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation.

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

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

Revision

User's Manual of PLANET Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch

Models: GS-6311-24T4X, GS-6311-24HP4X, GS-6311-16S8C4XR, GS-6311-48T6X, GS-6311-48P6XR,

MGS-6311-8P2X, MGS-6311-10T2X, XGS-6311-12X

Revision: 1.0

Part No: EM-GS-6311_MGS-6311_XGS-6311 Series_v1.0

Contents

Chapter 1 INTRODUCTION

Thank you for purchasing Layer 3 Gigabit/10 Gigabit Managed Ethernet Switch

The descriptions of these models are as follows:

Model	Description
XGS-6311-12X	Layer 3 12-Port 10GBASE-X SFP+ Managed Ethernet Switch
GS-6311-24T4X	L3 24-Port 10/100/1000T + 4-Port 10G SFP+ Managed Ethernet Switch
GS-6311-16S8C4XR	L3 16-Port 100/1000X SFP + 8-Port Gigabit TP/SFP + 4-Port 10G SFP+ Managed Ethernet Switch with 36-72V DC Redundant Power
GS-6311-48T6X	L3 48-Port 10/100/1000T + 6-Port 10G SFP+ Managed Ethernet Switch
GS-6311-24HP4X	L3 8-Port 2.5GBASE-T 802.3at PoE + 2-Port 10GBASE-T + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch
GS-6311-48P6X	L3 48-Port 10/100/1000T 802.3at PoE + 6-Port 10G SFP+ Managed Ethernet Switch
MGS-6311-10T2X	L3 8-Port 2.5GBASE-T + 2-Port 10GBASE-T + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch
MGS-6311-8P2X	L3 8-Port 2.5GBASE-T 802.3at PoE + 2-Port 10GBASE-X SFP+ Managed Ethernet Switch

1.1 Packet Contents

Unless specified, "**Managed Switch**" mentioned in this users manual refers to the GS-6311-24T4X, GS-6311-24HP4X, GS-6311-16S8C4XR, GS-6311-48T6X, GS-6311-48P6X .

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

Item / Model	Quick Installation Guide Sheet	DB9 to RJ45 Console Cable	Rack-mount Accessory Kit	SFP Dust Cap	AC Power Cord	Rubber Feet
XGS-6311-12X	■	■	■	12	1	4
GS-6311-24T4X	■	■	■	4	1	4
GS-6311-16S8C4XR	■	■	■	28	1	4
GS-6311-48T6X	■	■	■	6	1	4
GS-6311-24HP4X	■	■	■	4	1	4
GS-6311-48P6X	■	■	■	6	1	4
MGS-6311-10T2X	■	■	■	2	1	4
MGS-6311-8P2X	■	■	■	2	1	4

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

1.2 Product Description

Powerful 10Gbps and Layer 3 Routing Solution for Enterprise Backbone and Data Center Networking

PLANET M(X)GS-6311 series is a Layer 3 Managed Gigabit Switch that provides high-density performance, **Layer 3 static routing, RIP (Routing Information Protocol)** and **OSPF (Open Shortest Path First).** With **10Gbps** interfaces, the M(X)GS-6311 series can handle extremely large amounts of data in a secure topology linking to an enterprise backbone or high-capacity servers. The powerful network security features make the M(X)GS-6311 series perform effective data traffic control for ISP and enterprise VoIP, video streaming, and multicast applications.

The hardware specifications of these models are shown below:

Models	Copper	Fiber	PoE Ports	Power Input
XGS-6311-12X	--	12 1G/10G SFP+	--	AC
GS-6311-24T4X	24 10/100/1G RJ45	4 1G/10G SFP+	--	AC
GS-6311-24HP4X	24 10/100/1G RJ45	4 1G/10G SFP+	8bt + 16at	AC
GS-6311-16S8C4XR	8 (combo) 10/100/1G RJ45	24 100/1G SFP 4 1G/10G SFP+	--	AC + DC
GS-6311-48T6X	48 10/100/1G RJ45	6 1G/10G SFP+	--	AC
GS-6311-48P6X	48 10/100/1G RJ45	6 1G/10G SFP+	48at	AC
MGS-6311-102X	8 10/100/1G/2.5G RJ45 2 100/1G/2.5G/5G/10G RJ45	2 1G/10G SFP+	--	AC
MGS-6311-8P2X	8 10/100/1G/2.5G BASET	2 1G/10G SFP+	8at	AC

High Performance 10Gbps Ethernet Capacity

The two to six SFP+ ports built in the M(X)GS-6311 series boasts a high-performance switch architecture that is capable of providing non-blocking switch fabric and wire-speed throughput as high as up to **120Gbps**, which greatly simplifies the tasks of upgrading the LAN for catering to increasing bandwidth demands. Each of the SFP+ ports supports **Dual-Speed, 10GBASE-SR/LR** or **1000BASE-SX/LX**, meaning the administrator now can flexibly choose the suitable SFP/SFP+ transceiver according to the transmission distance or the transmission speed required to extend the network efficiently.

Redundant Ring, Fast Recovery for Critical Network Applications

The M(X)GS-6311 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 15ms to quickly bring the network back to normal operation.

Layer 3 Routing Support

The M(X)GS-6311 series enables the administrator to conveniently boost network efficiency by configuring Layer 3 static routing manually, the **RIP** (Routing Information Protocol) or **OSPF** (Open Shortest Path First) settings automatically.

- The RIP can employ the hop count as a routing metric and prevent routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.
- The OSPF is an interior dynamic routing protocol for autonomous system based on link state. The protocol creates a database for link state by exchanging link states among Layer 3 switches, and then uses the Shortest Path First algorithm to generate a route table based on that database.

Strong Multicast

The M(X)GS-6311 series supports abundant multicast features. In Layer 2, it features IPv4 IGMPv1/v2/v3 snooping and IPv6 MLD v1/v2 snooping. With Multicast VLAN Register (MVR), multicast receiver/sender control and illegal multicast source detect functions which make the M(X)GS-6311 series great for any robust networking.

Full IPv6 Support

The M(X)GS-6311 series provides **IPv6 management** and enterprise-level secure features such as **SSH, ACL, WRR** and **RADIUS** authentication. It thus helps the enterprises to step in the IPv6 era with the lowest investment. In addition, you don't need to replace the network facilities when the IPv6 FTTx edge network is built.

Robust Layer 2 Features

The M(X)GS-6311 series can be programmed for basic switch management functions such as port speed configuration, port aggregation, VLAN, Multiple Spanning Tree Protocol, bandwidth control and IGMP snooping. This switch provides 802.1Q tagged VLAN, Q-in-Q, voice VLAN and GVRP Protocol functions. By supporting port aggregation, the M(X)GS-6311 series allows the operation of a high-speed trunk combined with multiple ports. It enables up to 64 groups for trunking with a maximum of 8 ports for each group.

Excellent Layer 2 to Layer 4 Traffic Control

The M(X)GS-6311 series is loaded with powerful traffic management and WRR features to enhance services offered by telecoms. 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. It also empowers the enterprises to take full advantage of the limited network resources and guarantees the best in VoIP and video conferencing transmission.

Powerful Network Security

The M(X)GS-6311 series offers comprehensive Layer 2 to Layer 4 **Access Control List** (ACL) for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP address, TCP/UDP ports or defined typical network applications. Its protection mechanism also comprises 802.1x Port-based, MAC-based and web-based user and device authentications, which can be deployed with RADIUS, to ensure the port level security and block illegal users.

Advanced IP Network Protection

The M(X)GS-6311 series also provides DHCP Snooping, IP Source Guard and Dynamic ARP Inspection functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. The network administrators can now construct highly-secure corporate networks with considerably less time and effort than before.

Efficient and Secure Management

For efficient management, the M(X)GS-6311 series is equipped with console, Web and SNMP management interfaces.

- With the built-in Web-based management interface, the M(X)GS-6311 series offers an easy-to-use, platform-independent management and configuration facility.
- For text-based management, it can be accessed via Telnet and the console port. For reducing product learning time, the M(X)GS-6311 series offers Cisco-like command and customer doesn't need to learn new command from these switches
- For standard-based monitor and management software, it offers SNMPv3 connection which encrypts the packet content at each session for secure remote management.

Moreover, the M(X)GS-6311 series offers secure remote management by supporting SSHv2 connection which encrypts the packet content at each session.

Intelligent SFP Diagnosis Mechanism

The M(X)GS-6311 series supports **SFP-DDM** (**Digital Diagnostic Monitor**) function that greatly helps network administrator to easily monitor real-time parameters of the SFP and SFP+ transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

Centralized Power Management for Gigabit Ethernet PoE Networking

To fulfill the needs of higher power required PoE network applications with Gigabit speed transmission. The GS-6311-24HP4X features 8 10/100/1000BASE-T high-performance Gigabit IEEE 802.3bt PoE++ up to 90 watts on port 1~port 8 and 16 IEEE 802.3at PoE+ up to 32 watts on port 9~port 24. The GS-6311-48P6X features 48 10/100/1000BASE-T high-performance Gigabit IEEE 802.3at PoE+ up to 32 watts on port 1~port 48.It perfectly meets the power requirements of PoE VoIP phone and all kinds of PoE IP cameras such as IR, PTZ, speed dome cameras or even box type IP cameras with built-in fan and heater.

The GS-6311-24P4X's PoE capabilities also help to reduce deployment costs for network devices as a result of freeing from the restrictions of power outlet locations. Power and data switching are integrated into one unit, delivered over a single cable and managed centrally. It thus eliminates the cost for additional AC wiring and reduces installation time.

PoE Schedule for Energy Savings

Besides being used for IP surveillance, the GS-6311-24HP4X and GS-6311-48P6X are certainly applicable to build any PoE network including VoIP and wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the GS-6311 PoE Series can effectively control the power supply besides its capability of giving high watts power. The “PoE schedule” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save energy and budget.

1.3 Product Features

- **Physical Ports**

GS-6311-24T4X

- **24 10/100/1000BASE-T** RJ45 copper ports (Ports 1 to 24)
- **4 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 25 to 28)
- RJ45 to DB9 console interface for switch basic management and setup

GS-6311-24HP4X

- 8 10/100/1000BASE-T with **90W 802.3bt PoE++** injector function (Ports 1 to 8)
- 16 10/100/1000BASE-T with **32W 802.3at PoE+** injector function (Ports 9 to 24)
- **4 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 25 to 28)
- RJ45 to DB9 console interface for switch basic management and setup

GS-6311-16S8C4XR

- 24 100/1000BASE-X SFP ports (Ports 1 to 24)
- **8 10/100/1000BASE-T RJ45** copper ports, shared with (Ports 1 to 8)
- **4 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

GS-6311-48T6X

- **48 10/100/1000BASE-T RJ45** copper ports (Ports 1 to 48)
- **6 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 49 to 54)
- RJ45 to DB9 console interface for switch basic management and setup

GS-6311-48P6X

- 48 10/100/1000BASE-T with **32W 802.3at PoE+** injector function
- **6 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

MGS-6311-8P2X

- 8 10/100/1000/2500BASE-T ports with 32W 802.3at PoE+ injector function
- 2 10GBASE-SR/LR SFP+ slots, compatible with 1000BASE-SX/LX/BX SFP
- RJ45 to DB9 console interface for switch basic management and setup

MGS-6311-10T2X

- **8** 10/100/1000**/2500BASE-T** RJ45 copper ports (Ports 1 to 8)
- **2** 100/1G/2.5G/5G/**10GBASE-T** RJ45 auto-negotiation copper ports (Ports 9 to 10)
- **2 10GBASE-SR/LR SFP+** slots, compatible with 1000BASE-SX/LX/BX SFP (Ports 11 to 12)
- RJ45 to DB9 console interface for switch basic management and setup

XGS-6311-12X

- **12 10GBASE-SR/LR SFP+** slots, backward compatible with 1000BASE-SX/LX/BX SFP
- RJ45 type RS232 console interface for switch basic management and setup

- **IP Routing Features**
  - IP routing protocol supports **RIPv1/v2**, **OSPFv2**
  - Routing interface provides per VLAN routing mode
  - Supports route redistribution

- **Layer 2 Features**
  - Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standard
  - 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 detection
  - 16K ~ 32K MAC address table, automatic source address learning and aging
  - Supports VLAN

- IEEE 802.1Q tag-based VLAN
- GVRP for dynamic VLAN management
- 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
- IP subnet VLAN

  - Supports Link Aggregation
    - Maximum 64 trunk groups, 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)
    - Supports 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
  - Support for 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
  - Supports IPv6 MLD v1 and v2 snooping
  - Querier mode support
  - Supports Multicast VLAN Register (MVR)

- **Security**
  - IEEE 802.1x port-based network access authentication
  - MAC-based network access authentication
  - Built-in RADIUS client to cooperate with the RADIUS servers for IPv4 and IPv6
  - TACACS+ login users access authentication
  - IP-based Access Control List (ACL)
  - MAC-based Access Control List
  - Supports DHCP snooping
  - Supports ARP inspection
  - **IP Source Guard** prevents IP spoofing attacks
  - **Dynamic ARP Inspection** discards ARP packets with invalid MAC address to IP address binding

- **Management**
  - Management IP for IPv4 and IPv6
  - Switch Management Interface

    - Console/Telnet Command Line Interface
    - Web switch management
    - SNMP v1, v2c, and v3 switch management
    - SSH/TLS secure access
  - BOOTP and DHCP for IP address assignment
  - Firmware upload/download via TFTP or HTTP Protocol for IPv4 and IPv6
  - SNTP (Simple Network Time Protocol) for IPv4 and IPv6
  - User privilege levels control
  - Syslog server for IPv4 and IPv6
  - Supports DDM
  - Four RMON groups 1, 2, 3, 9 (history, statistics, alarms and events)
  - Supports sFlow
  - Supports ULDP
  - Supports ULPP (Uplink Protection Protocol)
  - Supports ULSM (Uplink State Monitor protocol)
  - Supports LLDP/LLDP MED
  - Supports DHCP Option82/43/60/61/67
  - Supports ping, trace route function for IPv4 and IPv6
  - PLANET Smart Discovery Utility for deployment management

- **Power over Ethernet**

GS-6311-24HP4X

- Complies with IEEE 802.3bt Power over Ethernet Plus Plus
- 8 IEEE 802.3bt PoE++ up to 90 watts on port 1~port 8
- 16 IEEE 802.3at PoE+ up to 32 watts on port 9~port 24
- Maximum 480-watt PoE budget

GS-6311-48P6X

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 48 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- 110VAC supports maximum 500-watt PoE budget
- 220VAC supports maximum 600-watt PoE budget

MGS-6311-8P2X

- Complies with IEEE 802.3at/af Power over Ethernet Plus
- Up to 8 ports of IEEE 802.3af/802.3at devices powered
- Supports PoE power up to 32 watts for each PoE port
- Supports maximum 150-watt PoE budget

- Auto detects powered device (PD)
- Circuit protection prevents power interference between ports
- Remote power feeding up to 100 meters
- PoE management
  - Total PoE power budget control
  - Per port PoE function enable/disable
  - PoE port power feeding priority
  - Per PoE port power limitation
  - PD classification detection
- Intelligent PoE features
  - PD alive check
  - PoE schedule

- **Redundant Power System**

GS-6311-16S8C4XR

- 100~240V AC / 36 -72V DC dual power redundancy
- Active-active redundant power failure protection
- Backup of catastrophic power failure on one supply

1.4 Product Specifications

Product	**GS-6311-24T4X**	**GS-6311-24HP4X**	**GS-6311-16S8C4XR**	**GS-6311-48T6X**	**GS-6311-48P6X**
Hardware Specifications					
10/100/1000 RJ45 Ports	24	24	8 (combo)	48	48
100/1000BASE-X SFP Ports	--	--	24	--	--
10G SFP+ Ports	4	4	4	6	6
	10GBASE-SR/LR SFP+ interface Backward compatible with 1000BASE-SX/LX/BX SFP transceiver				
Console Port	1 x RJ45-to-RS232 serial port (9600, 8, N, 1)				
CPU	MIPS 800MHz				
RAM	512Mbytes				
Flash Memory	32Mbytes				
Dimensions (W x D x H)	440 x 207 x 44mm	440 x 207 x 44mm	440 x 260 x 44mm	440 x 260 x 44 mm	440 x 330 x 44mm
Weight	2742g	3542g	3495g	3676g	5368g
Power Consumption	23.2 watts/79.11 BTU	15 watts / 51.1BTU (System)	36.2 watts/ 102.9 BTU	53.7 watts/183BTU	39.9 watts/ 136BTU (System)
		540 watts/ 1841.4 BTU (System+PoE)			698 watts/ 2380 BTU (System+PoE)
Power Requirements- AC	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC: 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Power Requirements - DC	--	--	DC: 36~72V	--	--
Fan	--	2	2	1	5
LED	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)
	Ports: LNK/ACT (Green)	**Ports:** LNK/ACT (Green) PoE-in-Use (Amber)	**Ports:** LNK/ACT (Green)	**Ports:** LNK/ACT (Green)	**Ports:** LNK/ACT (Green) PoE-in-Use (Amber)
Switching Specifications					
Switch Architecture	Store-and-forward				
Switch Fabric	128Gbps/non-blocking			216Gbps/non-blocking	
Switch Throughput	95.23Mpps			160.7Mpps	
Address Table	16K MAC address table with auto learning function			32K MAC address table with auto learning function	
ARP Table	8K	8K	8K	8K	8K
Routing Table	6K	6K	6K	12K	12K
IP Interface	1024	1024	1024	1024	1024

ACL Table	2K	2K	2K	4K	4K
Shared Data Buffer	12MB	12MB	12MB	16MB	16MB
Jumbo Frame	12KBytes				
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex				
Power over Ethernet Specifications					
PoE Standard	--	IEEE 802.3bt PoE++ PSE (Ports 1 to 8) IEEE 802.3af/at PoE+ PSE (Ports 9 to 24)	--	--	IEEE 802.3at PoE+ PSE
PoE Power Supply Type	--	End-span/Mid-span/802.3bt (Ports 1 to 8) End-span (Ports 9 to 24)	--	--	End-span
PoE Power Output	--	Port 1-8 90W (max), Port 9-24 32W (max)	--	--	32W(MAX)
Power Pin Assignment	--	End-span: 1/2 (-), 3/6 (+) Mid-span: 4/5 (+), 7/8 (-) 802.3bt: 1/2 (-), 3/6 (+), 4/5 (+), 7/8 (-)	--	--	1/2(+), 3/6(-)
PoE Power Budget	--	480 watts (max.)	--	--	500W/110VAC 600W/220VAC
IPv4 Layer 3 Functions					
IP Routing Protocol	Static route RIPv1/v2 OSPFv2				
Layer 3 Protocol	ARP ARP Proxy IGMP Proxy				
IPv6 Layer 3 Functions					
Other	ICMPv6,ND,DNSv6				
Layer 2 Functions					
Port Configuration	Port disable/enable Flow control disable/enable				

	Bandwidth control on each port Port loopback detect
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status
VLAN	802.1Q tagged VLAN, up to 4K VLAN groups 802.1ad Q-in-Q (VLAN stacking) GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN IP subnet VLAN
Bandwidth Control	TX/RX/Both
Link Aggregation	IEEE 802.3ad LACP/static trunk Supports 64 groups with 8 ports per trunk group
QoS	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: - IEEE 802.1p CoS/ToS - IPv4/IPv6 DSCP - Port-based WRR
Multicast	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR) Up to 1024
Security Functions	
Access Control List	Supports Standard and Expanded ACL IP-based ACL/MAC-based ACL Time-based ACL Up to 2K entries
Security	Port isolation 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 82/43/60/61/67 Command line authority control based on user levels
AAA	TACACS+ and IPv4/IPv6 over RADIUS
Authentication	IEEE 802.1x port-based network access control
Switch Management Functions	
System Configuration	Console, Telnet, Web browser, SNMP v1, v2c
Secure Management Interfaces	SSHv2, TLSv1.2, SNMPv3
Management	IPv4 and IPv6 dual stack management User IP security inspection for IPv4/IPv6 SNMP SNMP v1, v2c and v3 SNMP MIB and TRAP SNMP RMON 1, 2, 3, 9 four groups IPv4/IPv6 FTP/TFTP IPv4/IPv6 NTP RADIUS authentication for IPv4/IPv6 Telnet user name and password IPv4/IPv6 SSH The right configuration for users to adopt RADIUS server's shell management CLI, console, Telnet Security IP safety net management function: avoid unlawful landing at nonrestrictive area Syslog server for IPv4 and IPv6 TACACS+ PLANET Smart Discovery Utility
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Internet Engineering Task Force RFC 1271 RMON RFC 1354 IP-Forwarding MIB RFC 1493 Bridge MIB RFC 1643 Ether-like MIB RFC 1907 SNMP v2 RFC 2011 IP/ICMP MIB RFC 2012 TCP MIB RFC 2013 UDP MIB RFC 2096 IP forward MIB RFC 2233 if MIB RFC 2452 TCP6 MIB RFC 2454 UDP6 MIB RFC 2465 IPv6 MIB RFC 2466 ICMP6 MIB RFC 2573 SNMP v3 notify RFC 2574 SNMP v3 vacm

	RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB) RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)
Standard Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit 1000BASE-SX/LX IEEE 802.3ab Gigabit 1000BASE-T IEEE 802.3ae 10Gb/s Ethernet IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1ag CFM 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 IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet PLUS IEEE 802.3bt 4-pair Power over Ethernet Plus Plus RFC 768 UDP RFC 783 TFTP RFC 793 TCP 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 RFC 3810 MLD v2 RFC 2328 OSPF v2 RFC 1058 RIP v1 RFC 2453 RIP v2 ITU-T G.8032 ERPS Ring
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

Product	**MGS-6311-8P2X**	**MGS-6311-10T2X**	**XGS-6311-12X**
Hardware Specifications			
10/100/1000/2500 RJ45 Ports	8	8	--
100/1G/2.5G/5G/10G RJ45 Ports	--	2	--
10G SFP+ Ports	2	2	12
	10GBASE-SR/LR SFP+ interface Backward compatible with 1000BASE-SX/LX/BX SFP transceiver		
Console Port	1 x RJ45-to-RS232 serial port (9600, 8, N, 1)		
CPU	MIPS 800MHz		
RAM	512Mbytes		
Flash Memory	32Mbytes		
Dimensions (W x D x H)	330 x 230 x 43.6 mm, 1U height	330 x 230 x 43.6 mm, 1U height	330 x 230 x 43.6 mm, 1U height
Weight	2172g	1953g	1988g
Power Consumption	10.7 watts / 36.4BTU (System)	26.6 watts/ 90.7 BTU	30.2 watts/102.9 BTU
	174 watts/ 593.3 BTU (System+PoE)		
Power Requirements- AC	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz	AC 100~240V, 50/60Hz
Fan	1	1	1
LED	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)	**System:** PWR (Green), SYS (Green)
	Ports: **Per 2.5GBASE-T RJ45 Ports:** 2500Mbps LNK/ACT (Green) 10/100/1000Mbps LNK/ACT (Amber) 802.3at/af PoE-in-Use (Amber) **Per 10GBASE-X SFP Ports:** 10G LNK/ACT (Green) 1G LNK/ACT (Amber)	**Ports:** **Per 2.5GBASE-T RJ45 Ports:** 2500Mbps LNK/ACT (Green) 10/100/1000Mbps LNK/ACT (Amber) **Per 10GBASE-T RJ45 Ports:** 10G LNK/ACT (Green) 100/1G/2.5G/5G LNK/ACT (Amber) **Per 10GBASE-X SFP Ports:** 10G LNK/ACT (Green) 1G LNK/ACT (Amber)	**Ports:** 10G LNK/ACT (Green) 1G LNK/ACT (Amber)
Switching Specifications			
Switch Architecture	Store-and-forward	Store-and-forward	Store-and-forward

Switch Fabric	80Gbps/non-blocking	120Gbps/non-blocking	240Gbps/non-blocking
Switch Throughput	59.52Mpps	89.28Mpps	178.56Mpps
Address Table	16K MAC address table with auto learning function	16K MAC address table with auto learning function	32K MAC address table with auto learning function
ARP Table	8K	8K	8K
Routing Table	6K	6K	12K
IP Interface	1024	1024	1024
ACL Table	4K	4K	4K
Shared Data Buffer	12MB	12MB	16MB
Multicast Table	1K	1K	1K
Jumbo Frame	12KBytes		
Flow Control	Back pressure for half duplex IEEE 802.3x pause frame for full duplex		
Power over Ethernet Specifications			
PoE Standard	IEEE 802.3at PoE+ PSE	--	--
PoE Power Supply Type	End-span	--	--
PoE Power Output	32W(max.)	--	--
Power Pin Assignment	1/2(-), 3/6(+)	--	--
PoE Power Budget	150 watts (max.)	--	--
IPv4 Layer 3 Functions			
IP Routing Protocol	Static route RIPv1/v2 OSPFv2		
Layer 3 Protocol	ARP ARP Proxy IGMP Proxy		
IPv6 Layer 3 Functions			
Other	ICMPv6,ND,DNSv6		
Layer 2 Functions			
Port Configuration	Port disable/enable Flow control disable/enable Bandwidth control on each port Port loopback detect		
Port Status	Display each port's speed duplex mode, link status, flow control status and auto negotiation status		
VLAN	802.1Q tagged VLAN, up to 4K VLAN groups 802.1ad Q-in-Q (VLAN stacking) GVRP for VLAN management Private VLAN Edge (PVE) supported Protocol-based VLAN MAC-based VLAN		

	IP subnet VLAN
Bandwidth Control	TX/RX/Both
Link Aggregation	IEEE 802.3ad LACP/static trunk Supports 64 groups with 8 ports per trunk group
QoS	8 priority queues on all switch ports Supports strict priority and Weighted Round Robin (WRR) CoS policies Traffic classification: - IEEE 802.1p CoS/ToS - IPv4/IPv6 DSCP - Port-based WRR
Multicast	IPv4 IGMP v1/v2/v3 snooping IPv4 Querier mode support IPv6 MLD v1/v2 snooping Multicast VLAN Register (MVR) Up to 1024
Security Functions	
Access Control List	Supports Standard and Expanded ACL IP-based ACL/MAC-based ACL Time-based ACL Up to 4K entries
Security	Port isolation 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 82/43/60/61/67 Command line authority control based on user levels
AAA	TACACS+ and IPv4/IPv6 over RADIUS
Authentication	IEEE 802.1x port-based network access control
Switch Management Functions	
System Configuration	Console, Telnet, Web browser, SNMP v1, v2c
Secure Management Interfaces	SSHv2, TLSv1.2, SNMPv3
Management	IPv4 and IPv6 dual stack management User IP security inspection for IPv4/IPv6 SNMP SNMP v1, v2c and v3 SNMP MIB and TRAP SNMP RMON 1, 2, 3, 9 four groups IPv4/IPv6 FTP/TFTP IPv4/IPv6 NTP RADIUS authentication for IPv4/IPv6 Telnet user name and password IPv4/IPv6 SSH The right configuration for users to adopt RADIUS server's shell management CLI, console, Telnet Security IP safety net management function: avoid unlawful landing at nonrestrictive area Syslog server for IPv4 and IPv6

	TACACS+ PLANET Smart Discovery Utility
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Internet Engineering Task Force RFC 1271 RMON RFC 1354 IP-Forwarding MIB RFC 1493 Bridge MIB RFC 1643 Ether-like MIB RFC 1907 SNMP v2 RFC 2011 IP/ICMP MIB RFC 2012 TCP MIB RFC 2013 UDP MIB RFC 2096 IP forward MIB RFC 2233 if MIB RFC 2452 TCP6 MIB RFC 2454 UDP6 MIB RFC 2465 IPv6 MIB RFC 2466 ICMP6 MIB RFC 2573 SNMP v3 notify RFC 2574 SNMP v3 vacm RFC 2674 Bridge MIB Extensions (IEEE 802.1Q MIB) RFC 2674 Bridge MIB Extensions (IEEE 802.1P MIB)
Standard Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit 1000BASE-SX/LX IEEE 802.3ab Gigabit 1000BASE-T IEEE 802.3ae 10Gb/s Ethernet IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1ag CFM 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 IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet PLUS RFC 768 UDP RFC 783 TFTP RFC 793 TCP 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 RFC 3810 MLD v2 RFC 2328 OSPF v2 RFC 1058 RIP v1 RFC 2453 RIP v2 ITU-T G.8032 ERPS Ring
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 5 ~ 90% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

Chapter 2 Installation

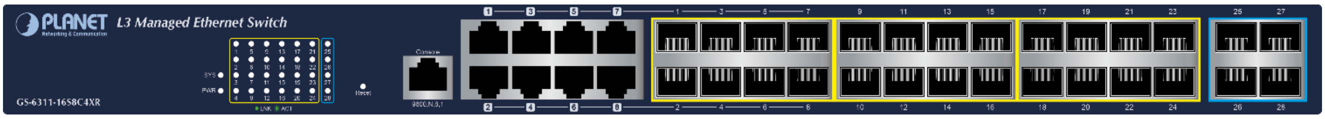
This section describes the hardware features and installation of the Managed Switch on the desktop or rack mount. For easier management and control of the Managed Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators.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

2.1 Hardware Description

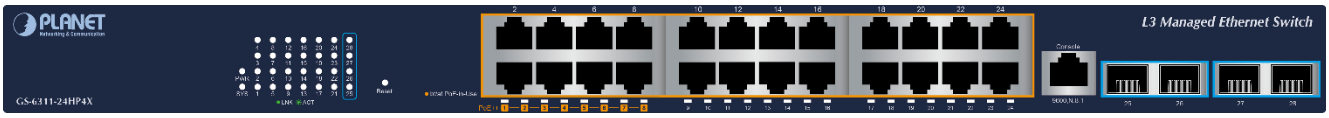
2.1.1 Switch Front Panel

The unit front panel provides a simple interface monitoring the switch. Are show the front panel of the Managed Switches as belwo.

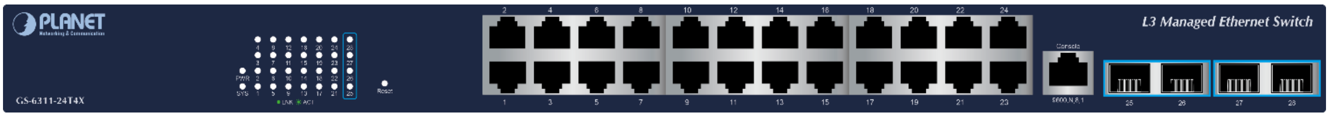
GS-6311-16S8C4XR Front Panel



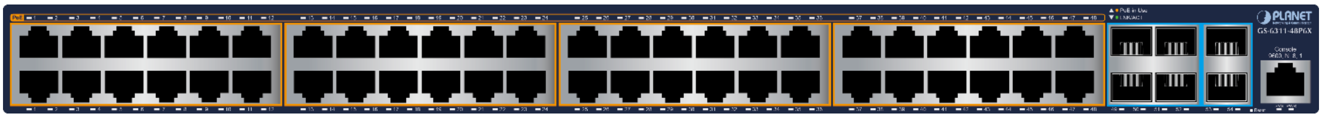
GS-6311-24HP4X Front Panel



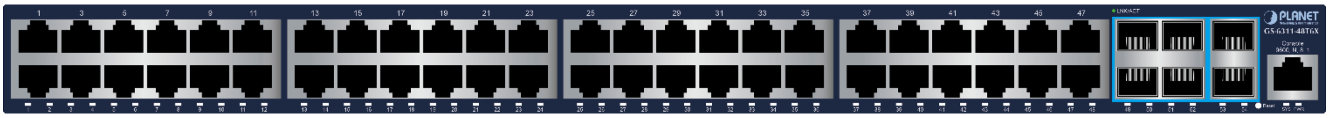
GS-6311-24T4X Front Panel



GS-6311-48P6X Front Panel



GS-6311-48T6X Front Panel



- **Gigabit TP interface**

  10/100/1000BASE-T copper, RJ45 twisted-pair: Up to 100 meters.

- **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.

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.

GS-6311-24T4X

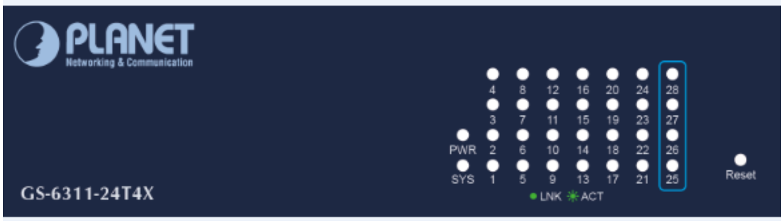


Figure GS-6311-24T4X front panel

- **System**

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

- **Interfaces**

LED	Color	Function	
LNK/ACT	Green	Lights	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

GS-6311-24HP4X

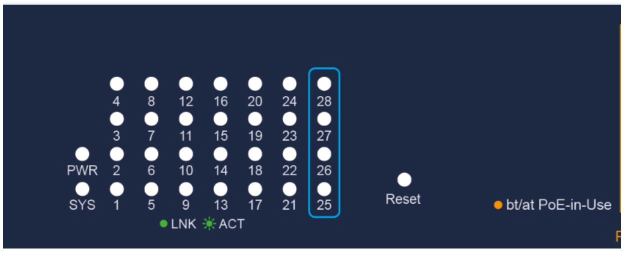


Figure GS-6311-24HP4X front panel

- **System**

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

- **Interfaces**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	**Amber**	**Lights**	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

GS-6311-16S8C4XR

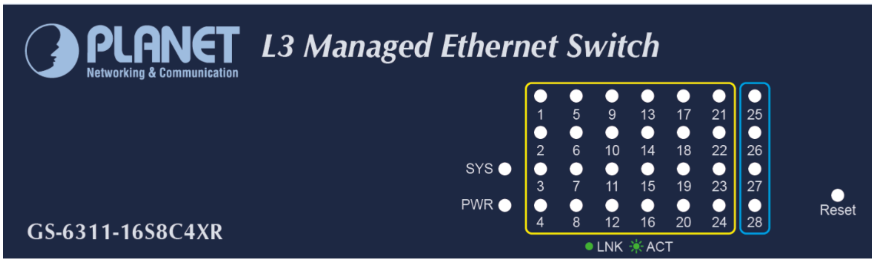


Figure GS-6311-16S8C4XR front panel

- **System**

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

- **Interfaces**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

GS-6311-48T6X

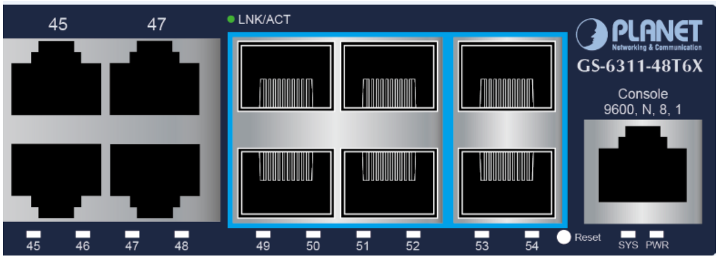


Figure GS-6311-48T6X front panel

■ **System**

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

■ **Interfaces**

LED	Color	Function	
LNK/ACT	Green	**Lights**	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

GS-6311-48P6X

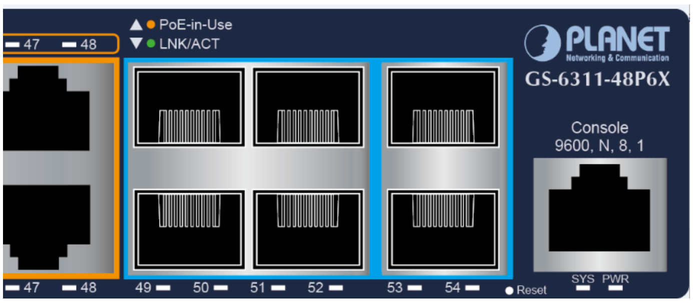


Figure GS-6311-48P6X front panel

■ **System**

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

■ **Interfaces**

LD	Color	Function	
LNK/ACT	Green	**Lights**	Indicating the port is running and the connection is successfully established.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
PoE-in-Use	Amber	**Lights**	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

MGS-6311-8P2X

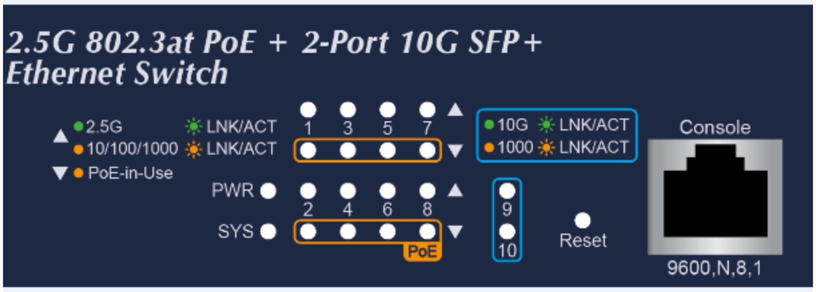


Figure MGS-6311-8P2X front panel

- **System**

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

- **Per 10/100/1000/2500BASE-T RJ45 (Port-1 to Port-8)**

LED	Color	Function	
2.5G LNK/ACT	Green	**Lights**:	To indicate the port is running in **2500Mbps** speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100/1000 LNK/ACT	Amber	**Lights**:	To indicate the port is running in **10/100/1000Mbp**s speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
PoE In-Use	Amber	**Lights**	PD is connected and PoE power supply is normal.
		Off	PD is not connected or PoE power supply is not provided.

- **Per 1G/10G BASE-SR/LR SFP+ Port (Port-9 to Port-10)**

LED	Color	Function	
10G LNK/ACT	Green	**Lights**	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	Amber	**Lights**	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

MGS-6311-10T2X

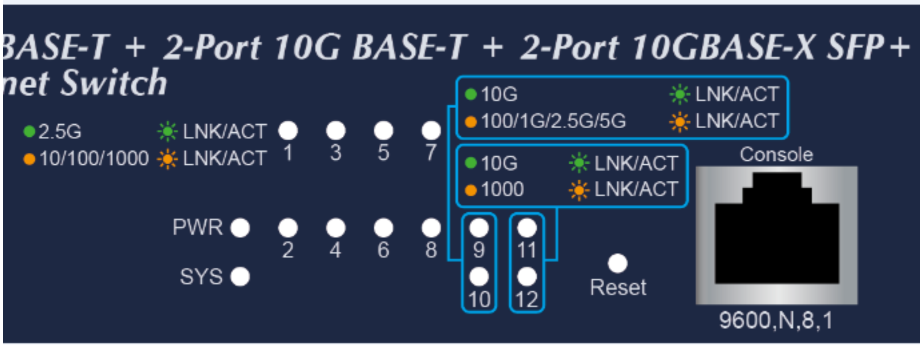


Figure MGS-6311-10T2X front panel

- **System**

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

- **Per 10/100/1000/2500BASE-T RJ45 (Port-1 to Port-8)**

LED	Color	Function	
2.5G LNK/ACT	**Green**	**Lights**:	To indicate the port is running in **2500Mbps** speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100/1000 LNK/ACT	**Amber**	**Lights**:	To indicate the port is running in **10/100/1000Mbp**s speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

- **Per 100/1G/2.5G/5G/10GBASE-T RJ45 (Port-9 to Port-10)**

LED	Color	Function	
10G LNK/ACT	**Green**	**Lights**:	To indicate the port is running in **10Gbps** speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
100/1G/2.5G/5G LNK/ACT	**Amber**	**Lights**:	To indicate the port is running in **100/1G/2.5G/5Gbps** speed and successfully established.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

- **Per 1G/10G BASE-SR/LR SFP+ Port (Port-11 to Port-12)**

LED	Color	Function	
10G LNK/ACT	**Green**	**Lights**	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	**Amber**	**Lights**	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

XGS-6311-12X

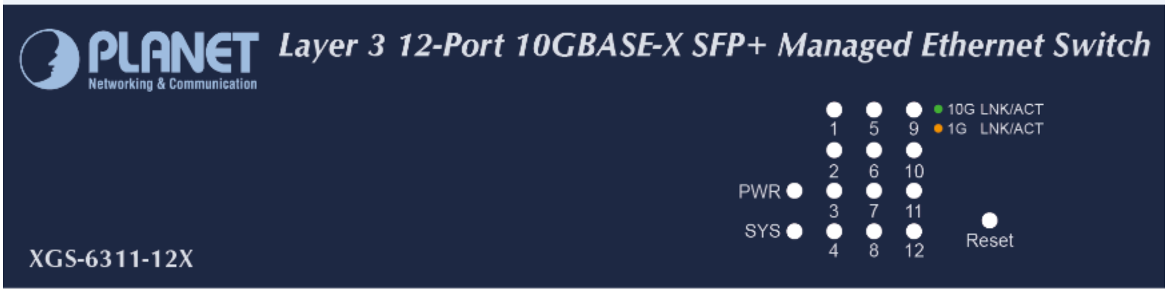

PLANET
Networking & Communication
Layer 3 12-Port 10GBASE-X SFP+ Managed Ethernet Switch
10G LNK/ACT
1G LNK/ACT
1
5
9
2
6
10
PWR
3
7
11
SYS
4
8
12
Reset
XGS-6311-12X

Figure XGS-6311-12X front panel

- **System**

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

- **Per 1G/10G BASE-SR/LR SFP+ Port (Port-1 to Port-12)**

LED	Color	Function	
10G LNK/ACT	**Green**	**Lights**	To indicate the port is running at 10Gbps and successfully established
		Blinks	Indicating that the switch is actively sending or receiving data over that port.
1G LNK/ACT	**Amber**	**Lights**	To indicate the port is running at 1Gbps.
		Blinks	Indicating that the switch is actively sending or receiving data over that port.

2.2 Switch Installation

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

2.2.1 Desktop Installation

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

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

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

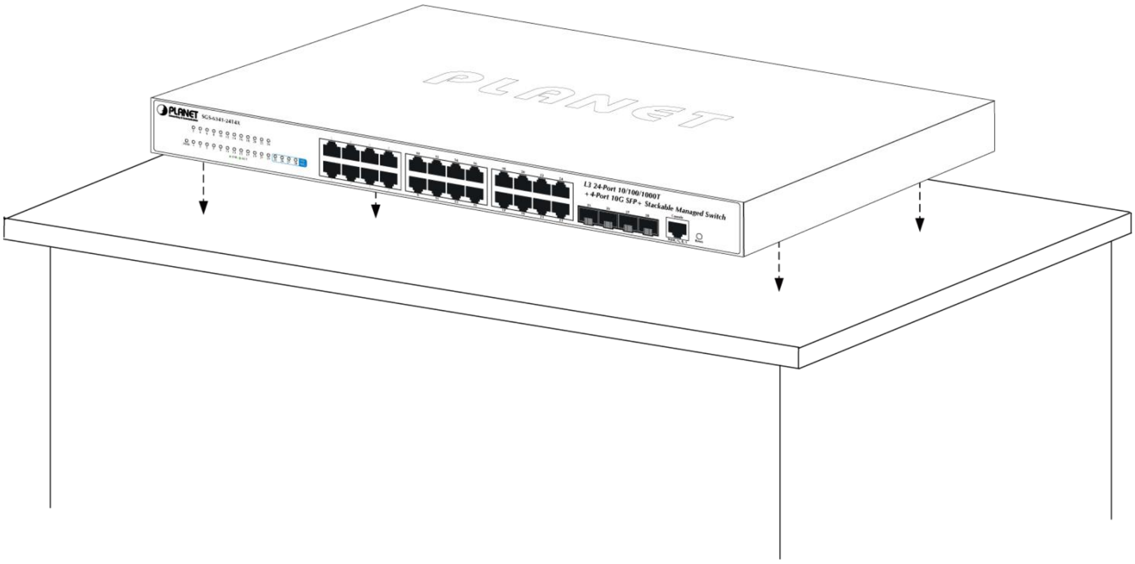


Figure 2-2-1 Place the Managed Switch on the desktop

Step 3: Keep enough ventilation space between the Managed Switch and the surrounding objects.

Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4 under **Specifications**.

Step 4: Connect the Managed Switch to network devices.

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

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

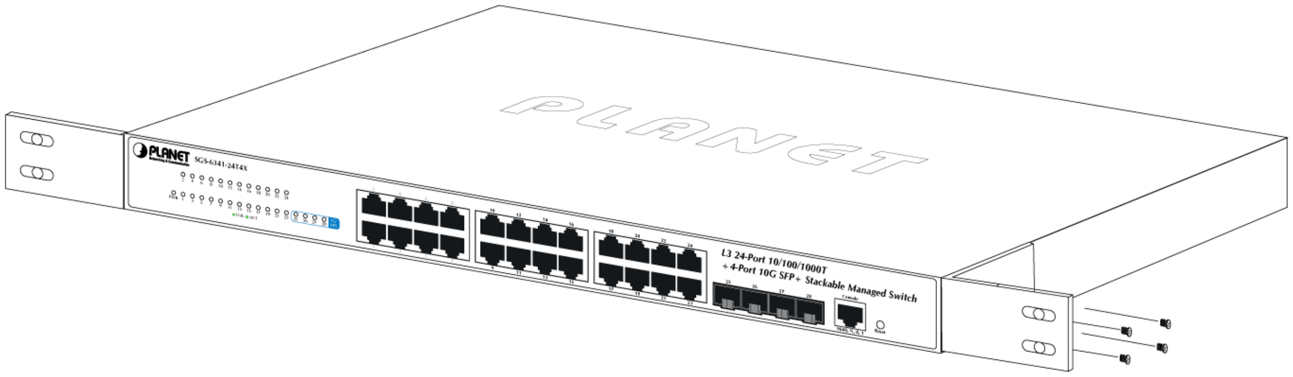


Figure 2-2-2 Attach brackets to the Managed Switch.

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

Step 3: Secure the brackets tightly.

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

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

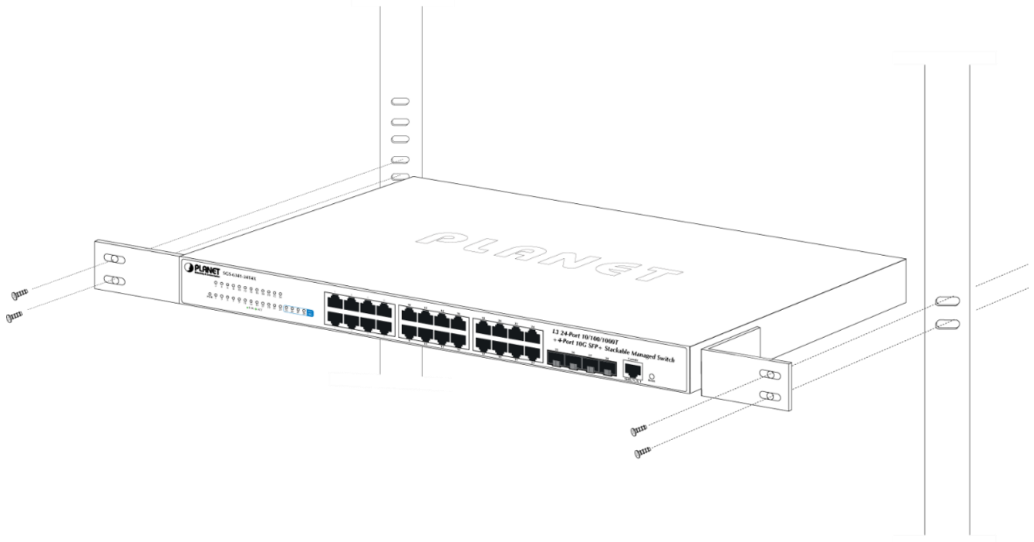


Figure 2-2-3 Mounting X(M)GS-6311 Series in a Rack

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.

2.2.3 Installing the SFP/SFP+ Transceiver

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

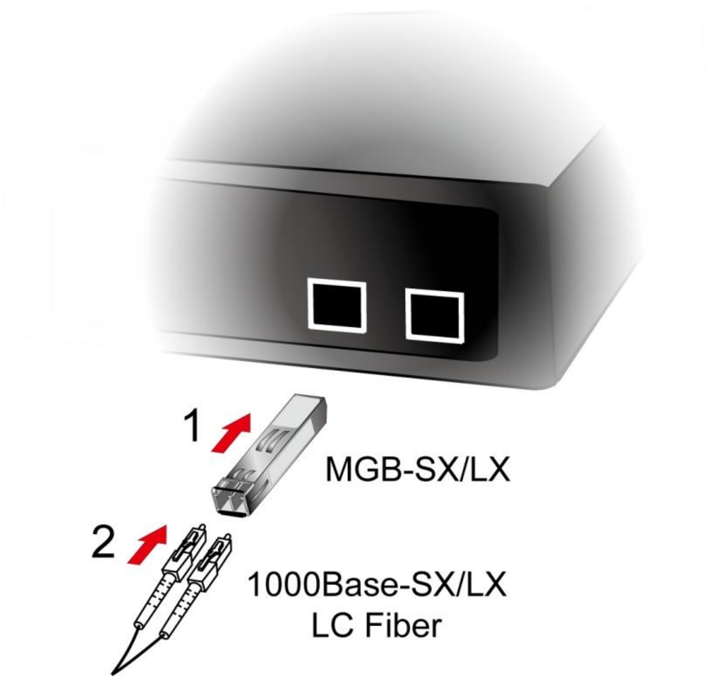


Figure 2-16 Plug in the SFP transceiver

- **Approved PLANET SFP/SFP+ Transceivers**

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

10Gigabit Ethernet Transceiver

MTB-LB40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1330nm RX:1270nm) (-40~85°C)
MTB-LA40	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 40km (TX:1270nm RX:1330nm) (-40~85°C)
MTB-LB20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1330nm RX:1270nm) (-40~85°C)
MTB-LA20	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 20km (TX:1270nm RX:1330nm) (-40~85°C)
MTB-SR	1-Port 10GBASE-SR SFP+ Fiber Optic Module - 300m (-40~85°C)
MTB-LR	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 10km (-40~85°C)
MTB-LA60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1270nm RX:1330nm) (-40~85°C)
MTB-LB60	1-Port 10GBASE-BX SFP+ Fiber Optic Module - 60km (TX:1330nm RX:1270nm) (-40~85°C)
MTB-LR40	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 40km (-40~85°C)
MTB-SR2	1-Port 10GBASE-SR SFP+ Fiber Optic Module – 2km (-40~85°C)
MTB-LR20	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 20km (-40~85°C)
MTB-LR60	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 60km (-40~85°C)
MTB-LR80	1-Port 10GBASE-LR SFP+ Fiber Optic Module - 80km (-40~85°C)

Gigabit Ethernet Transceiver (1000BASE-X SFP)

MGB-GT	SFP-Port 1000BASE-T Module (-40~85°C)

MGB-LX	SFP-Port 1000BASE-LX mini-GBIC module - 20km (-40~85°C)
MGB-SX	SFP-Port 1000BASE-SX mini-GBIC module - 550m (-40~85°C)
MGB-SX2	SFP-Port 1000BASE-SX mini-GBIC module - 2km (-40~85°C)
MGB-L40	SFP-Port 1000BASE-LX mini-GBIC module - 40km (-40~85°C)
MGB-L80	SFP-Port 1000BASE-LX mini-GBIC module - 80km (-40~85°C)
MGB-LA10	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 10km (-40~85°C)
MGB-LB10	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 10km (-40~85°C)
MGB-LA20	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 20km (-40~85°C)
MGB-LB20	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 20km (-40~85°C)
MGB-LA40	SFP-Port 1000BASE-BX (WDM, TX:1310nm) mini-GBIC module - 40km (-40~85°C)
MGB-LB40	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 40km (-40~85°C)
MGB-LA80	SFP-Port 1000BASE-BX (WDM, TX:1490nm) mini-GBIC module - 80km (-40~85°C)
MGB-LB80	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 80km (-40~85°C)
MGB-LA120	SFP-Port 1000BASE-BX (WDM, TX:1490nm) mini-GBIC module - 120km (-40~85°C)
MGB-LB120	SFP-Port 1000BASE-BX (WDM, TX:1550nm) mini-GBIC module - 20km (-40~85°C)

Note

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

1. Before we connect the X(M)GS-6311 series to the other network device, we have to make sure both sides of the SFP 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 SFP 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 SFP/SFP+ transceiver.
2. Connect the other end of the cable to a device with SFP/SFP+ transceiver installed.
3. Check the LNK/ACT LED of the SFP/SFP+ slot on the front of the Managed Switch. Ensure that the SFP/SFP+ transceiver is operating correctly.
4. Check the Link mode of the SFP/SFP+ port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to "**10G Force**", "**1000M Force**" or "**100M 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 MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

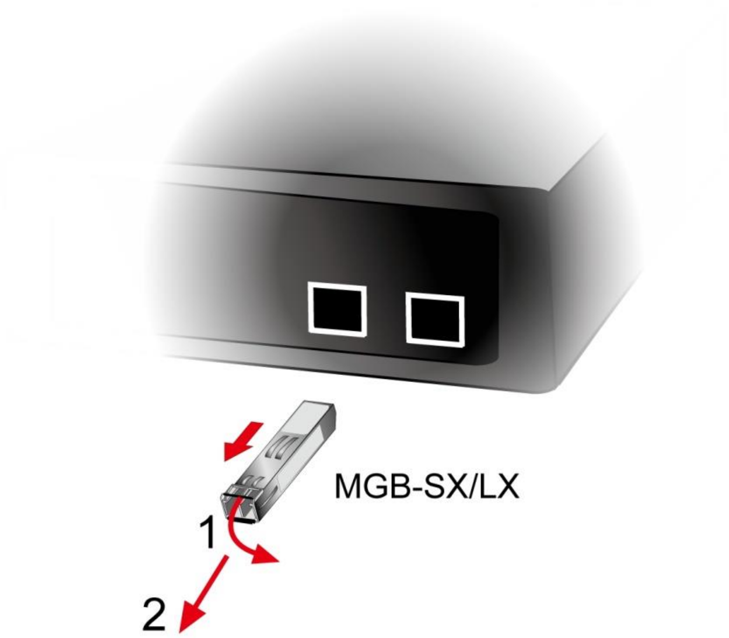


Figure 2-17: How to Pull Out the SFP/SFP+ Transceiver

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/SFP+ 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. For instance, the X(M)GS-6311 series default IP address is 192.168.0.254 or the user can try to assign a new IP address to the switch via the Console interface to be able to access the switch through Telnet.

3.3 In-band Management

In-band management refers to the management by logging in to the Managed Switch using Telnet or HTTP, 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 HTTP 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 Managed Switch is shipped with **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 HTTP.

3.4 Requirements

Workstations running Windows XP/2003/Vista/2008/7/8/10/11, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.

Workstations are installed with Ethernet NIC (Network Interface Card)

Serial Port Connection (Terminal)

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

Ethernet Port Connection

4) Network cables -- Use standard network (UTP) cables with RJ45 connectors.

5)The above PC is installed with Web browser

Note

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.

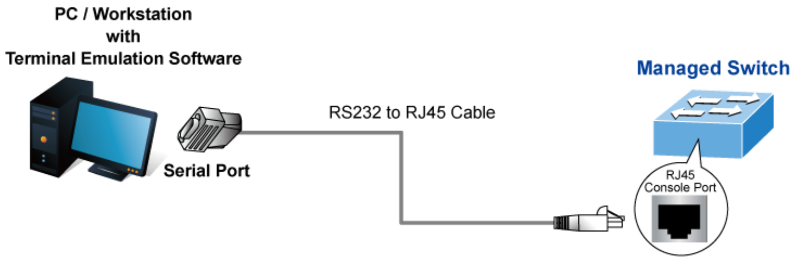
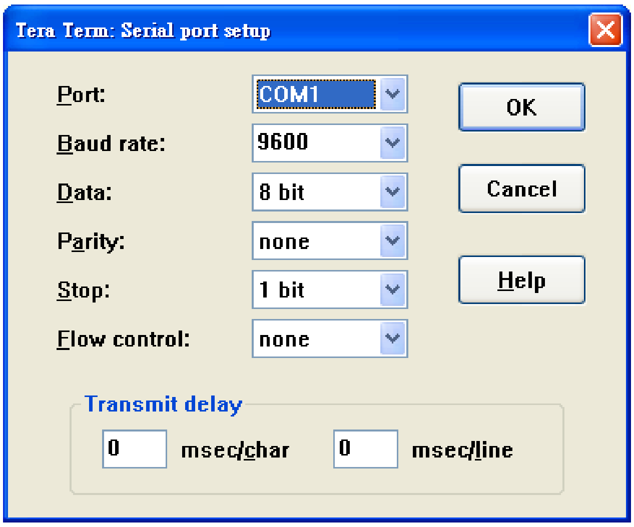


Figure 4-1 Managed Switch Console Connectivity

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.

1. Click **START** menu, then **Programs**, and then **Tera Term**.
2. When the following screen appears, make sure that the COM port should be configured as:
   - **Baud: 9600**
   - **Parity: None**
   - **Data bits: 8**
   - **Stop bits: 1**
   - **Flow control: None**



Tera Term: Serial port setup

Port: COM1

Baud rate: 9600

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay

0 msec/char 0 msec/line

Figure 4-2 Tera Term COM Port Configuration

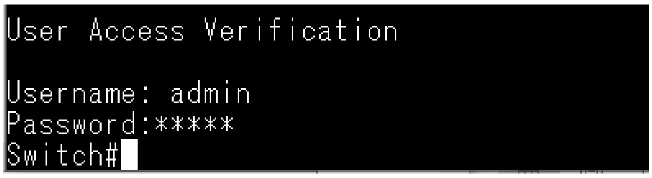
3.6 Logging on to the Console

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 in Figure 4-3 appears.

Username: **admin**

Password: **admin**



```
User Access Verification

Username: admin
Password:*****
Switch#
```

Figure 4-3 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

For security reason, please change and memorize the new password after this first setup.

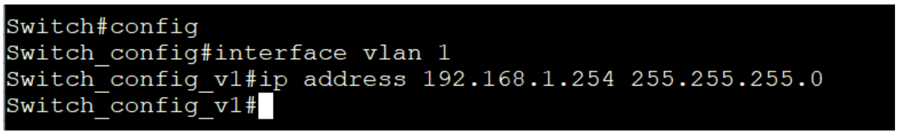
3.7 Configuring IP Address

The IP address configuration **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 vlan 1
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 vlan 1
Switch_config_v1#ip address 192.168.1.254 255.255.255.0
Switch_config_v1#
```

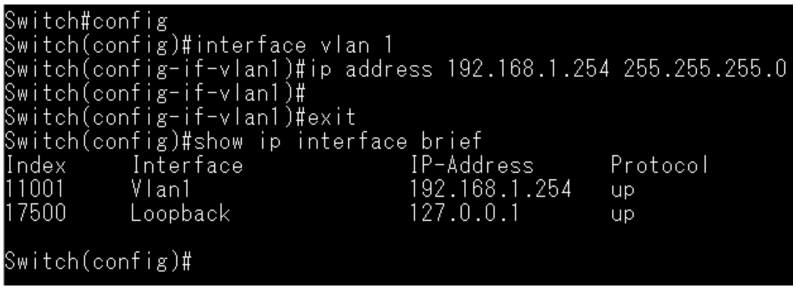
Figure 4-4 Configuring IPv4 Address Screen

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 Figure 4-5.



```
Switch#config
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip address 192.168.1.254 255.255.255.0
Switch(config-if-vlan1)#
Switch(config-if-vlan1)#exit
Switch(config)#show ip interface brief
Index     Interface             IP-Address      Protocol
11001     Vlan1                 192.168.1.254   up
17500     Loopback              127.0.0.1       up

Switch(config)#
```

Figure 4-5 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 Google Chrome, Mozilla Firefox, Google Chrome or Apple Safari.

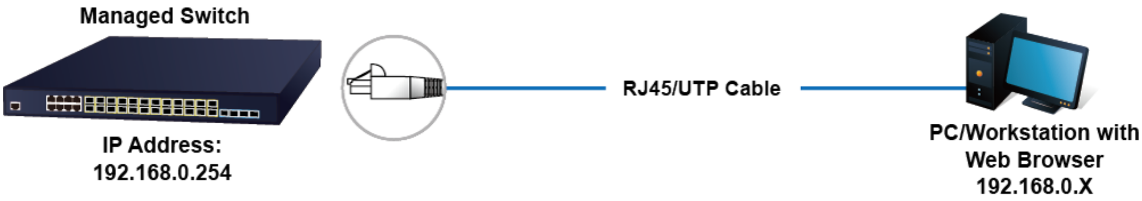


Figure IP Management Diagram

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.

For example, the IP address of the Managed Switch is configured with 192.168.0.254 on Interface VLAN 1, then the manager PC should be set to 192.168.0.x (where x is a number between 2 and 253, except 1 or 254), and the default subnet mask is 255.255.255.0.

The factory default user name and password are as follows:

Default IP of Interface VLAN 1: **192.168.0.254**
Username: **admin**
Password: **admin**

3.9 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.

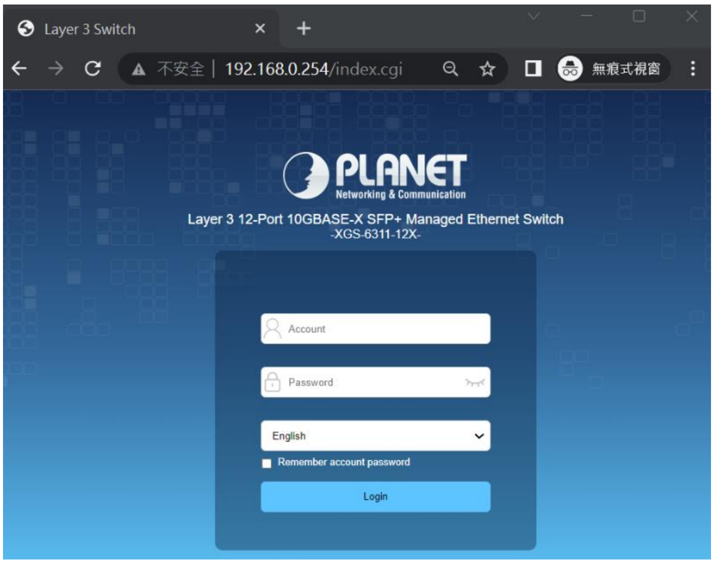
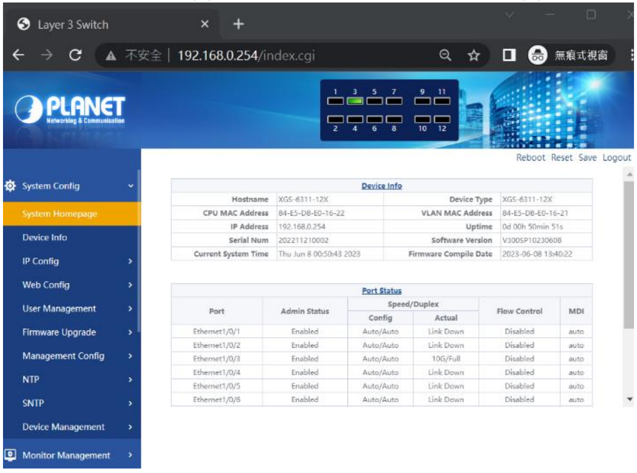

Layer 3 Switch
不安全 | 192.168.0.254/index.cgi
無痕式視窗
PLANET Networking & Communication
Layer 3 12-Port 10GBASE-X SFP+ Managed Ethernet Switch
-XGS-6311-12X-
Account
Password
English
Remember account password
Login

Figure Login Screen

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



Device Info

Hostname	XGS-6311-12X	Device Type	XGS-6311-12X
CPU MAC Address	84-E5-D8-E0-16-22	VLAN MAC Address	84-E5-D8-E0-16-21
IP Address	192.168.0.254	Uptime	0d 00h 50min 51s
Serial Num	202211210002	Software Version	V300SP10230608
Current System Time	Thu Jun 8 00:50:43 2023	Firmware Compile Date	2023-06-08 13:40:22

Port Status

Port	Admin Status	Speed/Duplex		Flow Control	MDI
		Config	Actual		
Ethernet1/0/1	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/2	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/3	Enabled	Auto/Auto	10G/Full	Disabled	auto
Ethernet1/0/4	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/5	Enabled	Auto/Auto	Link Down	Disabled	auto
Ethernet1/0/6	Enabled	Auto/Auto	Link Down	Disabled	auto

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.

Chapter 4 Basic Switch Configuration

4.1 Basic Configuration

4.1.1 authentication line

Command

authentication line {console | vty | web} login {local | radius | tacacs}
no authentication line {console | vty | web} login

Parameter

console	Log on the switch through the console serial port
vty	Log on the switch through the vty(SSH or Telnet)
web	Log on the switch through the web

Default

No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Mode

Global Mode

Usage Guide

This command can configure the authentication methods for Console, VTY, and Web login separately.
The authentication method can be any one or combination of Local. RADIUS and TACACS.
Preferences from left to right when the login method is combined configuration.
If the user has passed the authentication method, the authentication method of the lower preference is ignored.
As long as pass an authentication method, the user can log in.
AAA function and RADIUS server should be configured before the RADIUS authentication can be used.
If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.

They all support the following authentication methods.
Local: Use the local user account database for authentication.
Tacacs: Authentication using remote Tacas server.
Radius: Authentication using remote Radius server.

no command restores default authentication.

Example

Configure Telnet and ssh login methods to Local and RADIUS authentication methods.

Switch(config)# authentication line vty login local radius lists

4.1.2 banner

Command	**banner motd<LINE>** **no banner motd**	
Parameter	**<LINE>**	The information displayed when the authentication is successful, length limit from 1 to 100 characters
Default	Do not show the information when the authentication is successful.	
Mode	Global Mode	
Usage Guide	This command is used to configure the information displayed when the login authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.	
Example	Display "Welcome" after authentication is successful. **Switch(config)# banner motd Welcome**	

4.1.3 boot img

Command

boot img <img-file-url> {primary | backup}

Parameter

<img-file-url>	Full path to the img file
primary	First entry to the img document
backup	Second entry to the img document

Default

The factory original configuration only specifies the first booting IMG file, it is nos.img file in the FLASH, without the second booting IMG file.

Mode

admin Mode

Usage Guide

This command is used to configure the first and second img files used by the switch next boot. The first and second img files can only use .img files stored in switch.

1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts.
2. The suffix of all file names should be .img.
3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.

Example

Set flash:/nos.img as the second booting IMG file used in the next booting of the switch.

```
Switch#boot img flash:/nos.img backup
```

4.1.4 boot startup-config

Command	**boot startup-config {NULL | <file-url> }**	
Parameter	**NULL**	Use the factory primitive configuration as the next reboot boot configuration
	<file-url>	Is the full path of CFG file used in the next booting.
Default	None.	
Mode	admin Mode	
Usage Guide	This command is used configure the CFG file used in the next booting of the switch. Configure the CFG file used in the next booting can only use .cfg files stored in the switch. 1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, and the file name. No space is allowed in each part or between two parts. 2. The suffix of all file names should be .cfg. 3. The length of the full file path should not be longer than 128 characters, while the file name can not be longer than 80 characters.	
Example	Set flash:/ startup.cfg as the CFG file used in the next booting of the switch. **Switch# boot startup-config flash:/ startup.cfg**	

4.1.5 clock set

Command

clock set <HH:MM:SS> <YYYY.MM.DD>

Parameter

<HH:MM:SS>	Time, HH effective range 0 to 23, MM and SS 0 to 59
<YYYY.MM.DD>	Year, month and date, and YYYY valid range is 1970 to 2038, MON is month 1 to 12, DD is date 1 to 31

Default

By default，upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.

Mode

admin Mode

Usage Guide

This command is used to configure switch system time and date.

The switch cannot continue timing with power off, hence the current date and time must be first set at environments where exact time is required.

Example

To set the switch current date and time to 2002.8.1 23: 0: 0.

```
Switch#clock set 23:0:0 2002.8.1
```

4.1.6 config

Command

config [terminal]

Parameter

[terminal]	indicates terminal configuration

Default

None.

Mode

admin Mode.

Usage Guide

This command is used to switch from admin management mode to config global configuration mode.

Example

Enter config global configuration mode from admin management mode.

```
Switch#config
```

4.1.7 disable

Command	**disable**	
Parameter	**none**	none
Default	None.	
Mode	admin Mode.	
Usage Guide	This command is used for switch exit admin mode back to general user mode.	
Example	Exit admin mode back to general user mode. **Switch#disable** **Switch>**	

4.1.8 enable

Command	**enable [<1-15>]**	
Parameter	**[<1-15>]**	User Permission Level
Default	None.	
Mode	User mode/ admin mode	
Usage Guide	Use enable command to enter Admin Mode from User Mode, or change the privilege level of the users. To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong,it remains in the User Mode. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level,or else it will not authenticate the password. Set the Admin user password under Global Mode with "enable password" command.	
Example	Enter management mode from user mode.	

```
Switch>enable
Switch#
```

4.1.9 enable password

Command

enable password [level <1-15>] [0 | 7] <password>

no enable password [level <1-15>]

Parameter

[level <1-15>]	used to specify the privilege level, the default level is 15
[0 | 7]	If enter option 0 on password settings,the password is not encrypted; If enter option 7 on password settings,the password is encrypted
<password>	the password for the user

Default

This password is empty by system default.

Mode

Global Mode

Usage Guide

Configure the password used for enter Admin Mode from the User Mode.

Configure this password to prevent unauthorized entering Admin Mode.

It is recommended to set the password at the initial switch configuration.

Also, it is recommended to exit Admin Mode with “exit” command when the administrator needs to leave the terminal for a long time.

The “no enable password” command deletes this password.

Example

Configure the command for general users to enter the admin mode by rule as test.

```
Switch(config)#enable password 0 test
```

4.1.10 end

Command	**end**	
Parameter	**none**	none
Default	None.	
Mode	Except user mode / admin mode	
Usage Guide	This command is used to configure the command for general users to enter the admin mode by rule as test.	
Example	Quit VLAN mode and return to Admin mode. **Switch(config-vlan1)#end** **Switch#**	

4.1.11 exec-timeout

Command	**exec-timeout <minutes> [<seconds>]** **no exec-timeout**	
Parameter	**<minutes>**	the time value shown in minute and ranges between 0~35791
	[<seconds>]	the time value shown in seconds and ranges between 0~59
Default	Default timeout is 10 minutes.	
Mode	Global mode	
Usage Guide	This command is used Configure the timeout of exiting admin mode. Timeout exit admin management mode, need to enter management code and password to enter admin management mode again. When the timeout is set to 0, the timeout timer is disabled. "no exec-timeout"command to restore default values.	

Example

Set the admin mode timeout value to 5 minutes, 30 seconds.

Switch(config)#exec-timeout 5 30

4.1.12 exit

Command

exit

Parameter

none	none

Default

None.

Mode

All Modes

Usage Guide

This command is used quit current mode and return to it’s previous mode.

Example

Quit global mode to it’s previous mode

Switch(config)#exit
Switch#

4.1.13 help

Command

help

Parameter

none	none

Default

None.

Mode

All Modes

Usage Guide

An instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help.The user can type in ‘?’ any time to get online help.

Example

Get help in global mode.

```
Switch(config)#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
```

4.1.14 hostname

Command

hostname <hostname>

no hostname

Parameter

<hostname>	the string for the prompt, up to 64 characters are allowed

Default

The default prompt is relative with the switch.

Mode

Global Mode

Usage Guide

Use this command，set the prompt in the switch command line interface.

The no operation cancels the configuration.

Example	Set the prompt to "Test". **Switch(config)#hostname Test** **Test(config)#**

4.1.15 ip host

Command	**ip host <hostname> <ip_addr>** **no ip host {<hostname>|all}**

Parameter	**<hostname>**	the string for the prompt, up to 64 characters are allowed
	<ip_addr>	the corresponding IP address for the host name, takes a dot decimal format
	all	all of the host name

Default	None.
Mode	Global Mode
Usage Guide	By using this command, you can set the mapping relationship between the host and the IP address. Set the association between host and IP address, which can be used in commands like "ping <host>". The "no ip host" parameter of this command will delete the mapping.
Example	Set IP address of a host with the hostname of "beijing" to 200.121.1.1. **Switch(config)#ip host beijing 200.121.1.1**

4.1.16 ipv6 host

Command

ipv6 host <hostname> <ipv6_addr>
no ipv6 host { <hostname> | all}

Parameter

<hostname>	the string for the prompt, up to 64 characters are allowed
<ipv6_addr>	the corresponding IPv6 address for the host name, takes a dot decimal format
all	all of the host name

Default

None.

Mode

Global Mode

Usage Guide

By using this command, you can set the mapping relationship between the host and the IPv6 address.
Set the association between host and IPv6 address, which can be used in commands like "traceroute6 <host>".

The "no ip host" parameter of this command will delete the mapping.

Example

Set the IPv6 address of the host named beijing to 2001:1:2:3::1.

```
Switch(config)#ipv6 host beijing 2001:1:2:3::1
```

4.1.17 ip http server

Command

ip http server
no ip http server

Parameter

none	none

Default

Enable.

Mode

Global Mode

Usage Guide

Use this command to enable Web configuration.

	The "no ip http server" command disables Web configuration.
Example	Enable Web Server function and enable Web configurations. **Switch(config)#ip http server**

4.1.18 login

Command	**login** **no login**	
Parameter	**none**	none
Default	No login by default.	
Mode	Global Mode	
Usage Guide	By using this command, users have to enter the password set by password command to enter normal user mode with console. No login cancels this restriction.	
Example	Enable password. **Switch(config)#login**	

4.1.19 password

Command	**password [0 | 7] <password>** **no password**
Parameter	**[0 | 7]** if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted **<password>** password for the user
Default	This password is empty by system default.
Mode	Global Mode
Usage Guide	With this command,configure the password used for enter normal user mode on the console. The "no password" command deletes this password.
Example	Configure the password used to enter normal user mode as test, password is not encrypted. **Switch(config)#password 0 test**

4.1.20 privilege

Command

privilege mode level <1-15> LINE
no privilege mode level <1-15> LINE

Parameter

mode	register mode of the command, 'Tab' or '?' is able to show all register modes
<1-15>	level, its range between 1 and 15
LINE	the command needs to be configured, it supports the command abbreviation

Default

None.

Mode

Global Mode

Usage Guide

Use this command to configure the permission level for the specified command.
This function cannot change the command itself.
LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully.
Can choose to set the level of the NO command, but it does not affect the result.
When using a no command, the LINE must be a configured command line.
If the command line with the parameter, the parameter must be matched with the configured command.

The no command restores the original level of the command.

Example

Change the level of show ip route command to level 5.
Restore the original level of the show ip route command.

```
Switch(config)#privilege exec level 5 show ip route
Switch(config)#no privilege exec level 5 show ip route
```

4.1.21 reload

Command	**reload**
Parameter	**none** none
Default	None.
Mode	Admin Mode
Usage Guide	The user can use this command to restart the switch continuously.
Example	Hot restart switch. **Switch(config)#reload**

4.1.22 service password-encryption

Command	**service password-encryption** **no service password-encryption**
Parameter	**none** none
Default	No service password-encryption by system default.
Mode	Global Mode
Usage Guide	The current unencrypted passwords as well as the coming passwords configured by password, enable password, ip ftp and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.
Example	Encrypt system passwords. **Switch(config)#service password-encryption**

4.1.23 service terminal-length

Command	**service terminal-length <0-512>** **no service terminal-length**
Parameter	**<0-512>** Columns of characters displayed on each screen of vty, ranging between 0-512
Default	None.
Mode	Global Mode
Usage Guide	Use this command，configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telent.ssh client and the Console will be following this configuration. The “no service terminal-length” command cancels the screen shifting operation.
Example	Set the number of vty threads to 20. **Switch(config)#service terminal-length 20**

4.1.24 sysContact

Command	**sysContact <LINE>** **no sysContact**
Parameter	**<LINE>** the prompt character string, range from 0 to 255 characters
Default	The default is factory setting.
Mode	Global Mode
Usage Guide	With this command,the user can set the factory contact mode bases the fact instance. The “no sysContact” command reset the switch to factory settings.
Example	Set the factory contact mode to test.

Switch(config)#sysContact test

4.1.25 sysLocation

Command	**sysLocation<LINE>** **no sysLocation**
Parameter	**<LINE>** the prompt character string, range from 0 to 255 characters
Default	The default is factory setting.
Mode	Global Mode
Usage Guide	With this command,the user can set the factory address bases the fact instance. The "no sysLocation" command reset the switch to factory settings.
Example	Set the factory address to test. **Switch(config)#sysLocation test**

4.1.26 set default

Command	**set default**
Parameter	**none** none
Default	None.
Mode	Admin Mode
Usage Guide	Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time. **Note**: After the command, "write" command must be executed to save the operation. The switch will reset to factory settings after restart.
Example	Restore factory settings and restart. **Switch#set default** Are you sure? [Y/N] = y **Switch#write** **Switch#reload**

4.1.27 set boot password

Command

set boot password
no set boot password

Parameter

none	none

Default

None.

Mode

Global Mode

Usage Guide

Under the img mode, configure the password of entering the bootrom mode next time; under the global mode, input this command and the password according to the prompt and confirm it, then successfully to configure.
Notice: the characters length of the password is from 3 to 32.

The no command cancels the password.

Example

Sets the password when entering boot mode.

```
Switch(config)#set boot password
New password :*****
Confirm password :*****
Set password success!
```

4.1.28 setup

Command

setup

Parameter

none	none

Default

None.

Mode

Admin Mode

Usage Guide

Switch provides a Setup Mode, in which the user can configure IP addresses, etc.

Example

Enter setup mode.

```
Switch#setup
```

4.1.29 show clock

Command

show clock

Parameter

none	none

Default

None.

Mode

Admin Mode.

Usage Guide

Displays the current system clock.

Example

Displays the current system clock.

```
Switch#show clock
Current time is TUE AUG 22 11：00：01 2002
```

4.1.30 show cpu usage

Command

show cpu usage [<slotno>]

Parameter

[<slotno>]	Specify slots

Default

None.

Mode

Admin and configuration mode

Usage Guide

Display current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage by this command.

Only the chassis switch uses slotno parameter which is used to show the CPU usage rate of the card on specified slot, if there is no parameter, the default is current card.

Example

Show the current usage rate of CPU.

```
Switch#show cpu usage
Last 5 second CPU IDLE: 87%
Last 30 second CPU IDLE: 89%
Last 5 minute CPU IDLE: 89%
From running CPU IDLE: 89%
```

4.1.31 show cpu utilization

Command

show cpu utilization

Parameter

none	none

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.。

Example

Displays CPU utilization.

```
Switch#show cpu utilization
Last 5 second CPU USAGE: 9%
Last 30 second CPU USAGE: 11%
Last 5 minute CPU USAGE: 11%
From running CPU USAGE: 11%
```

4.1.32 show memory usage

Command

show memory usage [<slotno>]

Parameter

[<slotno>]	Specify slots

Default

None.

Mode

Admin Mode

Usage Guide

Show memory usage rate.

Only the chassis switch uses slotno parameter which is used to show the memory usage rate of card on the specified slot, if there is no parameter, the default is current card.

Example

Show the current usage rate of the memory.

```
Switch#show memory usage
The memory total 128 MB, free 58914872 bytes, usage is 56.10%
```

4.1.33 show privilege

Command	**show privilege**	
Parameter	**none**	none
Default	None.	
Mode	Global Mode	
Usage Guide	Show privilege of the current user.	
Example	Show privilege of the current user. **Switch(config)#show privilege** Current privilege level is 15	

4.1.34 show privilege mode LINE

Command	**show privilege mode LINE**	
Parameter	**mode**	register mode of the command, 'Tab' or '?' is able to show all register modes
	LINE	the command needs to be configured, it supports the command abbreviation
Default	None.	
Mode	Admin mode/Global mode	
Usage Guide	Show the level of the specified command. LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.	

Example

Show the level of privilege command.

```
Switch(config)#show privilege exec show ip route
The command : show ip route
Privilege is : 15
```

4.1.35 show tech-support

Command

show tech-support [no-more]

Parameter

[no-more]	Display the operational information and the task status of the switch directly, do not connect the user by "more".

Default

None.

Mode

Admin mode/Global mode

Usage Guide

This command is used to collect the relative information when the switch operation is malfunctioned.

Display the operational information and the task status of the switch.

The technique specialist use this command to diagnose whether the switch operate normally.

Example

Displays the operational information and the task status of the switch.

```
Switch#show tech-support
```

4.1.36 show version

Command

show version

Parameter

none	none

Default

None.

Mode

Admin mode/Global mode

Usage Guide

This command is used to show the version of the switch, it includes the hardware version and the software version information.

Example

Display the version information of the switch.

```
Switch#show version
```

4.1.37 username

Command

username <username> [privilege <privilege>] [password [0 | 7]<password>]
no username <username>

Parameter

<username>	the username, its range should not exceed 32 characters
<privilege>	the maximum privilege level of the commands that the user is able to execute, its value is limited between 1 and 15, and 1 by default
[0 | 7]	If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted (Use 32 bits password encrypted by MD5)
<password>	password for the user

Default

None.

Mode

Global Mode

Usage Guide

Configure local login username and password along with its privilege level.
16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.
The user can log in user and priority after the command configures, before issuing
the command authentication line console login local, it should be made sure that at one user

has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode.
If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.

The no command delete user.

Example

Configure an administrator account named admin, with the preference level as 15. And configure two normal accounts with its preference level as 1. Then enable local authentication method.

```
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)# username user1 privilege 1 password 7
4a7d1ed414474e4033ac29ccb8653d9b
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local
```

4.1.38 web-auth privilege <1-15>

Command

web-auth privilege <1-15>
no web-auth privilege

Parameter

<1-15>	Appoint the level of logging in the switch by web and the range is from 1 to 15

Default

The default level is 15.

Mode

Global Mode

Usage Guide

Configure the level of logging in the switch by web.
After configured the level of logging in the switch by web, only the user with the level that is equal to or higher than it can login in the switch by web.

Example

Configure the level of logging in the switch by web as 10.

```
Switch(config)# web-auth privilege 10
```

4.1.39 write

Command	**write**
Parameter	**none** none
Default	None.
Mode	Admin Mode
Usage Guide	Save the currently configured parameters to the Flash memory. After a set of configuration with desired functions, the setting should be saved to the specified configuration file, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the copy running-config startup-config command.
Example	Save the current configuration. **Switch#write**

4.1.40 write running-config

Command	**write running-config [<startup-config-file-name>]**
Parameter	**[<startup-config-file-name>]** the full path of the cfg file
Default	None.
Mode	Admin Mode
Usage Guide	Save the current running config as .cfg file to Flash Memory. The file path comprises of two parts: device prefix used as the root directory (flash:/)and the file name. No space is allowed in each part or between two parts. The suffix of all file names should be .cfg. The length of the full file path should not be longer than 128 characters, while the file name cannot be longer than 80 characters.
Example	Save the current running config as .cfg file with name of 123. **Switch#write running-config 123.cfg**

4.2 Telnet

4.2.1 aaa authorization config-commands

Command

```
aaa authorization config-commands
no aaa authorization config-commands
```

Parameter

none	none

Default

By default,disable.

Mode

Global Mode

Usage Guide

Enable command authorization function for the login user with VTY (login with
Telnet and SSH).

Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command.

The no command disables this function.

Example

Enable VTY command authorization function.

```
Switch(config)#aaa authorization config-commands
```

4.2.2 accounting exec

Command

```
accounting line {console | vty} exec {start-stop | stop-only | none} method1 [method2…]
no accounting line {console | vty} exec
```

Parameter

console	log in through serial port
vty	log in through telnet or ssh
start-stop	sends the accounting start or the accounting stop when the user is logging or exit the login
stop-only	sends the accounting stop when the user exits the login only
none	does not send the accounting start or the accounting stop
method	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count

Default

By default there is no accounting.

Mode

Global Mode

Usage Guide

Configure the list of the accounting method for the login user with VTY (login
with Telnet and SSH) and Console.
console and vty login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently.

The no command restores the default accounting method.

Example

Configure the login accounting with the telnet method.

Switch(config)#accounting line vty exec start-stop tacacs

4.2.3 accounting command

Command

accounting line {console | vty} command <1-15> {start-stop | stop-only |none} method1 [method2…]
no accounting line {console | vty} command <1-15>

Parameter

console	log in through serial port
vty	log in through telnet or ssh
command <1-15>	the level of the accounting command
start-stop	sends the accounting start or the accounting stop when the user is logging or exit the login
stop-only	sends the accounting stop when the user exits the login only
none	does not send the accounting start or the accounting stop
method	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count

Default

By default there is no accounting method.

Mode

Global Mode

Usage Guide

Configure the list of the command accounting method with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.
console and vty login method are able to set the corresponding command accounting method respectively, the accounting method only supports TACACS+ method currently.

Only the stop information of the accounting is recorded, whether command accounting configures start-stop method or stop-only method.

The no command restores the default accounting method.

Example

Configure command audit methods through telnet login, command level 15.

Switch(config)#authorization line vty command 15 start-stop tacacs

4.2.4 authentication enable

Command

authentication enable method1 [method2…]
no authentication enable

Parameter

method the list of the authentication method, it must be among local, tacacs and radius keywords；

local:uses the local database to authenticate；

tacacs:uses the remote TACACS+ authentication server to authenticate；

radius:uses the remote RADIUS authentication server to authenticate

Default

The local authentication is enable command by default.

Mode

Global Mode

Usage Guide

Configure the list of the enable authentication method.

The enable authentication method can be any one or combination of Local,RADIUS and TACACS.

When login method is configuration in combination, the preference goes from left to right.

If the users have passed the authentication method, authentication method of lower preferences will be ignored.

To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method)；it will attempt the next authentication method if it receives nothing.

And AAA function RADIUS server should be configured before the RADIUS configuration

	method can be used. And TACACS server should be configured before the TACACS configuration method can be used. The no command restores the default authentication method.
Example	Configure the enable authentication method to be tacacs and local. **Switch(config)#authentication enable tacacs local**

4.2.5 authentication ip access-class

Command	**authentication ip access-class {<num-std>|<name>}** **no authentication ip access-class**	
Parameter	**<num-std>**	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string length is ranging between 1 and 32
Default	The binding ACL to Telnet/SSH/Web function is closed by default.	
Mode	Global Mode	
Usage Guide	Binding standard IP ACL protocol to login with Telnet/SSH/Web. The no form command will cancel the binding ACL.	
Example	Binding standard IP ACL protocol to access-class 1. **Switch(config)#authentication ip access-class 1 in**	

4.2.6 authentication ipv6 access-class

Command	**authentication ipv6 access-class {<num-std>|<name>}** **no authentication ipv6 access-class**	
Parameter	**<num-std>**	the access-class number for standard numeric ACL, ranging between 500-599

<name>	the access-class name for standard ACL, the character string length is ranging between 1 and 32

Default

The binding ACL to Telnet/SSH/Web function is closed by default.

Mode

Global Mode

Usage Guide

Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web.

The no form command will cancel the binding ACL.

Example

Binding standard IP ACL protocol to access-class 500.

Switch(config)#authentication ipv6 access-class 500 in

4.2.7 authentication line login

Command

authentication line {console | vty | web} login method1 [method2…]
no authentication line {console | vty | web} login

Parameter

console	log in through serial port
vty	log in through telnet or ssh
web	log in through web
method	the list of the authentication method, it must be among local, tacacs and radius keywords； local:uses the local database to authenticate； tacacs:uses the remote TACACS+ authentication server to authenticate； radius:uses the remote RADIUS authentication server to authenticate

Default

No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.

Mode

Global Mode

Usage Guide

Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user.

Authentication method can be any one or combination of Local, RADIUS and TACACS.

When login method is configuration in combination, the preference goes from left to right.

If the users have passed the authentication method, authentication method of lower preferences will be ignored.

if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method)；

it will attempt the next authentication method if itreceives nothing.

And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The authentication line console login command is exclusive with the "login"command. The authentication line console login command configures the switch to use the Console login method. And the login command makes the Console login to use the passwords configured by the password command for authentication.

If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

The no form command restores the default authentication method.

Example

Configure the telnet and ssh login with the remote RADIUS authentication.

```
Switch(config)#authentication line vty login radius
```

4.2.8 authentication securityip

Command	**authentication securityip <ip-addr>** **no authentication securityip <ip-addr>**	
Parameter	**<ip-addr>**	the trusted IP address of the client in dotted decimal format which can login the switch
Default	No trusted IP address is configured by default.	
Mode	Global Mode	
Usage Guide	To configure the trusted IP address for Telnet and HTTP login method. IP address of the client which can login the switch is not restricted before the trusted IP address is not configured. After the trusted IP address is configured,only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch. The no form of this command will remove the trusted IP address configuration.	
Example	To configure 192.168.1.21 as the trusted IP address. **Switch(config)#authentication securityip 192.168.1.21**	

4.2.9 authentication securityipv6

Command	**authentication securityipv6 <ipv6-addr>** **no authentication securityipv6 <ipv6-addr>**
Parameter	**<ip-addr>** the security IPv6 address which can login the switch
Default	No security IPv6 addresses are configured by default.
Mode	Global Mode
Usage Guide	To configure the security IPv6 address for Telnet and HTTP login method. IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured. After the security IPv6 address is configured,only clients with security IPv6 addresses are able to login the switch. Up to 32 security IPv6 addresses can be configured in the switch. The no form of this command will remove the specified configuration.
Example	Configure the security IPv6 address is 2001:da8:123:1::1. **Switch(config)#authentication securityipv6 2001:da8:123:1::1**

4.2.10 authorization

Command

authorization line {console | vty | web} exec method [method…]

no authorization line {console | vty | web} exec

Parameter

console	log in through serial port
vty	log in through telnet or ssh
web	log in through web
method	the list of the authentication method, it must be among local, tacacs and radius keywords； local:uses the local database to authenticate； tacacs:uses the remote TACACS+ authentication server to authenticate； radius:uses the remote RADIUS authentication server to authenticate

Default

There is no authorization method by default.

Mode

Global Mode

Usage Guide

Configure the list of the authorization method for the login user with VTY (login
with Telnet and SSH), Web and Console.

And authorization method can be any one or combination of Local,RADIUS or TACACS.

When login method is configuration in combination, the preference goes from left to right.

If the users have passed the authorization method, authorization method of lower preferences will be ignored.

if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing.

And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

The local users adopt username command permission while authorization command
is not configured, the users login the switch via RADIUS/TACACS method and works
under common mode.

The no command restores the default authorization method.

Example

Configure the telnet authorization method to RADIUS.

Switch(config)#authorization line vty exec radius

4.2.11 authorization line vty command

Command

authorization line vty command <1-15> {local | radius | tacacs} (none|)

no authorization line vty command <1-15>

Parameter

command <1-15>	Level scope of authorization orders 1~15
local	Authorization is granted locally
radius	Authorization for remote radius
tacacs	Authorization for remote tacacs
none	Authorization mode is empty

Default

The authorization manner is not configured as default.

Mode

Global Mode

Usage Guide

Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH).

The enabling authorization method can be any one or combination of Local. RADIUS and TACACS.

When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order.

If the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored.

As long as one authorization manner receives a clear response of the corresponding agreement.Whether it is received or refused, the next authorization manner will not be attempted.If the clear response is not received, try the next manner.

When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured.

None is the manner of escaping and it only can be the last manner.

This manner returns to passed authorization directly and it is successful to configure the command.

The no command recovers to be default manner.

Example

Configure level 1 command authorization manner of telnet login user as TACACS.

```
Switch(config)#authorization line vty command 1 tacacs
```

4.2.12 clear line vty <0-31>

Command	**clear line vty <0-31>**
Parameter	**<0-31>** appointed line
Default	None.
Mode	Admin Mode
Usage Guide	After inputting this command, there is need to judge for this command, “Confirm[Y/N]: “, when inputting “Y“ or “y“, run to delete; when inputting “？ “, do not run to delete, print the notice information only. When inputting other characters, do not run to delete.
Example	Admin users who are forced to log in through VTY (using Telnet or SSH login) are off line. **Switch#clear line vty 0** Confirm[Y/N]:y [OK]

4.2.13 crypto key clear rsa

Command	**crypto key clear rsa**
Parameter	**none** none
Default	None.
Mode	Admin Mode
Usage Guide	This command is used to clear the secret key of the ssh and close the ssh service.
Example	Clear the secret key of the ssh and close the ssh service. **Switch#crypto key clear rsa** ssh host key is cleared successfully. ssh is closed successfully.

4.2.14 terminal length

Command	**terminal length <0-512>** **terminal no length**	
Parameter	**<0-512>**	Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display)
Default	Default Length is 25.	
Mode	Admin Mode	
Usage Guide	Set length of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen. The "terminal no length" cancels the screen switching operation and display content once in all.	
Example	Configure length of characters in each display to 20. **Switch#terminal length 20**	

4.2.15 telnet

Command	**telnet [vrf <vrf-name>] {<ip-addr> | <ipv6-addr> | host <hostname>}[<port>]**	
Parameter	**<vrf-name>**	the specific VRF name
	<ip-addr>	the IP address of the remote host, shown in dotted decimal notation
	<ipv6-addr>	the IPv6 address of the remote host
	<hostname>	the name of the remote host, containing max 64 characters
	<port>	the port number, ranging between 0 and 65535
Default	None.	
Mode	Admin Mode	
Usage Guide	This command is used when the switch is applied as Telnet client, for logging on remote host	

to configure.

When a switch is applied as a Telnet client, it can only

establish one TCP connection with the remote host.

To connect to another remote host, the current TCP connection must be disconnected with a hotkey "CTRL+ \".

To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured.

For required commands please refer to ip host and ipv6 host.

In case a host corresponds to both an IPv4 and an IPv6 addresses,the IPv6 should be preferred when telneting this host name.

Example

The switch telnets to a remote host whose IP address is 20.1.1.1.

```
Switch#telnet 20.1.1.1 23
Connecting Host 20.1.1.1 Port 23...
Service port is 23
Connected to 20.1.1.1
login:123
password:***
router>
```

4.2.16 telnet server enable

Command

telnet server enable

no telnet server enable

Parameter

none none

Default

Telnet server function is enabled by default.

Mode

Global Mode

Usage Guide

Enable the Telnet server function in the switch

This command is available in Console only.

The administrator can use this command to enable or disable the Telnet client to login to the switch.

The "no telnet server enable"command disables the Telnet function in the switch.

Example

Disable the Telnet server function in the switch.

```
Switch(config)#no telnet server enable
```

4.2.17 telnet-server max-connection

Command	**telnet-server max-connection {<max-connection-number> | default}**	
Parameter	**<max-connection-number>**	the max connection number supported by the Telnet service, ranging from 5 to 16
	default	restore the default configuration
Default	The system default value of the max connection number is 5.	
Mode	Global Mode	
Usage Guide	Configure the max connection number supported by the Telnet service of the switch.	
Example	Set the max connection number supported by the Telnet service as 10. **Switch(config)#telnet-server max-connection 10**	

4.2.18 ssh-server authentication-retries

Command	**ssh-server authentication-retries <authentication-retries>** **no ssh-server authentication-retries**	
Parameter	**<authentication-retries>**	the number of times for retrying authentication,valid range is 1 to 10
Default	The number of times for retrying SSH authentication is 3 by default.	
Mode	Global Mode	
Usage Guide	Configure the number of times for retrying SSH authentication. The "no ssh-server authentication-retries" command restores the default number of times for retrying SSH authentication.	
Example	Set the time for retrying SSH authentication to 5. **Switch(config)#ssh-server authentication-retries 5**	

4.2.19 ssh-server enable

Command	**ssh-server enable** **no ssh-server enable**
Parameter	**none** none
Default	SSH function is disabled by default.
Mode	Global Mode
Usage Guide	Enable SSH function on the switch. In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch. The "no ssh-server enable" command disables SSH function.
Example	Enable SSH function on the switch. **Switch(config)#ssh-server enable**

4.2.20 ssh-server host-key create rsa

Command	**ssh-server host-key create rsa [modulus < modulus >]**
Parameter	**< modulus >** the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024
Default	The system uses the key generated when the ssh-server is started at the first time.
Mode	Global Mode

Usage Guide

This command is used to generate a new SSH service host rsa key.

When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and “write” command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024.

No command disables SSH service.

Example

Generate new host key.

Switch(config)#ssh-server host-key create rsa

4.2.21 ssh-server max-connection

Command

ssh-server max-connection {<max-connection-number>|default}

Parameter

<max-connection-number>	the max connection number supported by the SSH service, ranging from 5 to 16.
default	restore default

Default

The system default value of the max connection number is 5.

Mode

Global Mode

Usage Guide

Configure the max connection number supported by the SSH service of the switch.

Example

Set the max connection number supported by the SSH service as 10.

Switch(config)#ssh-server max-connection 10

4.2.22 ssh-server timeout

Command	**ssh-server timeout <timeout>** **no ssh-server timeout**
Parameter	**<timeout>** timeout value; valid range is 10 to 600 seconds
Default	SSH authentication timeout is 180 seconds by default.
Mode	Global Mode
Usage Guide	Configure timeout value for SSH authentication. The "no ssh-server timeout"command restores the default timeout value for SSH authentication.
Example	Set SSH authentication timeout to 240 seconds. **Switch(config)#ssh-server timeout 240**

4.2.23 show crypto key

Command	**show crypto key**
Parameter	**none** none
Default	None.
Mode	Admin Mode
Usage Guide	Show the secret key of ssh.
Example	Show the secret key of ssh. **Switch#show crypto key**

4.2.24 show ssh-server

Command

show ssh-server

Parameter

none	none

Default

None.

Mode

Admin Mode

Usage Guide

Display SSH state and users which log on currently.

Example

Display SSH state and users which log on currently.

```
Switch#show ssh-server
ssh server is enabled
ssh-server timeout 180s
ssh-server authentication-retries 3
ssh-server max-connection number 6
ssh-server login user number 2
```

4.2.25 show telnet login

Command

show telnet login

Parameter

none	none

Default

None.

Mode

Admin Mode

Usage Guide

Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

Example

Display Telnet client information.

```
Switch#show telnet login
Authenticate login by local
Login user:
aa
```

4.2.26 show users

Command

show users

Parameter

none none

Default

None.

Mode

Admin Mode

Usage Guide

Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP.

Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.

Example

Displays user information.

Switch#show users

```
  Line        User           Location
  vty 16        a           192.168.1.1
  vty 0       admin         192.168.1.2
  vty 17       mab          192.168.1.13
  vty 1        test         192.168.1.40
```

4.2.27 who

Command

who

Parameter

none none

Default

None.

Mode

All configuration modes

Usage Guide

Show the current login users with vty.

Example

Show the current login users with vty.

Switch#who

```
Telnet user a login from 192.168.1.20
```

4.3 Configuring Switch IP

4.3.1 interface vlan

Command

interface vlan <vlan-id>
no interface vlan <vlan-id>

Parameter

<vlan-id>	the VLAN ID of an existing VLAN, ranging from 1 to 4094

Default

None.

Mode

Global Mode

Usage Guide

This command is used enter the VLAN interface configuration mode

Users should first make sure the existence of a VLAN before configuring it.

User "exit" command to quit the VLAN interface configuration mode back to the global configuration mode.

the no operation of this command will delete the existing VLAN interface.

Example

Enter the VLAN interface configuration mode of VLAN1.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#
```

4.3.2 ip address

Command

ip address <ip-address> <mask> [secondary]
no ip address [<ip-address> <mask>] [secondary]

Parameter

<ip-address>	the IP address in dot decimal format
<mask>	the subnet mask in dot decimal format
[secondary]	indicates the IP configured is a secondary IP address

Default

No IP address is configured upon switch shipment.

Mode

VLAN Interface Mode

Usage Guide

Set the IP address and mask for the specified VLAN interface.
A VLAN interface must be created first before the user can assign an IP address to the switch.

The no command deletes the specified IP address setting.

Example

Set 10.1.128.1/24 as the IP address of VLAN1 interface.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

4.3.3 ipv6 address

Command

```
ipv6 address <ipv6address | prefix-length> [eui-64]
no ipv6 address <ipv6address | prefix-length> [eui-64]
```

Parameter

<ipv6address >	the prefix of an IPV6 address
<prefix-length>	the length of the prefix of an IPV6 address, ranging from 3 to 128
[eui-64]	means that the eui64 interface id of the interface will automatically create an IPV6 address

Default

No IPv6 address is configured upon switch shipment.

Mode

VLAN Interface Mode

Usage Guide

Configure aggregatable global unicast address, site-local address and link-local address for the interface.
The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage.
Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff ::, with a length no shorter than 3.And the prefix length of a site-local address or a link-local address should not be shorter than 10.

The no command deletes the specified IPv6 address setting.

Example

Configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

4.3.4 ip bootp-client enable

Command

ip bootp-client enable
no ip bootp-client enable

Parameter

none	none

Default

BootP client function is disabled by default.

Mode

VLAN Interface Mode

Usage Guide

Enable the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation.
Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed.
To obtain IP address via BootP, a DHCP server or a BootP server is required in the network.

The no command disables the BootP Client function and releases the IP address obtained in BootP.

Example

Get IP address through BootP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip bootp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

4.3.5 ip dhcp-client enable

Command

ip dhcp-client enable

no ip dhcp-client enable

Parameter

none	none

Default

By default, the dhcp service is disabled.

Mode

VLAN Interface Mode

Usage Guide

Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation.

To obtain IP address via DHCP, a DHCP server is required in the network.

Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.

The no command disables the DHCP client function and releases the IP address obtained in DHCP.

Example

Getting an IP address through DHCP.

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip dhcp-client enable
Switch(Config-if-Vlan1)#exit
Switch(config)#
```

4.4 SNMP

4.4.1 rmon enable

Command	**rmon enable** **no rmon enable**
Parameter	**none** none
Default	RMON is enabled by default.
Mode	Global Mode
Usage Guide	This command is used to enable RMON remote network monitoring protocol. The no command disables RMON.
Example	Disable RMON. **Switch(config)#no rmon enable**

4.4.2 show private-mib oid

Command	**show private-mib oid**
Parameter	**none** none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Show the original oid of the private mib. Check the beginning oid of the private mib by show private-mib oid command.
Example	Show the original oid of the private mib. **Switch#show private-mib oid** Private MIB OID:1.3.6.1.4.1.6339

4.4.3 show snmp

Command	**show snmp**	
Parameter	**none**	none
Default	None.	
Mode	Admin and configuration mode	
Usage Guide	Display all SNMP counter information.	
Example	Display all SNMP counter information.	

```
Switch#show snmp
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Set-request PDUs
0 SNMP packets output
0 Too big errors (Max packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs
```

4.4.4 show snmp engineid

Command **show snmp engineid**

Parameter

none	none

Default None.

Mode Admin and configuration mode

Usage Guide Display the engine ID commands.

Example Display the engine ID commands.

```
Switch#show snmp engineid
SNMP engineID:3138633303f1276c
```

4.4.5 show snmp group

Command **show snmp group**

Parameter

none	none

Default None.

Mode Admin and configuration mode

Usage Guide Display the group information .

Example Display the group information .

```
Switch#show snmp group
Group Name:initial Security Level:noAuthnoPriv
Read View:one
Write View:<no writeview specified>
Notify View:one
```

4.4.6 show snmp mib

Command	**show snmp mib**	
Parameter	**none**	none
Default	None.	
Mode	Admin and configuration mode	
Usage Guide	Display all MIB supported by the switch.	
Example	Display all MIB supported by the switch. **Switch#show snmp mib**	

4.4.7 show snmp status

Command	**show snmp status**	
Parameter	**none**	none
Default	None.	
Mode	Admin and configuration mode	
Usage Guide	Display SNMP configuration information.	
Example	Display SNMP configuration information. **Switch#show snmp status** Trap enable RMON enable Community Information: V1/V2c Trap Host Information: V3 Trap Host Information: Security IP Information:	

4.4.8 show snmp user

Command

show snmp user

Parameter

none	none

Default

None.

Mode

Admin and configuration mode

Usage Guide

Display the user information commands.

Example

Display the user information commands.

```
Switch#show snmp user
User name: initialsha
Engine ID: 1234567890
Auth Protocol:MD5 Priv Protocol:DES-CBC
Row status:active
```

4.4.9 show snmp view

Command

show snmp view

Parameter

none	none

Default

None.

Mode

Admin and configuration mode

Usage Guide

Display the view information.

Example

Display the view information.

```
Switch#show snmp view
View Name :readview       1. -Included active
                         1.3. Excluded active
```

4.4.10 snmp-server community

Command

```
snmp-server community {ro | rw} {0 | 7} <string> [access {<num-std> | <name>}]
[ipv6-access {<ipv6-num-std> | <ipv6-name>}] [read <read-view-name>]
[write <write-view-name>]
no snmp-server community {ro | rw} {0 | 7} <string> [access {<num-std> | <name>}]
[ipv6-access {<ipv6-num-std> | <ipv6-name>}]
```

Parameter

{ro | rw}	the specified access mode to MIB, ro for read-only and rw for read-write
{0 | 7}	if key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted
<string>	the configured community string
<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
<read-view-name>	the name of readable view which includes 1-32 characters
<write-view-name>	the name of writable view which includes 1-32 characters

Default

None.

Mode

Global Mode

Usage Guide

Configure the community string for the switch.

The switch supports up to 4 community strings. It can realize the access-control for specifically community view by binding the community name to specifically readable view or writable view.

The no command deletes the configured community string.

Example

Add a community string named "private" with read-write permission.

```
Switch(config)#snmp-server community rw 0 private
```

Delete the community string named "private".

```
Switch(config)#no snmp-server community 0 private
```

4.4.11 snmp-server enable

Command	**snmp-server enable** **no snmp-server enable**
Parameter	**none** none
Default	None.
Mode	Global Mode
Usage Guide	Enable the SNMP proxy server function on the switch. To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command. The "no snmp-server enable" command disables the SNMP proxy server function.
Example	Enable the SNMP proxy server function on the switch. **Switch(config)#snmp-server enable**

4.4.12 snmp-server enable traps

Command	**snmp-server enable traps** **no snmp-server enable traps**
Parameter	**none** none
Default	By default forbid to send Trap message.
Mode	Global Mode
Usage Guide	Enable the switch to send Trap message. When Trap message is enabled, if Down/Up in device ports or of system occurs,the device will send Trap messages to NMS that receives Trap messages. The no command disables the switch to send Trap message.
Example	Enable to send Trap messages. **Switch(config)#snmp-server enable traps**

4.4.13 snmp-server engineid

Command

```
snmp-server engineid <engine-string>
no snmp-server engineid
```

Parameter

<engine-string>	the engine ID shown in 1-32 digit hex characters

Default

Default value is the company ID plus local MAC address.

Mode

Global Mode

Usage Guide

Configure the engine ID.

The "no" form of this command restores to the default engine ID.

Example

Set current engine ID to A66688999F

```
Switch(config)#snmp-server engineid A66688999F
```

4.4.14 snmp-server group

Command

snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [[read <read-string>] [write <write-string>] [notify <notify-string>]] [access {<num-std> | <name>}] [ipv6-access {<ipv6-num-std> | <ipv6-name>}]

no snmp-server group <group-string> {NoauthNopriv | AuthNopriv | AuthPriv} [access {<num-std> | <name>}] [ipv6-access {<ipv6-num-std> | <ipv6-name>}]

Parameter

<group-string>	group name which includes 1-32 characters
NoauthNopriv	Applies the non recognizing and non encrypting safety level
AuthNopriv	Applies the recognizing but non encrypting safety level
AuthPriv	Applies the recognizing and encrypting safety level
<read-string>	Name of readable view which includes 1-32 characters
<write-string>	Name of writable view which includes 1-32 characters
<notify-string>	Name of trappable view which includes 1-32 characters
<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL,ranging between 500-599
<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32

Default

None.

Mode

Global Mode

Usage Guide

This command is used to configure a new group.

There is a default view "v1defaultviewname" in the system. It is recommended to use this view as the view name of the notification. If the read or write view name is empty, corresponding operation will be disabled.

The "no" form of this command deletes this group.

Example

Create a group CompanyGroup, with the safety level of recognizing andencrypting, the read viewname isreadview, and the writing is disabled.

```
Switch (config)#snmp-server group CompanyGroup AuthPriv read readview
```

4.4.15 snmp-server host

Command

```
snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {v1 | v2c |
{v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>
no snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {v1 | v2c |
{v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>
```

Parameter

<host-ipv4-address>	IP address of NMS management station which receives Trap message
<host-ipv6-address>	IPv6 address of NMS management station which receives Trap message
v1 | v2c | v3	the version number when sending the trap
NoauthNopriv	Applies the non recognizing and non encrypting safety level
AuthNopriv	Applies the recognizing but non encrypting safety level
AuthPriv	Applies the recognizing and encrypting safety level
<user-string>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3

Default

None.

Mode

Global Mode

Usage Guide

As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for receiving the network manage station IPv4 or IPv6 address and the Trap user name and safety level.

The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version are less than 8 in all.

The "no"form of this command cancels this IPv4 or IPv6 address.

Example

Configure an IP address to receive Trap.

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

4.4.16 snmp-server securityip

Command

snmp-server securityip {<ipv4-address> | <ipv6-address>}

no snmp-server securityip {<ipv4-address> | <ipv6-address>}

Parameter

<ipv4-address>	NMS security IPv4 address, dotted decimal notation
<ipv6-address>	NMS security IPv6 address, colon hexadecimal

Default

None.

Mode

Global Mode

Usage Guide

Configure security IPv4 or IPv6 address allowed to access NMS management station

It is only the consistency between NMS administration station IPv4 or IPv6 address and security IPv4 or IPv6 address configured by the command, so it send SNMP packet could be processed by switch, the command only applies to SNMP. Allows configuration the IPv4 or IPv6 address of the network manage station receiving the SNMP Trap message, but the IP addresses are less than 20 in all.

The no command deletes security IPv4 or IPv6 address configured.

Example

Configure security IP address of NMS management station.

```
Switch(config)#snmp-server securityip 1.1.1.5
```

4.4.17 snmp-server securityip enable

Command

snmp-server securityip {enable | disable}

Parameter

enable | disable	SNMP security ip configuration enabled or disabled

Default

Enable the security IP address authentication function.

Mode

Global Mode

Usage Guide

Enable/disable the security IP address authentication on NMS management station.

Example

Disable the security IP address authentication function.

```
Switch(config)#snmp-server securityip disable
```

4.4.18 snmp-server trap-source

Command

snmp-server trap-source {<ipv4-address> | <ipv6-address>}
no snmp-server trap-source {<ipv4-address> | <ipv6-address>}

Parameter

<ipv4-address>	IPv4 address is used to send trap packet in dotted decimal notation
<ipv6-address>	IPv6 address is used to send trap packet in colon hexadecimal

Default

None.

Mode

Global Mode

Usage Guide

Set the source IPv4 or IPv6 address which is used to send trap packet.
If there is no configuration, select the source address according to the interface address sent by actual trap packet, when configure the IP address,adopt the configured source address as the source address of trap packet.

The no command deletes the configuration.

Example

Set the IP address which is used to send trap packet.

```
Switch(config)#snmp-server trap-source 1.1.1.5
```

4.4.19 snmp-server user

Command

snmp-server user <use-string> <group-string> [{authPriv [auth {md5 | sha} <word>]} | {authNoPriv [{3des | aes | des} <word>]} [auth {md5 | sha} <word>]] [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]

no snmp-server user <user-string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}]

Parameter

<use-string>	the user name containing 1-32 characters
<group-string>	the name of the group the user belongs to, containing 1-32 characters
authPriv	use DES for the packet encryption

authNoPriv	not use DES for the packet encryption
auth	perform packet authentication
md5	packet authentication using HMAC MD5 algorithm
sha	packet authentication using HMAC SHA algorithm
3des	packet authentication using 3DES to encrypt
aes	packet authentication using AES to encrypt
des	packet authentication using DES to encrypt
<word>	user password, containing 8-32 character
<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32

Default

None.

Mode

Global Mode

Usage Guide

Add a new user to an SNMP group.
If the encryption and authentication is not selected, the default settings will
be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

The "no" form of this command deletes this
user.

Example

Add a new user tester in the UserGroup with HMAC md5 for authentication, the password is hellohello;Delete an User

```
Switch (config)#snmp-server user tester UserGroup authNoPriv auth md5 hellohello
Switch (config)#no snmp-server user tester
```

4.4.20 snmp-server view

Command

```
snmp-server view <view-string> <oid-string> {include | exclude}
no snmp-server view <view-string> [ <oid-string> ]
```

Parameter

<view-string>	view name, containing 1-32 characters
<oid-string>	OID number or corresponding node name, containing 1-255 characters
include | exclude	include/exclude this OID

Default

None.

Mode

Global Mode

Usage Guide

This command is used to create or renew the view information.

The command supports not only the input using the character string of the variable OID as parameter. But also supports the input using the node name of the parameter.

the “no" form of this command deletes the view information.

Example

Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them.

```
Switch(config)#snmp-server view readview iso include
Switch(config)#snmp-server view readview iso.3 exclude

Switch(config)#no snmp-server view readview
```

4.4.21 switchport updown notification enable

Command	**switchport updown notification enable** **no switchport updown notification enable**
Parameter	**none** none
Default	Send the trap message to the port of IP/DOWN event as default.
Mode	Port Mode
Usage Guide	Enable/disable the function of sending the trap message to the port of UP/DOWN event. This command can control to send the trap message when the port happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap. The no command deletes the configuration.
Example	Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event. **Switch(config)#in e 1/0/1** **Switch(config-if-ethernet1/0/1)#no switchport updown notification enable** **Switch(config-if-ethernet1/0/1)#show running-config current-mode** ! Interface Ethernet1/0/1 no switchport updown notification enable

4.5 Switch Upgrade

4.5.1 copy（FTP）

Command

copy <source-url> <destination-url> [ascii | binary]

Parameter

<source-url>	the location of the source files or directories to be copied
<destination-url>	the destination address to which the files or directories to be copied
ascii	ASCII standards will be adopted
binary	File transfer will be in binary mode (default transfer method)

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to transfer files by TFP.

When URL represents an FTP address, its form should be: ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>,amongst <username> is the FTP user name, <password> is the FTP user password, <ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the FTP server/client,<hostname> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <filename> is the name of the FTP upload/download file.

Special keywords of the filename

keywords	explain
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files
stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode
stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode

This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> ftp:// or copy ftp:// <filename> and press Enter, following hints will be provided by the system：

ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] >

ftp username>

ftp password>

ftp filename>

Requesting for FTP server address, user name, password and file name

Example

Save images in the FLASH to the FTP server of 10.1.1.1, FTP server username is Switch, password is superuser:

```
Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img
```

Obtain system file nos.img from the FTP server 10.1.1.1, the username is Switch, password is superuser

```
Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img
```

Save the running configuration files.

```
Switch#copy running-config startup-config
```

4.5.2 copy（TFTP）

Command

copy <source-url> <destination-url> [ascii | binary]

Parameter

<source-url>	the location of the source files or directories to be copied
<destination-url>	the destination address to which the files or directories to be copied
ascii	ASCII standards will be adopted
binary	File transfer will be in binary mode (default transfer method)

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to transfer files by TTFP.

When URL represents a TFTP address, its form should be:

tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>, amongst <ipaddress>|<ipv6address> is the IPv4 or IPv6 address of the TFTP server/client, <hostname> is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, <filename> is the name of the TFTP upload/download file.

Special keyword of the filename

keywords	explain
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files

This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> tftp:// or copy tftp:// <filename> and press Enter, following hints will be provided by the system:tftp server ip/ipv6 address[x.x.x.x]/[x:x::x:x]>tftp filename> Requesting for TFTP server address, file name

Example

Save images in the FLASH to the TFTP server of 10.1.1.1

Switch#copy nos.img tftp://10.1.1.1/nos.img

Obtain system file nos.img from the TFTP server 10.1.1.1

Switch#copy tftp://10.1.1.1/nos.img nos.img

Save the running configuration files

Switch#copy running-config startup-config

4.5.3 ftp-dir

Command	**ftp-dir <ftp-server-url>**
Parameter	**<ftp-server-url>** ftp server address
Default	None.
Mode	Admin Mode
Usage Guide	Browse the file list on the FTP server. The form of <ftp-server-url> is ： ftp://<username>:<password>@{ <ipv4address> | <ipv6address> }, amongst <username> is the FTP user name, <password> is the FTP user password, { <ipv4address> | <ipv6address> } is the IPv4 or IPv6 address of the FTP server.
Example	Browse the list of the files on the server with the FTP client, the username is "Switch", the password is "superuser". **Switch#ftp-dir ftp://Switch:superuser @10.1.1.1**

4.5.4 ftp-server enable

Command	**ftp-server enable** **no ftp-server enable**
Parameter	**none** none
Default	FTP server is not started by default.
Mode	Global Mode
Usage Guide	This command is used to start the FTP server. When FTP server function is enabled, the switch can still perform ftp client functions. The "no ftp-server enable" command shuts down FTP server and prevents FTP user from logging in.
Example	Enable FTP server services. **Switch(config)# ftp-server enable**

4.5.5 ftp-server timeout

Command	**ftp-server timeout <seconds>**	
Parameter	**<seconds>**	the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600
Default	The system default is 600 seconds.	
Mode	Global Mode	
Usage Guide	This command is used to configure FTP data connection idle time. When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.	
Example	Modify the idle threshold to 100 seconds. **Switch(config)#ftp-server timeout 100**	

4.5.6 ip ftp

Command	**ip ftp username <username> password [0 | 7] <password>** **no ip ftp username <username>**	
Parameter	**<username>**	the username of the FTP link, its range should not exceed 32 characters
	[0 | 7]	0 means password is not encrypted ,7 means password is encrypted
	<password>	FTP link password
Default	The system uses anonymous FTP links by default.	
Mode	Global Mode	
Usage Guide	Configure the username and password for logging in to the FTP. The no operation of this command will delete the configured username and password simultaneously.	
Example	Configure the username as Switch and the password as superuser. **Switch(config)#ip ftp username Switch password 0 superuser**	

4.5.7 show ftp

Command	**show ftp**
Parameter	**none** none
Default	None.
Mode	Admin and Global Mode
Usage Guide	Display the parameter settings for the FTP server.
Example	Display the parameter settings for the FTP server. **Switch#show ftp** Timeout : 600

4.5.8 show tftp

Command	**show tftp**
Parameter	**none** none
Default	None.
Mode	Admin and Global Mode
Usage Guide	Display the parameter settings for the TFTP server.
Example	Display the parameter settings for the TFTP server. **Switch#show tftp** timeout : 60 Retry Times : 10

4.5.9 tftp-server enable

Command	**tftp-server enable** **no tftp-server enable**
Parameter	**none** none
Default	Disable TFTP Server.
Mode	Global Mode
Usage Guide	This command is used to start the TFTP server. The "no ftp-server enable" command shuts down TFTP server and prevents TFTP user from logging in.
Example	Start the TFTP server. **Switch(config)#tftp-server enable**

4.5.10 tftp-server retransmission-number

Command	**tftp-server retransmission-number <number>**
Parameter	**<number>** the time to re-transfer, the valid range is 1 to 20
Default	Retransmit 5 times.
Mode	Global Mode
Usage Guide	Set the retransmission time for TFTP server.
Example	Modify the retransmission to 10 times. **Switch(config)#tftp-server retransmission-number 10**

4.5.11 tftp-server transmission-timeout

Command	**tftp-server transmission-timeout <seconds>**
Parameter	**<seconds>** the timeout value, the valid range is 5 to 3600s
Default	The system default timeout setting is 600 seconds.
Mode	Global Mode
Usage Guide	Set the transmission timeout value for TFTP server.
Example	Modify the timeout value to 60 seconds. **Switch(config)#tftp-server transmission-timeout 60**

4.6 File System

4.6.1 cd

Command	**cd <directory>**	
Parameter	**<directory>**	the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80
Default	The default working directory is Flash.	
Mode	Admin Mode	
Usage Guide	Change the working directory for the storage device. After this command implemented, the current storage device will switch to the new working directory, which can be viewed by the "pwd" command.	
Example	Change the working directory of the current storage device to flash. **Switch#cd flash:** **Switch#pwd** flash:/	

4.6.2 copy

Command

copy <source-file-url > <dest-file-url>

Parameter

<source-file-url>	The source address of the file or directory to be copied
<dest-file-url>	The destination address of the file or directory to be copied

Default

None.

Mode

Admin Mode

Usage Guide

Copy a designated file on the switch and store it as a new file.

When users operate on files stored in backup master board and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements.

1. The prefix of the source file URL should be in one of the following forms: □ starting with "flash:/"

□ "ftp://username:pass@server-ip/file-name"

□ "tftp://server-ip/file-name"

2. The prefix of the destination file URL should be in one of the following forms:

□ starting with "flash:/"

□ "ftp://username:pass@server-ip/file-name"

□ "tftp://server-ip/file-name"

when the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.

To use this command, the designated source file should exist, and the destination file should not be named the same as any existing directory or file, otherwise, there might be a prompt warning about a failed copy operation or an attempt to overwrite an existing file.

If the source and destination files are in different directories, with this command implemented, users can copy files from other directories into the current one.

Example

Copy the file "flash:/nos.img" and store it as "flash/ 6.1.11.0.img".

```
Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y
Copyed file flash:/nos.img to flash:/nos-6.1.11.0.img
```

4.6.3 delete

Command	**delete <file-url>**	
Parameter	**<file-url>**	the full path of the file to be deleted
Default	None.	
Mode	Admin Mode	
Usage Guide	Delete the designate file on the storage device.	

Example

Delete file flash:/nos.img.

```
Switch#delete flash:/nos5.img
Delete file flash:/nos5.img?[Y:N]y
Deleted file flash:/nos.img
```

4.6.4 dir

Command	**dir [WORD]**	
Parameter	**[WORD]**	the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.
Default	No <WORD> means to display information of the current working directory.	
Mode	Admin Mode	
Usage Guide	Display the information of the designated directory on the storage device. This command does not support a recursive display of all sub-directories.	

Example

Display information of the directory “flash:/”.

```
Switch#dir flash:/
nos.img                  2,449,496       1980-01-01 00:01:06 ----
startup-config           2,064           1980-01-01 00:30:12 ----
Total 7, 932, 928 byte(s) in 4 file(s)，  free 4, 966, 400 byte(s)

Switch#
```

4.6.5 pwd

Command	**pwd**	
Parameter	**none**	none
Default	The default directory is flash.	
Mode	Admin Mode	
Usage Guide	Display the current working directory.	
Example	Display the current working directory. **Switch#pwd** flash:/	

4.6.6 rename

Command	**rename <source-file-url> <new-filename >**	
Parameter	**<source-file-url>**	the source file, in which whether specifying or not its path are both acceptable
	<new-filename >	filename without specifying its path
Default	None.	
Mode	Admin Mode	
Usage Guide	Rename a designated file on the switch. When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.	
Example	Change the name of file "nos.img" in the current working directory to "nos-6.1.11.0.img". **Switch# rename nos5.img nos-6.1.11.0.img** Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok！	

Chapter 5 Port Configuration

5.1 Ethernet Port Configuration

5.1.1 bandwidth

Command

bandwidth control <*bandwidth***> {transmit | receive | both}**

no bandwidth control

parameter

bandwidth	is the bandwidth limit, which is shown in kbps ranging between 1-1000000K

default

Disable bandwidth restrictions by default

Mode

Port Configuration Mode

Usage Guide

Use the **bandwidth control <bandwidth>[both | receive | transmit]** command to set the bandwidth rate.

Use the **no bandwidth control** restore default configuration

Example

Set the bandwidth limit of 1/0/1-8 port is 40000K.

```
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#bandwidth control 40000 both
```

5.1.2 clear counters interface

Command	**clear counters [interface {ethernet <*interface-list*> | vlan <*vlan-id*> |** **port-channel <*port-channel-number*> | <*interface-name*>}]**
parameter	

interface-list	stands for the Ethernet port number;
vlan-id	stands for the VLAN interface number;
port-channel-number	for trunk interface number;
interface-name	for interface name, such as port-channel 1.

default	Port statistics default not cleared
Mode	Admin Mode
Usage Guide	If no port is specified, statistics for all ports are cleared.
Example	Clearing the statistics for Ethernet port1/0/1. Switch#clear counters interface ethernet 1/0/1

5.1.3 description

Command	**description <*string*>** **no description**
parameter	

string	is a character string, which should not exceeds 200 characters

default	No port name by default
Mode	Port Mode
Usage Guide	This command is for helping the user manage switches, such as the user assign names according to the port application, e.g. financial as the name of 1/0/1-2 ports

which is used by financial department, engineering as the name of 1/0/9 ports which belongs to the engineering department, while the name of 1/0/12 ports is assigned with Server, which is because they connected to the server. In this way the port distribution state will be brought to the table.

Example

Specify the description of 1/0/1-2 port as financial.

```
Switch(config)#interface ethernet 1/0/1-2
Switch(Config-If-Port-Range)#description financial
```

5.1.4 flow control

Command

flow control

no flow control

parameter

-

default

Disable port traffic control by default

Mode

Port Mode

Usage Guide

After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. Ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Example

Enabling the flow control function in ports 1/0/1-8.

```
Switch(config)#interface ethernet 1/0/1-8
Switch(Config-If-Port-Range)#flow control
```

5.1.5 interface Ethernet

Command	**interface ethernet <*interface-list*>**	
parameter	*interface-list*	stands for port number.
default	-	
Mode	Global Mode	
Usage Guide	This command can be used to enter port configuration mode and run exit command to exit Ethernet port mode to global mode.	
Example	Entering the Ethernet Port Mode for ports1/0/1，1/0/4-5，1/0/8。 Switch(config)#interface ethernet 1/0/1;1/0/4-5;1/0/8 Switch(Config-If-Port-Range)#	

5.1.6 Loopback

Command	**loopback** **no loopback**
parameter	-
default	By default, disable loop testing in the Ethernet port
Mode	Port Mode
Usage Guide	Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.
Example	Enabling loopback test in Ethernet ports 1/0/1-8. Switch(config)#interface ethernet 1/0/1-8 Switch(Config-If-Port-Range)#loopback

5.1.7 Negotiation

Command	**negotiation {on | off}**
parameter	-
default	Auto-negotiation is enabled by default.
Mode	Port configuration Mode
Usage Guide	This command applies to 1000Base-FX interface only. The negotiation command is not available for 1000Base-TX or 100Base-TX interface. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use speed-duplex command instead.
Example	Port 21 of Switch1 is connected to port 21 of Switch2, the following will disable the negotiation for both ports. Switch1(config)#interface ethernet1/0/21 Switch1(Config-If-Ethernet1/0/21)#negotiation off Switch2(config)#interface ethernet1/0/21 Switch2(Config-If-Ethernet1/0/21)#negotiation off

5.1.8 Port-rate-statistics interval

Command	**port-rate-statistics interval <***interval-value***>**	
parameter	*interval-value*	The interval of port-rate-statistics, unit is second, ranging from 5 to 600 with the configuration step of 5.
default	Only port-rate-statistics of 5 seconds and 5 minutes are displayed.	
Mode	Global Mode	
Usage Guide	This command can be used to set the port rate statistics interval time.	
Example	Count the interval of port-rate-statistics as 20 seconds. Switch(config)#port-rate-statistics interval 20	

5.1.9 rate-violation

Command

```
rate-violation [broadcast | multicast | unicast | all] <200-2000000>
no rate-violation
```

parameter

broadcast	broadcast packet
multicast	multicast packet
unicast	unicast packet
all	all packets
<200-2000000>	the number of packets allowed to pass per second.

default

There is no limit for the packet reception rate.

Mode

Port Mode

Usage Guide

This command is mainly used to detect the abnormal port flow. For example, when there are a large number of broadcast packets caused by a loopback, which affect the processing of other tasks, the port will be shut down or block to ensure the normal processing of the switch. This command needs to associate with rate-violation control command.

Example

Set the rate-violation of port 1/0/8-10 (GB ports) as 10000pps, it will be shutdown after rate-violation and the port recovery time as 1200 seconds, when the packet reception rate exceeds 10000, the port will but shut down, and then, after 1200 seconds, the port will be UP again.

```
Switch(config)#interface ethernet 1/0/8-10
Switch(Config-Port-Range)#rate-violation unicast 10000
Switch(Config-Port-Range)#rate-violation control shutdown recovery 1200
```

5.1.10 rate-violation control

Command	**rate-violation control [shutdown recovery <0-86400> | block]** **no rate-violation control**	
parameter	**shutdown**	A port is shutdown after rate-violation
	recovery	After a period of time the port can recover Shutdown to UP again.
	block	A port is block after rate-violation, this parameter and MSTP, EAPS(MRPP), Loopback Detection, ULPP are mutually exclusive. If other modules set STP state, this function can not be set to block mode.
	<0-86400>	Automatic recovery time
default	There is no control operation for rate-violation.	
Mode	Port Mode	
Usage Guide	This command is mainly used to the control operation after rate-violation.	
Example	After set the rate-violation of the unicast packet of port 1/8-10 (GB ports) as 10000pps, the port will be block.	

```
Switch(Config)#interface ethernet 1/0/8-10
Switch(Config-Port-Range)#rate-violation unicast 10000
Switch(Config-Port-Range)#rate-violation control block
```

5.1.11 show interface

Command

show interface [ethernet <*interface-number*> | port-channel <*port-channel-number*> | vlan <*vlan-id*> | <*interface-name*>] [detail]

show interface ethernet status

show interface ethernet counter {packet | rate}

parameter

interface-number	is the port number of the Ethernet,
port-channel-number	is the number of the aggregation interface
vlan-id	is the VLAN interface number, the value range from 1 to 4094
interface-name	is the name of the interface such as port-channel1
detail	show the detail of the port

default

Information not displayed by default

Mode

Admin and Configuration Mode.

Usage Guide

Use this command to view interface-related configuration information

Example

Show the information of VLAN 1 .

```
Vlan1 is up, line protocol is up, dev index is 11001
  Device flag 0x1003(UP BROADCAST MULTICAST)
  Time since last status change:0w-0d-1h-14m-57s   (4497 seconds)
  IPv4 address is:
    192.168.2.1         255.255.255.0        (Primary)
  VRF Bind: Not Bind
  Hardware is EtherSVI, address is 00-1f-ce-10-b0-1a
  MTU is 1500 bytes , BW is 0 Kbit
  Encapsulation ARPA, loopback not set
  5 minute input rate 244 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  The last 5 second input rate 0 bits/sec, 0 packets/sec
  The last 5 second output rate 0 bits/sec, 0 packets/sec
  Input packets statistics:
    Input queue 0/600, 0 drops
    1012 packets input, 193127 bytes, 0 no buffer
    0 input errors, 0 CRC, 0 oversize, 0 undersize
     0 jabber, 0 fragments
  Output packets statistics:
    448 packets output, 108316 bytes, 0 underruns
    0 output errors, 0 collisions
```

5.1.12 Shutdown

Command	**Shutdown**
parameter	-
default	Ethernet port is open by default.
Mode	Port Mode.
Usage Guide	When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the "show interface" command is "down".
Example	Opening ports 1/0/1-8. Switch(config)#interface ethernet1/0/1-8 Switch(Config-If-Port-Range)#no shutdown

5.1.13 speed-duplex

Command

speed-duplex {auto [10 [100 [1000]] [auto | full | half |]] | force10-half | force10-full | force100-half | force100-full | force100-fx [module-type {auto-detected |
no-phy-integrated | phy-integrated}] | {{force1g-half | force1g-full} [nonegotiate [master | slave]]}}

no speed-duplex

parameter

auto	is the auto speed and duplex negotiation
10	10kbps
100	100kbps
1000	1000kbps
force10-half	is the forced 10Mbps at half-duplex mode
force10-full	is the forced 10Mbps at full-duplex mode
force100-half	is the forced 100Mbps at half-duplex mode
force100-full	is the forced 100Mbps at full-duplex mode
force1g-half	is the forced 1000Mbps at half-duplex mode
force1g-full	is the forced 1000Mbps at full-duplex mode
force100-fx	is the forced 100Mbps at full-duplex mode
auto-detected	automatic detection

no-phy-integrated	there is no phy-integratd 100Base-FX module
phy-integrated	phy-integratd 100Base-FX module
nonegotiate	disables auto-negotiation forcibly for 1000Mb port
master	forces the 1000Mb port to be master mode
slave	Forces the 1000Mb port to be slave mode

default

Auto-negotiation for speed and duplex mode is set by default

Mode

Port Mode

Usage Guide

This command is configures the port speed and duplex mode. When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

1000Gb ports are by default **master** when configuring **nonegotiate** mode. If one end is set to **master** mode, the other end must be set to **slave** mode.

force1g-half is not supported yet.

Example

Port 1 of Switch1 is connected to port 1 of Switch2, the following will set both ports in forced 100Mbps at half-duplex mode.

```
Switch1(config)#interface ethernet1/0/1
Switch1(Config-If-Ethernet1/0/1)#speed-duplex force100-half
Switch2(config)#interface ethernet1/0/1
Switch2(Config-If-Ethernet1/0/1)#speed-duplex force100-half
```

5.1.14 storm-control

Command

storm-control { kbps | pps }
no storm-control pps

parameter

kbps	means the unit of limit is kbits/s
pps	means the limit unit ispackets/s.

default

The default is kbps.

Mode

Global Mode

Usage Guide

Configure the kbps or pps as the limit mode in global mode, then set broadcast, multicast or unknown unicast limit value in port mode.

Example

Setting ports 1-8 allow 1000kbit broadcast packets per second.

```
Switch(config)#storm-control kbps
Switch(config-if-port-range)#storm-control broadcast 1000
```

5.1.15 storm-control

Command

storm-control {unicast | broadcast | multicast} <*value*>
no storm-control {unicast | broadcast | multicast}

parameter

unicast	to limit unicast traffic for unknown destination
broadcast	to limit broadcast traffic.
multicast	to limit multicast traffic
value	Limit the flow rate per second, PPS range from 1 to 1488095; kbps range from 1 to 1000000.

default

No limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.

Mode

Port Mode

Usage Guide

All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the above mentioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance.

Enabling Broadcast Storm Control can better protect the switch from broadcast storm. If the allowed traffic is set to 1000kbps, this means allow 1000 kbit per second and suppress the rest. The switch supports two kind of speed limit, it includes kbps which is limit by bandwidth and pps which is limit by the numbers of packets. It only can select one from the two ways and cannot set the two way in the same time (by global mode) Broadcast suppression is similar to bandwidth control. There is granularity limitation for the chip; the switch support 16Kbps granularities. If the <Kbits> that user input is not the integer times of 16, the system will adjust to the integer times of 16 automatically and print the true limit value to user.

Example

Setting ports 1-8 allow 1000kbit broadcast packets per second.

```
Switch(config-if-port-range)#storm-control broadcast 1000
```

5.1.16 storm-control bypass

Command

storm-control bypass {arp | bpdu | igmp | rma | rek } <enable | disable >

parameter

arp	means the protocol packets of arp-request
bpdu	means bpdu protocol packets
igmp	means igmp protocol packets
rma	means multicast address is the saved multicast packets
rek	means the special private packets that realtak used
enable	enable some protocol to limit filter function
disable	disable some protocol to broadcast limit filter function.

default

Disable

Mode

Global Mode.

Usage Guide

Configure broadcast limit filter function of some protocol in global mode,
then configure broadcast limit in port mode. At this moment, the protocol packets flow from
the port cannot be limited.

Example

Configure arp protocol filter function to make the arp-request data packets
thatfrom 1 port in cannot be limited.

```
Switch (config)#storm-control bypass arp enable
Switch(config-if-ethernet1/0/1)#storm-control broadcast 1000
```

5.1.17 virtual-cable-test

Command

virtual-cable-test interface ethernet <_interface-list_**>**

parameter

interface-list	Port ID

default

-

Mode

Admin Mode.

Usage Guide

The RJ-45 port connected with the twisted pair under test should be in accordance with the wiring sequence rules of IEEE802.3, or the wire pairs in the test result may not be the actual ones. On a 100M port, only two pairs are used: (1, 2) and (3, 6), whose results are the only effective ones. If a 1000M port is connected to a 100M port, the results of (4, 5) and (7, 8) will be of no meaning. The result may have deviations according to the type of the twisted pair, the temperature, working voltage and other conditions. When the temperature is 20 degree Celsius, and the voltage is stable without interference, and the length of the twisted pair is not longer than 100 meters, a deviation of +/-2 meters is allowed. When the port is at Link UP status, a deviation of +/-10 meters is allowed. Notice: the test procedure will block all data flow on the line for 5-10 seconds, and then restore the original status.

568A wiring sequence: (1 green white, 2 green), (3 orange white, 6 orange), (4 blue, 5 blue white), (7 brown white, 8 brown).

568B wiring sequence: (1 orange white, 2 orange), (3 green white, 6 green), (4 blue, 5 blue white), (7 brown white, 8 brown).

Example

Test the link status of the twisted pair connected to the 1000M port 1/0/1.

```
Switch#virtual-cable-test interface ethernet 1/0/1

Interface Ethernet1/0/1:
----------------------------------------------
Cable pairs      Cable status     Length (meters)
-----------      ------------     ---------------
(1, 2)            well                    1
(3, 6)            well                    1
(4, 5)            well                    1
(7, 8)            well                    1
```

5.1.18 switchport discard packet

Command

switchport discard packet { all | untag }
no switchport discard packet { all | untag }

parameter

all	means it does not receive any packet including untag, tag and the deal packet
untag	means it does not receive untag

default

The default does not have the restriction.

Mode

Port Mode

Usage Guide

This command is not suggested to be configured only if there is the special requirement.

Example

Configure the port of 1/0/8 not to receive all packets.

```
Switch(config)#interface ethernet 1/0/8
Switch(config-if-ethernet1/0/8)#switchport discard packet all
```

5.1.19 switchport flood-control

Command

switchport flood-control { bcast|mcast|ucast }
no switchport flood-control { bcast|mcast|ucast }

parameter

bcast	prevents that broadcast packets cannot be transmitted to the specified port
mcast	prevents that unknown multicast packets cannot be transmitted to the specified port
ucast	prevents that unknown unicast packets cannot be transmitted to the specified port

default

Switch transmits broadcast, unknown multicast and unknown unicast packets to other port in broadcast domain.

Mode

Port configuration mode.

Usage Guide

This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. When this command is valid, the port will allow unicast or multicast flow to pass after port learned the corresponding unicast mac or multicast mac. This command only control that broadcast, multicast and unknown unicast packets sent by other ports cannot be transmitted to the specified port, but it cannot control these packets from the specified port. For example, set switchport flood-control bcast command in port 1/0/1, broadcast packets cannot be transmitted from other ports to port 1/0/1, but port 1/0/1 can receive and transmit broadcast packets.

Example

Configure flood-control of bcast and mcast for port 1/0/1 or port 1/0/8-10 respectively.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport flood-control bcast
Switch(config)#interface ethernet 1/0/8-10
Switch(config-if-port-range)#switchport flood-control mcast
```

5.1.20 switchport flood-forwarding

Command

switchport flood-forwarding mcast

no switchport flood-forwarding mcast

parameter

mcast	prevents that unknown multicast packets can be transmitted to the specified port.

default

Switch transmits unknown multicast packets to other port in broadcast domain.

Mode

Port Mode

Usage Guide

This command takes effect for 100M and 1000M ports; it is also takes effect for Access, Trunk and Hybrid ports. The command is usually combined with ip imgp snooping, ip imgp snooping does not supports unknown multicast and broadcast, it can transfer unknown multicast flow after configure switchport flood-forwarding mcast.

Example

Set switch 1/0/1 port broadcast flood-forwarding.

```
switch#
switch#confi
switch(config)#interface ethernet 1/0/1
switch(config-if-ethernet1/0/1)# switchport flood-forwarding mcast
switch(config-if-ethernet1/0/1)#exit
switch(config)#
```

5.2 Port Isolation Function

5.2.1 isolate-port group

Command	**isolate-port group <*WORD*>** **no isolate-port group <*WORD*>**	
parameter	*WORD*	is the name identification of the group, no longer than 32 characters
default	-	
Mode	Global Mode	
Usage Guide	Users can create different port isolation groups based on their requirements. For example, if a user wants to isolate all downlink ports in a vlan of a switch, he can implement that by creating a port isolation group and adding all downlink ports of the vlan into it. No more than 16 port isolation groups can a switch have. When the users need to change or redo the configuration of the port isolation group, he can delete the existing group with the no operation of this command.	
Example	Create a port isolation group and name it as ”test”. Switch>enable Switch#config Switch(config)#isolate-port group test	

5.2.2 isolate-port group switchport interface

Command	**isolate-port group <*WORD*> switchport interface [ethernet] <*IFNAME*>** **no isolate-port group <*WORD*> switchport interface [ethernet] <*IFNAME*>**	
parameter	*WORD*	is the name identification of the group, no longer than 32 characters
	IFNAME	is the name of the interface
default	-	
Mode	Global Mode or Vlan Configuration Mode	
Usage Guide	Users can add Ethernet ports into a port isolation group according to their requirements, the isolation group can isolation it from each other (Global mode) in all	

vlan,
it also can isolate it from each other (vlan mode) in some vlan or remove them from a port isolation group according to their requirements. When an Ethernet port is a member of more than one port isolate group, it will be isolated from every port of all groups it belongs to.

Example

Add Ethernet ports 1/0/1-2 and 1/0/5 into a port isolation group named as ”test”, add Ethernet ports 1/0/3-4 into a port isolation group named as ”1” in vlan10.

```
Switch(config)#isolate-port group test switchport interface ethernet 1/0/1-2; 1/0/5
Switch(config-vlan10)#isolate-port group 1 switchport interface ethernet 1/0/3-4
```

5.2.3 show isolate-port group

Command

show isolate-port group [<*WORD*>]

parameter

WORD	the name identification of the group, no longer than 32 characters

default

Display the configuration of all port isolation groups.

Mode

Admin Mode and Global Mode

Usage Guide

Users can view the configuration of port isolation with this command.

Example

Display the port isolation configuration of the port isolation group named as “test”.

```
Switch(config)#show isolate-port group test

Isolate-port group test
        The isolate-port Ethernet1/0/5
        The isolate-port Ethernet1/0/2
```

5.3 Port Loopback Detection Function

5.3.1 loopback-detection control

Command

loopback-detection control {shutdown |block }
no loopback-detection control

parameter

shutdown	set the control method as shutdown, which means to close down the port if a port loopback is found.
block	set the control method as block, which means to block a port by allowing bpdu and loopback detection messages only if a port loopback is found.

default

Disable the function of loopback diction control.

Mode

Port Mode.

Usage Guide

Enable loopback detection control on the port, which is disabled by the NO operation of this command.

Example

Enable the function of loopback detection control under port1/2 mode.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#loopback-detection control shutdown
Switch(Config-If-Ethernet1/0/2)#no loopback-detection control
```

5.3.2 loopback-detection control-recovery timeout

Command

loopback-detection control-recovery timeout <0-3600>

parameter

0-3600	second is recovery time for be controlled state, 0 is not recovery state.

default

The recovery is not automatic by default.

Mode

Global Configuration Mode.

Usage Guide

When a port detects a loopback and works in control mode, the ports always work in control mode and not recover. The port will not sent packet to detection in shutdown mode, however, the port will sent loopback-detection packet to detection whether have loopback in block or learning mode. If the recovery time is configured, the ports will recovery normal state when the overtime is time-out. The recovery time is a useful time for shutdown control mode, because the port can keep on detection loopback in the other modes, so suggest not to use this command.

Example

Enable automatic recovery of the loopback-detection control mode after 30s.

Switch(config)#loopback-detection control-recovery timeout 30

5.3.3 loopback-detection interval-time

Command

loopback-detection interval-time <*loopback***> <***no-loopback***>**

no loopback-detection interval-time

parameter

loopback	the detection interval if any loopback is found, ranging from 5 to 300, in seconds.
no-loopback	the detection interval if no loopback is found, ranging from 1 to 30, in seconds.

default

The default value is 5s with loopbacks existing and 3s otherwise.

Mode

Global Mode

Usage Guide

When there is no loopback detection, the detection interval can be relatively shorter, for too short a time would be a disaster for the whole network if there is any loopback. So, a relatively longer interval is recommended when loopbacks exist.

Example

Set the loopback diction interval as 35, 15.

Switch(config)#loopback-detection interval-time 35 15

5.3.4 loopback-detection specified-vlan

Command

loopback-detection specified-vlan <*vlan-list*>
no loopback-detection specified-vlan [<*vlan-list*>]

parameter

vlan-list	VLAN ID

default

Disable the function of detecting the loopbacks through the port.

Mode

Port Mode

Usage Guide

If a port can be a TRUNK port of multiple Vlans, the detection of loopbacks can be implemented on the basis of port+Vlan, which means the objects of the detection can be the specified Vlans on a port. If the port is an ACCESS port, only one Vlan on the port is allowed to be checked despite the fact that multiple Vlans can be configured. This function is not supported under Port-channel.

Example

Enable the function of loopback detection under port 1/2 mode.

```
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#switchport mode trunk
Switch(Config-If-Ethernet1/0/2)#switchport trunk allowed vlan all
Switch(Config-If-Ethernet1/0/2)#loopback-detection specified-vlan 1;3;5-20
Switch(Config-If-Ethernet1/0/2)#no loopback-detection specified-vlan 1;3;5-20
```

5.3.5 show loopback-detection

Command

show loopback-detection [interface <*interface-list*>]

parameter

interface-list	the list of ports to be displayed, for example: ethernet 1/0/1.

default

-

Mode

Admin and Configuration Mode.

Usage Guide

Display the state and result of loopback detection on ports with this command.

Example

Display the state of loopback detection on port 4.

```
Switch(config)#show loopback-detection interface Ethernet 1/0/4

loopback detection config and state information in the switch!
PortName Loopback Detection Control Mode Is Controlled
Ethernet1/4 Enable Shutdown No
```

5.4 ULDP

5.4.1 uldp aggressive-mode

Command	**uldp aggressive-mode** **no uldp aggressive-mode**
parameter	-
default	Global Configuration Mode and Port Configuration Mode.
Mode	Normal mode.
Usage Guide	The ULDP working mode can be configured only if it is enabled globally. When ULDP aggressive mode is enabled globally, all the existing fiber ports will work in aggressive mode. For the copper ports and fiber ports which are available after the configuration is available, aggressive mode should be enabled in port configuration mode.
Example	To enable ULDP aggressive mode globally. Switch(config)#uldp aggressive-mode

5.4.2 uldp enable

Command	**uldp {enable|disable}**
parameter	-
default	By default ULDP is not configured.
Mode	Global Configuration Mode and Port Configuration Mode.
Usage Guide	ULDP can be configured for the ports only if ULDP is enabled globally. If ULDP is enabled globally, it will be effect for all the existing fiber ports. For copper ports and fiber ports which are available after ULDP is enabled, this command should be issued in the port configuration mode to make ULDP be effect.
Example	Enable ULDP in global configuration mode. Switch(config)#uldp enable

5.4.3 uldp hello-interval

Command	**uldp hello-interval <***integer***>** **no uldp hello-interval**	
parameter	*integer*	The interval for the Hello messages, with its value limited between 5 and 100 seconds, 10 seconds by default.
default	10 seconds by default.	
Mode	Global Configuration Mode.	
Usage Guide	Interval for hello messages can be configured only if ULDP is enabled globally, its value limited between 5 and 100 seconds.	
Example	To configure the interval of Hello messages to be 12 seconds. Switch(config)#uldp hello-interval 12	

5.4.4 uldp manual-shutdown

Command	**uldp manual-shutdown** **no uldp manual-shutdown**
parameter	-
default	Auto mode.
Mode	Global Configuration Mode
Usage Guide	This command can be issued only if ULDP has been enabled globally
Example	To enable manual shutdown globally. Switch(config)#uldp manual-shutdown

5.4.5 uldp recovery-time

Command	**uldp recovery-time<***integer***>** **no uldp recovery-time**	
parameter	*integer*	the time out value for the ULDP recovery timer. Its value is limited between 30 and 86400 seconds.
default	0 is set by default which means the recovery is disabled.	
Mode	Global Configuration Mode.	
Usage Guide	If an interface is shutdown by ULDP, and the recovery timer times out, the interface will be reset automatically. If the recovery timer is set to 0, the interface will not be reset.	
Example	To set the recovery timer to be 600 seconds. Switch(config)#uldp recovery-time 600	

5.4.6 uldp reset

Command	**uldp reset**
parameter	-
default	-
Mode	Globally Configuration Mode and Port Configuration Mode.
Usage Guide	This command can only be effect only if the specified interface is disabled by ULDP.
Example	To reset all the port which are disabled by ULDP. Switch(config)#uldp reset

5.4.7 show uldp

Command	**show uldp [interface ethernet<*interface-name*>]**
parameter	*interface-name* is the interface name.
default	-
Mode	Admin and Configuration Mode.
Usage Guide	If no parameters are appended, the global ULDP information will be displayed. If the interface name is specified, information about the interface and its neighbors will be displayed along with the global information.
Example	To display the global ULDP information.

```
Switch(config)#show uldp

uldp enable
uldp hello interval is              10
uldp shut down mode is                 AUTO
uldp global work mode is              NORMAL
the total number of the port is      4

--------------------------------------------------------------------------
   PortName      PhyLink    LineProto    WorkMode        PortState   NeighborNum
--------------------------------------------------------------------------
 Ethernet1/0/25     UP          DOWN        NORMAL          INACTIVE        0
 Ethernet1/0/26     UP          DOWN        NORMAL          INACTIVE        0
 Ethernet1/0/27     UP          DOWN        NORMAL          INACTIVE        0
 Ethernet1/0/28     UP          DOWN        NORMAL          INACTIVE        0
--------------------------------------------------------------------------
```

5.5 LLDP Function

5.5.1 clear lldp remote-table

Command	**clear lldp remote-table**
parameter	-
default	Do not clear the entries.
Mode	Port Configuration Mode
Usage Guide	Clear the Remote table entries on this port.
Example	Clear the Remote table entries on this port. Switch(Config-If-Ethernet 1/0/1)# clear lldp remote-table

5.5.2 lldp enable

Command	**lldp {enable|disable}**
parameter	-
default	Disable LLDP function.
Mode	Global Mode
Usage Guide	If LLDP function is globally enabled, it will be enabled on every port.
Example	Enable LLDP function on the switch. Switch(config)#lldp enable

5.5.3 lldp enable（port）

Command	**lldp {enable|disable}**
parameter	-
default	Default Open
Mode	Port Configuration Mode.
Usage Guide	When LLDP is globally enabled, it will be enabled on every port, the switch on a port is used to disable this function when it is unnecessary on the port.
Example	Disable LLDP function of port on the port ethernet 1/0/5 of the switch. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp disable

5.5.4 lldp management-address tlv

Command	**lldp management-address tlv [A.B.C.D]** **no lldp management-address tlv**	
parameter	**A.B.C.D**	it is the optional parameter, and it is the management address that user appoints for the port, it must be the unicast IPv4 address
default	Disable	
Mode	Port Mode	
Usage Guide	User can choose the feat management IPv4 address according to the configuration. If user appointed the management address when enable the function, this address will be used to send the management address TLV; if user does not appoint the management address, choose the IPv4 address from the VLAN layer3 as the management address to send the management address TLV. When the address is not appointed, if there is no feat address, the management address TLV information will not be sent.	
Example	Enable the management address TLV function of ethernet 1/0/1 and appoint the address. Switch1(Config-If-Ethernet1/0/1)# lldp management-address tlv 192.168.24.32	

5.5.5 lldp mode

Command	**lldp mode <send | receive | both | disable>**	
parameter	**send**	Configure the LLDP function as only being able to send messages.
	receive	Configure the LLDP function as only being able to receive messages.
	both	Configure the LLDP function as being able to both send and receive messages.
	disable	Configure the LLDP function as not being able to send or receive messages.
default	The operating state of the port is "both".	
Mode	Port Configuration Mode.	
Usage Guide	Choose the operating state of the lldp Agent on the port.	
Example	Configure the state of port ethernet 1/0/5 of the switch as "receive". Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp mode receive	

5.5.6 lldp msgTxHold

Command	**lldp msgTxHold <*value*>** **no lldp msgTxHold**	
parameter	*value*	is the aging time multiplier, ranging from 2 to 10.
default	the value of the multiplier is 4 by default.	
Mode	Global Mode.	
Usage Guide	After configuring the multiplier, the aging time is defined as the product of the multiplier and the interval of sending messages, and its maximum value is 65535 seconds.	
Example	Set the value of the aging time multiplier as 6. Switch(config)#lldp msgTxHold 6	

5.5.7 lldp neighbors max-num

Command	**lldp neighbors max-num <***value***>** **no lldp neighbors max-num**
parameter	*value* is the configured number of entries, ranging from 5 to 500.
default	The maximum number of entries can be stored in Remote MIB is 100.
Mode	Port Configuration Mode.
Usage Guide	The maximum number of entries can be stored in Remote MIB.
Example	Set the Remote as 200 on port ethernet 1/0/5 of the switch. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)# lldp neighbors max-num 200

5.5.8 lldp notification interval

Command	**lldp notification interval <***seconds***>** **no lldp notification interval**
parameter	*seconds* is the time interval, ranging from 5 to 3600 seconds.
default	The time interval is 5 seconds.
Mode	Global Mode.
Usage Guide	After configuring the notification time interval, a "trap" message will be sent at the end of this time interval whenever the Remote Table changes.
Example	Set the time interval of sending Trap messages as 20 seconds. Switch(config)#lldp notification interval 20

5.5.9 lldp tooManyNeighbors

Command	**lldp tooManyNeighbors {discard | delete}**	
parameter	**discard**	discard the current message.
	delete	Delete the message with the least TTL in the Remoter Table
default	Discard	
Mode	Port Configuration Mode	
Usage Guide	When the Remote MIB is full, Discard means to discard the received message; Delete means to the message with the least TTL in the Remoter Table.	
Example	Set port ethernet 1/0/5 of the switch as delete. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp tooManyNeighbors delete	

5.5.10 lldp transmit delay

Command	**lldp transmit delay <*seconds*>** **no lldp transmit delay**	
parameter	*seconds*	is the time interval, ranging from 1 to 8192 seconds.
default	The interval is 2 seconds by default.	
Mode	Global Mode	
Usage Guide	When the messages are being sent continuously, a sending delay is set to prevent the Remote information from being updated repeatedly due to sending messages simultaneously.	
Example	Set the delay of sending messages as 3 seconds. Switch(config)#lldp transmit delay 3	

5.5.11 lldp transmit optional tlv

Command	**lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]** **no lldp transmit optional tlv**
parameter	**portDesc** the description of the port **sysName** the system name **sysDesc** The description of the system **sysCap** the capability of the system
default	The messages carry no optional TLV by default
Mode	Port Configuration Mode
Usage Guide	When configuring the optional TLV, each TLV can only appear once in a message, portDesc optional TLV represents the name of local port; sysName optional TLV represents the name of local system; sysDesc optional TLV represents the description of local system; sysCap optional TLV represents the capability of local system.
Example	Configure that port ethernet 1/0/5 of the switch carries portDesc and sysCap TLV. Switch(config)#in ethernet 1/0/5 Switch(Config-If-Ethernet1/0/5)# lldp transmit optional tlv portDesc sysCap

5.5.12 lldp trap

Command	**lldp trap <enable | disable>**
parameter	-
default	The Trap function is disabled on the specified port by default
Mode	Port Configuration Mode
Usage Guide	The function of sending Trap messages is enabled on the port.
Example	Enable the Trap function on port ethernet 1/0/5 of the switch. Switch(config)#in ethernet1/0/5 Switch(Config-If-Ethernet1/0/5)#lldp trap enable

5.5.13 lldp tx-interval

Command	**lldp tx-interval <*integer*>** **no lldp tx-interval**	
parameter	*integer*	is the interval of sending updating messages, ranging from 5 to 32768 seconds.
default	30s	
Mode	Global Mode	
Usage Guide	After configuring the interval of sending messages, LLDP messages can only be received after a period as long as configured. The interval should be less than or equal with half of aging time, for a too long interval will cause the state of being aged and reconstruction happen too often; while a too short interval will increase the flow of the network and decrease the bandwidth of the port. The value of the aging time of messages is the product of the multiplier and the interval of sending messages. The maximum aging time is 65535 seconds. When tx-interval is the default value and transmit delay is configured via some commands, tx-interval will become four times of the latter, instead of the default 40.	
Example	Set the interval of sending messages as 40 seconds. Switch(config)#lldp tx-interval 40	

5.5.14 show debugging lldp

Command	**show debugging lldp**
parameter	-
default	-
Mode	Admin and Configuration Mode
Usage Guide	With show debugging lldp, all ports with lldp debug enabled will be displayed.
Example	Display all ports with lldp debug enabled.

```
Switch(config)#show debugging lldp

====BEGINNING OF   LLDP DEBUG SETTINGS====

debug lldp packets interface Ethernet1/0/1
=============END OF DEBUG SETTINGS===============
```

5.5.15 show lldp

Command	**show lldp**
parameter	-
default	Do not display the configuration information of global LLDP.
Mode	Admin Mode, Global Mode.
Usage Guide	Users can check all the configuration information of global LLDP by using "show lldp".
Example	Check the configuration information of global LLDP after it is enabled on the switch.

```
Switch(config)#show lldp

-----LLDP GLOBAL INFORMATIONS-----
LLDP has been enabled globally.
LLDP enabled port : Ethernet1/0/1 Ethernet1/0/7
LLDP interval :30
LLDP txTTL :120
LLDP NotificationInterval :5
LLDP txDelay :2
LLDP-MED FastStart Repeat Count :4
-------------END-----------------
```

5.5.16 show lldp interface Ethernet

Command

show lldp interface ethernet <*IFNAME*>

parameter

IFNAME	Interface name

default

Do not display the configuration information of LLDP on the port.

Mode

Admin Mode, Global Mode.

Usage Guide

Users can check the configuration information of LLDP on the port by using “show lldp interface ethernet XXX”.

Example

Check the configuration information of LLDP on the port after LLDP is enabled on the switch.

```
Switch (config-if-ethernet1/0/1)#show lldp int e 1/0/1

  Port name :Ethernet1/0/1
  LLDP Agent Adminstatus : Both
  LLDP Operation TLV : default

  LLDP Management Address TLV status : unenable

  LLDP Trap Status : disable
  LLDP maxRemote :100
  LLDP Overflow handle : discard
  LLDP interface remote status : Free

  lldp dot3 TLV:

  MED Optional TLV : default
  MED Trap Status:Disable
  MED TLV Transmit Status:Disable
  MED Fast Transmit Status:Disable
************************************************************
```

5.5.17 show lldp neighbors interface Ethernet

Command

show lldp neighbors interface ethernet < *IFNAME* **>**

parameter

IFNAME	Interface name

default

Do not display the LLDP neighbor information of the port.

Mode

Admin Mode, Global Mode.

Usage Guide

Users can check the configuration information of LLDP on the port by using "show lldp interface ethernet XXX".

Example

Check the LLDP neighbor information of the port after LLDP is enabled on the port.

```
Switch (config-if-ethernet1/0/1)#show lld nei int e 1/0/1

Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :92
ChassisIdSubtype :4
ChassisId :00-e0-4c-00-00-00
PortIdSubtype :Local
PortId :gi1

Lldp Port Pvid TLV :
Lldp port Pvid                              : 1

*********************************************************
```

5.5.18 show lldp traffic

Command

show lldp traffic

parameter

-

default

Do not display the statistics of LLDP data packets.

Mode

Admin Mode, Global Mode.

Usage Guide

Users can check the statistics of LLDP data packets by using “show lldp traffic”.

Example

Check the statistics of LLDP data packets after LLDP is enabled on the switch.

```
Switch(config)#show lldp traffic
    PortName          Ageouts    FramesDiscarded    FramesInErrors
FramesIn    FramesOut    TLVsDiscarded    TLVsUnrecognized
------------------    -------    ---------------    --------------    --------    ---------
-------------    ----------------
   Ethernet1/0/1         0                0                 0           43
42                  0                    0
   Ethernet1/0/7         0                0                 0            0
42                  0                    0
```

5.6 Port Channel

5.6.1 interface port-channel

Command	**interface port-channel <***port-channel-number***>**	
parameter	*port-channel-number*	Port Channel Number
default	-	
Mode	Global Mode	
Usage Guide	Enable port channel configuration mode	
Example	Entering configuration mode for port-channel 1. Switch(config)#interface port-channel 1 Switch(Config-If-Port-Channel1)#	

5.6.2 lacp port-priority

Command	**lacp port-priority <***port-priority***>** **no lacp port-priority**	
parameter	*port-priority*	the port priority of LACP protocol, the range from 0 to 65535.
default	The default priority is 32768 by system.	
Mode	Port Mode.	
Usage Guide	Use this command to modify the port priority of LACP protocol, the no command restores the default value.	
Example	Set the port priority of LACP protocol. Switch(Config-If-Ethernet1/0/1)# lacp port-priority 30000	

5.6.3 lacp system-priority

Command	**lacp system-priority <*system-priority*>** **no lacp system-priority**	
parameter	*system-priority*	The system priority of LACP protocol, ranging from 0 to 65535.
default	The default priority is 32768.	
Mode	Global Mode	
Usage Guide	Use this command to modify the system priority of LACP protocol, the no command restores the default value.	
Example	Set the system priority of LACP protocol. Switch(config)#lacp system-priority 30000	

5.6.4 lacp timeout

Command	**lacp timeout {short | long}** **no lacp timeout**
parameter	-
default	Long
Mode	Port Mode
Usage Guide	Set the timeout mode of LACP protocol.
Example	Set the timeout mode as short in LACP protocol. Switch(Config-If-Ethernet1/0/1)#lacp timeout short

5.6.5 load-balance

Command

load-balance {src-mac | dst-mac | dst-src-mac | src-ip | dst-ip | dst-src-ip | ingress-port | dst-src-mac-ip}

no load-balance

parameter

src-mac	performs load-balance according to the source MAC
dst-mac	performs load-balance according to the destination MAC
dst-src-mac	performs load-balance according to the source and destination MAC
src-ip	performs load-balance according to the source IP
dst-ip	performs load-balance according to the destination IP
dst-src-ip	performs load-balance according to the destination and source IP
ingress-port	performs load-balance according to the destination and source mac and destination, source IP
dst-src-mac-ip	performs load-balance according to the port of receive flow.

default

Perform load-balance according to the source MAC.

Mode

Global mode.

Usage Guide

Use port-channel to implement load-balance, user can configure the load-balance mode according to the requirements. If the specific load-balance mode of the command line is different with the current load-balance mode of port-group, then modify the load-balance of port-group as the specific load-balance of command line; otherwise return a message to notice that the current mode is already configured.

Example

Set load-balance mode of port-group.

```
Switch(config)# load-balance src-mac
```

5.6.6 port-group

Command	**port-group <***port-group-number***>** **no port-group <***port-group-number***>**	
parameter	*port-group-number*	is the group number of a port channel from 1～128.
default	There is no port-group	
Mode	Global Mode	
Usage Guide	it can create 16 port group at most	
Example	Creating a port group. Switch(config)# port-group 1 Delete a port group. Switch(config)#no port-group 1	

5.6.7 port-group mode

Command	**port-group <***port-group-number***> mode {active | passive | on}** **no port-group**	
parameter	*port-group-number*	is the group number of port channel, from 1～128
	active	enables LACP on the port and sets it in Active mode
	passive	enables LACP on the port and sets it in Passive mode
	on	forces the port to join a port channel without enabling LACP.
default	Switch ports do not belong to a port channel by default; LACP not enabled by default.	
Mode	Port Mode	
Usage Guide	Add a physical port to the port channel NO remove the specified port from the port channel	
Example	Under the Port Mode of Ethernet1/0/1, add current port to "port-group 1" in "active" mode. Switch(Config-If-Ethernet1/0/1)#port-group 1 mode active	

5.6.8 show port-group

Command

show port-group [<*port-group-number*>] {brief | detail |}

parameter

port-group-number	is the group number of port channel to be displayed, from 1～128

default

-

Mode

All Configuration Mode

Usage Guide

If the user does not input port-group-number, that means the information of all the existent port-group are showed; if the port channel corresponds to port-group-number parameter and is not exist, then print a error message, otherwise display the current port-channel information of the specified group number.

Example

Display summary information for port-group 1

```
Switch#show port-group brief
ID: port group number;    Mode: port group mode such as on active or passive;
Ports: different types of port number of a port group,
        the first is selected ports number, the second is standby ports number, and
        the third is unselected ports number.

ID    Mode       Partner ID                    Ports        Load-balance
----------------------------------------------------------------------
1     active   0x0000,00-00-00-00-00-00    0,0,1         src-mac
```

5.7 MTU

5.7.1 Mtu

Command	**mtu [<*mtu-value*>]** **no mtu**	
parameter	*mtu-value*	the MTU value of frames that can be received, in byte, ranging from <1500-12270>. The corresponding frame size is <1518/1522-12288/12292>. Without setting is parameter, the allowed max frame size is 12288/12292.
default	MTU function not enabled by default	
Mode	Global Mode	
Usage Guide	Set switch of both ends mtu necessarily, or mtu frame will be dropped at the switch has not be set	
Example	Enable the mtu function of the switch. Switch(config)#mtu	

5.8 EFM OAM

5.8.1 clear ethernet-oam

Command	**clear ethernet-oam [interface {ethernet |} <*IFNAME*>]**	
parameter	*IFNAME*	the name of the port needs to clear OAM statistic information
default	N/A	
Mode	Admin mode	
Usage Guide	N/A	
Example	Clear the statistic information of OAM packets and link event on all ports. Switch(config)#clear ethernet-oam	

5.8.2 ethernet-oam

Command	**ethernet-oam** **no ethernet-oam**
parameter	-
default	Disable
Mode	Port mode
Usage Guide	N/A
Example	Enable ethernet-oam of Ethernet 1/0/4 Switch(config)#interface ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam

5.8.3 ethernet-oam errored-frame threshold high

Command	**ethernet-oam errored-frame threshold high {<*high-frames*> | none}** **no ethernet-oam errored-frame threshold high**	
parameter	*high-frames*	the high detection threshold of errored frame event, ranging from 2 to 4294967295.
	none	cancel the high threshold configuration.
default	**none**	
Mode	Port mode	
Usage Guide	During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold	
Example	Configure the high threshold of errored frame event on Ethernet 1/0/4 to be 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold high 3000	

5.8.4 ethernet-oam errored-frame threshold low

Command	**ethernet-oam errored-frame threshold low <*low-frames*>** **no ethernet-oam errored-frame threshold low**	
parameter	*low-frames*	the low detection threshold of errored frame event, ranging from 1 to 4294967295
default	1	
Mode	Port mode	
Usage Guide	During the specific detection period, errored frame event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold can not be larger than the high threshold.	
Example	Configure the low threshold of errored frame event on Ethernet 1/0/4 to 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame threshold low 100	

5.8.5 ethernet-oam errored-frame window

Command	**ethernet-oam errored-frame window <***seconds***>** **no ethernet-oam errored-frame window**	
parameter	*seconds*	is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms
default	5	
Mode	Port mode	
Usage Guide	Detect the errored frame number of the port after the time of specific detection period. If the number of errored frame is larger than or equal to the threshold, bring the corresponding event and notify the peer through OAMPDU.	
Example	Configure the detection period of errored frame event on port1/0/4 to be 20s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame window 100	

5.8.6 ethernet-oam errored-frame-seconds threshold high

Command	**ethernet-oam errored-frame-seconds threshold high {<***high-seconds***> | none}** **no ethernet-oam errored-frame-seconds threshold high**	
parameter	*high-seconds*	the high detection threshold of errored frame period event,ranging from 2 to 4294967295.
	none	cancel the high threshold configuration.
default	**none**	
Mode	Port mode	
Usage Guide	During the specific detection period, serious link event is induced if the number of errored frame is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold can not be less than the low threshold.	
Example	Configure the high threshold of errored frame period event on port 1/0/4 to be 3000. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold high 3000	

5.8.7 ethernet-oam errored-frame-seconds threshold Low

Command	**ethernet-oam errored-frame-seconds threshold low <*low-seconds*>** **no ethernet-oam errored-frame-seconds threshold low**	
parameter	*low-seconds*	the low detection threshold of errored frame seconds event, ranging from 1 to 65535 seconds.
default	1	
Mode	Port mode	
Usage Guide	During the specific detection period, errored frame period event is induced if the number of errored frame is larger than or equal to the low threshold and the device notifies the peer by event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.	
Example	Configure the low threshold of errored frame period event on port 1/0/4 to be 100. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds threshold low 100	

5.8.8 ethernet-oam errored-frame-seconds window

Command	**ethernet-oam errored-frame-seconds window <*seconds*>** **no ethernet-oam errored-frame-seconds window**	
parameter	*seconds*	is the time for counting the specified frame number, its range from 50 to 450, unit is 200ms.
default	300	
Mode	Port mode	
Usage Guide	Detect errored frame seconds of the port after the time of specific detection period. If the number of errored frame seconds is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.	
Example	Configure the detection period of errored frame seconds event on port 1/0/4 to be 120s. Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-frame-seconds window 600	

5.8.9 ethernet-oam errored-symbol-period threshold High

Command

ethernet-oam errored-symbol-period threshold high {<*high-symbols*> | none}

no ethernet-oam errored-symbol-period threshold high

parameter

high-symbols	the high detection threshold of errored symbol event, ranging from 2 to 18446744073709551615 symbols.
none	cancel the high threshold configuration.

default **none**

Mode Port mode

Usage Guide During the specific detection period, serious link event is induced if the number of errored symbols is larger than or equal to the high threshold and the device notifies the peer by sending Information OAMPDU of which the value of Link Fault flag in Flags field is 1. Note that the high threshold should not be less than the low threshold.

Example Set the high threshold of errored symbol event on port 1/0/4 to none.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold high
none
```

5.8.10 ethernet-oam errored-symbol-period threshold Low

Command

ethernet-oam errored-symbol-period threshold low <*low-symbols*>

no ethernet-oam errored-symbol-period threshold low

parameter

low-symbols	the low threshold of errored symbol event, ranging from 1 to 18446744073709551615 symbols.

default 1

Mode Port mode

Usage Guide During the specific detection period, errored symbol event is induced if the number of errored symbols is larger than or equal to the low threshold and the device notifies the peer by sending event notification OAMPDU. Note that the low threshold should not be larger than the high threshold.

Example Set the low threshold of errored symbol event on port 1/0/4 to be 5.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period threshold low 5
```

5.8.11 ethernet-oam errored-symbol-period window

Command

ethernet-oam errored-symbol-period window <*seconds***>**
no ethernet-oam errored-symbol-period window

parameter

seconds	is the time for counting the specified frame number, its range from 5 to 300, unit is 200ms.

default 5

Mode Port mode

Usage Guide

Detect errored symbols of the port after the time of specific detection period. If the number of errored symbols is larger than or equal to the threshold, corresponding event is induced and the device notified the peer through OAMPDU.

Example

Set the detection period of errored symbol event on port 1/0/4 to be 2s.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam errored-symbol-period window 10
```

5.8.12 ethernet-oam link-monitor

Command

ethernet-oam link-monitor
no ethernet-oam link-monitor

parameter -

default Enable

Mode Port mode

Usage Guide

Enable OAM to monitor local link errors. Generally link monitor is enabled when enabling OAM function of the port. When OAM link monitor is disabled, although local link error is not monitored, Event information OAMPDU from the peer is still normally received and processed.

Example

Enable the link monitor of port 1/0/4.

```
Switch(Config-If-Ethernet1/0/4)#ethernet-oam link-monitor
```

5.8.13 ethernet-oam mode

Command	**ethernet-oam mode {active | passive}** **no ethernet-oam mode**	
parameter	**active**	active mode
	passive	passive mode
default	active mode	
Mode	Port mode	
Usage Guide	At least one of the two connected OAM entities should be configured to active mode. Once OAM is enabled, the working mode of OAM cannot be changed and you need to disable OAM function if you have to change the working mode.	
Example	Set the mode of OAM function on ethernet 1/0/4 to passive mode. Switch(Config-If-Ethernet1/0/4)#ethernet-oam mode passive	

5.8.14 ethernet-oam period

Command	**ethernet-oam period <***seconds***>** **no ethernet-oam mode**	
parameter	*seconds*	sending period, ranging from 1 to 2 seconds.
default	1s	
Mode	Port mode	
Usage Guide	Use this command to configure the transmission interval of Information OAMPDU which keep OAM connection normally.	
Example	Set the transmission interval of Information OAMPDU for ethernet 1/0/4 to be 2s. Switch(Config-If-Ethernet1/0/4)# ethernet-oam period 2	

5.8.15 ethernet-oam remote-failure

Command	**ethernet-oam remote-failure** **no ethernet-oam remote-failure**
parameter	-
default	Enable
Mode	Port mode
Usage Guide	With remote failure indication is enabled, if critical-event or link fault event is occurred locally, it will notify the peer by sending Information OAMPDU, log the fault information and send SNMP trap warning. When the remote failure indication is disabled, although local critical-event or link fault event is not monitored, failure indication information from the peer is still normally received and processed.
Example	Enable remote failure indication of ethernet 1/0/4. Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-failure

5.8.16 ethernet-oam remote-loopback

Command	**ethernet-oam remote-loopback** **no ethernet-oam remote-loopback**
parameter	-
default	Disable
Mode	port mode
Usage Guide	Only OAM can send remote loopback reques in auto mode, the OAM work in passive mode can not send remote loopback; when remote OAM working in loopback mode, all packets except OAM PDU packets will back local port according to the same route (Notice: during OAM loopback, it can not communicate), administrator can check the link delay of loopback, shake and throughput capacity. It can do loopback configuration after create OAM link, if OAM link is broken during loopback, the loopback will be cancel automatically. The command mutex with ethernet-oam remote-loopback supported.
Example	Enable the remote OAM of port 1/0/4 to remote loopback mode. Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback Normal forwarding will be suspended during the remote-loopback, are you sure to start remote-loopback? [Y/N]

5.8.17 ethernet-oam remote-loopback supported

Command	**ethernet-oam remote-loopback supported** **no ethernet-oam remote-loopback supported**
parameter	-
default	Disable
Mode	Port mode.
Usage Guide	The port that only enable loopback support function can receive OAM loopback reques and in loopback mode. So when enable remote and in OAM loopback, please ensure remote configured loopback support. The command mutex with ethernet-oam remote-loopback.
Example	Enable OAM loopback support function of ethernet 1/0/4 Switch(Config-If-Ethernet1/0/4)#ethernet-oam remote-loopback supported

5.8.18 ethernet-oam timeout

Command	**ethernet-oam timeout <***seconds***>** **no ethernet-oam timeout**
parameter	*seconds* — the timeout ranging from 5 to 10 seconds.
default	5s
Mode	Port mode
Usage Guide	OAM connection will be disconnected if no OAMPDU is received after specified timeout.
Example	Set the timeout of OAM connection for ethernet 1/0/4 to be 6 seconds. Switch(Config-If-Ethernet1/0/4)#ethernet-oam timeout 6

5.8.19 show ethernet-oam

Command

show ethernet-oam [{local | remote} interface {ethernet |} <*IFNAME*>]

parameter

IFNAME	the port that OAM connection information will be shown

default

N/A.

Mode

Admin mode

Usage Guide

N/A.

Example

Show overview information of Ethernet OAM connection.
Switch#show ethernet-oam

```
Switch#show ethernet-oam
Capability codes: L - Link Monitor,    R - Remote Loopback
                  U - Unidirection,    V - Variable Retrieval
-------------------------------------------------------------------------------------
Interface Local-Mode Local-Capability Remote-MAC-Addr      Remote-Mode
Remote-Capability
1/0/1        active        L
```

5.8.20 show ethernet-oam events

Command

show ethernet-oam events {local | remote} [interface {ethernet |} <*IFNAME*>]

parameter

IFNAME	the port that the statistic information of OAM link events needs to be shown

default

N/A.

Mode

Admin mode

Usage Guide N/A.

Example Show the statistic information of link events on Ethernet 1/0/1.

```
Switch#show ethernet-oam events local interface 1/0/1

ethernet1/0/1 link-events：
OAM_local_errored-symbol-period-events:
----------------------------------------------------------------------------------------------------
event time stamp：3539 errored symbol window(200ms)：5
errored symbol low threshold：1 errored symbol high threshold：none
errored symbol：1200120 errored running total：2302512542
event running total：232
OAM_local_errored-frame-period-events:
----------------------------------------------------------------------------------------------------
event time stamp：3539 errored frame window(200ms)：50
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：52
OAM_local_errored-frame-events:
----------------------------------------------------------------------------------------------------
event time stamp：3539 errored frame window(200ms)：5
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：75
OAM_local_errored-frame-seconds-summary-events:
----------------------------------------------------------------------------------------------------
event time stamp：3520 errored frame seconds summary window(200ms)：300
errored frame low threshold：1 errored frame high threshold：none
errored frame：1200120 errored running total：2302512542
event running total：232
OAM_local_link-fault：0
OAM_local_dying gasp：0
OAM_local_critical event：0
```

5.8.21 show ethernet-oam link-events-configuration

Command	**show ethernet-oam link-events-configuration [interface {ethernet | } <*IFNAME*>]**	
parameter	*IFNAME*	the port that the statistic information of OAM link events needs to be shown
default	N/A.	
Mode	Admin mode	
Usage Guide	N/A.	

Example

Show configuration of link events on ethernet 1/0/1.

```
Switch#show ethernet-oam link-events-configuration interface ethernet 1/0/1
Ethernet1/0/1 link-monitor configuration：
event high-threshold low-threshold window(200ms)
-----------------------------------------------------------------------------------------------
Err-symbol-Period none 1 2
Err-frame-Period none 1 10
Err-frame none 2 5
Err-frame-second-summary none 2 600
-----------------------------------------------------------------------------------------------
```

5.8.22 show ethernet-oam loopback status

Command	**show ethernet-oam loopback status [interface {ethernet | } <*IFNAME*>]**	
parameter	*IFNAME*	means display the port of OAM loopback statusinformation
default	-	
Mode	Admin mode	
Usage Guide	Displays the loopback status OAM all or specified ports of the switch	

Example

Display the OAM loopback status of all port.

```
Switch(config)#show ethernet-oam loopback status
OAM Loopback Status:
Ethernet1/0/1: disable
Ethernet1/0/2: disable
Ethernet1/0/3: disable
```

5.9 PORT SECURITY

5.9.1 clear port-security

Command **clear port-security {all | configured | dynamic | sticky} [[address <*mac-addr*> | interface <*interface-id*>] [vlan <*vlan-id*>]]**

parameter

all	All secure MAC entries on the interfaces
configured	The configured secure MAC
dynamic	The dynamic secure MAC learnt by the interface
sticky	The secure MAC of sticky
mac-addr	The specified secure MAC address
interface-id	The secure MAC entries of the specified interface
vlan-id	The specified VLAN

default -

Mode Admin mode

Usage Guide Clear secure MACs on the interface

Example Clear all secure MACs on the interface

```
Switch#clear port-security all
```

5.9.2 show port-security

Command **show port-security [interface <***interface-id***>] [address | vlan]**

parameter

interface-id	Show port-security configuration of the interface
address	Show the secure address of the interface
vlan	Show the maximum number of each VLAN configured on trunk/hybrid interface.

default -

Mode Any modes

Usage Guide Display port security configuration.

Example Show all secure MACs on the interfaces.

```
Switch# show port-security address interface ethernet 1/0/1
```

5.9.3 switchport port-security

Command	**switchport port-security** **no switchport port-security**
parameter	-
default	Disable
Mode	Port mode
Usage Guide	Configure port security for the interface no disable port security with commands
Example	Enable port-security on the interface. Switch(config-if- ethernet1/0/1)#switchport port-security

5.9.4 switchport port-security mac-address

Command	**switchport port-security mac-address <***mac-address***> [vlan <***vlan-id***>]** **no switchport port-security mac-address <***mac-address***> [vlan <***vlan-id***>]**	
parameter	*mac-address*	Configure the specified MAC address as the static secure MAC.
	vlan-id	The specified VLAN of the MAC address, it only takes effect on trunk and hybrid interfaces.
default	No secure MAC is bound by the interface.	
Mode	Port mode	
Usage Guide	When configuring the static secure MAC, pay attention to the number of the current secure MAC whether exceed the maximum MAC limit allowed by the interface. If exceeding the maximum MAC limit, it will result in violation operation.	
Example	Configure the secure MAC address on the interface Switch (config-if- ethernet1/0/1)# switchport port-security mac-address 00-00-00-00-00-01	

5.9.5 switchport port-security maximum

Command	**switchport port-security maximum <**_value_**> [vlan <**_vlan-list_**>]** **no switchport port-security maximum <**_value_**> [vlan <**_vlan-list_**>]**	
parameter	_value_	Configure the maximum number of the secure MAC allowed by the interface, its range between 1 and 128. It is determined by the maximum MAC number of the device
	vlan-list	Configure the maximum value for the specified VLAN, it only takes effect on trunk and hybrid interfaces.
default	After enabling port-security, if there is no other configuration, the maximum number of the secure MAC is 1 on the interface. The interface number in VLAN is no limit by default	
Mode	Port mode	
Usage Guide	Pay attention to the coupling relation about the number between the interface and VLAN, set the maximum number configured by the interface as the standard firstly.	
Example	Configure the maximum number of the secure MAC on the interface. Switch(config-if- ethernet1/0/1)# switchport port-security maximum 100	

5.9.6 switchport port-security violation

Command	**switchport port-security violation {protect | recovery | restrict | shutdown}** **no switchport port-security violation**	
parameter	**protect**	Protect mode, it will trigger the action that do not learn the new MAC, drop the package and do not send the warning
	recovery	After triggering the violation action of the port, the mac learning function can be recovered
	restrict	Restrict mode, it will trigger the action that do not learn the new MAC, drop the package, send snmp trap and record the configuration in syslog.
	shutdown	Shutdown mode is the default mode. Under this condition, the interface is disabled directly, send snmp trap and record the configuration in syslog.
default	**shutdown**	
Mode	Port mode	
Usage Guide	When exceeding the maximum number of the configured MAC addresses, MAC address accessing the interface does not belongs to this interface in MAC address table or a MAC address is configured to several interfaces in same VLAN, both of them will violate the security of the MAC address.	
Example	Configure violation mode as protect for the interface. Switch(config-if-ethernet1/0/1)#switchport port-security violation protect	

5.10 DDM

5.10.1 clear transceiver threshold-violation

Command	**clear transceiver threshold-violation [interface ethernet <interface-list>]**	
parameter	**interface-list**	The interface list that the threshold violation of the transceiver monitoring needs to be cleared.
default	-	
Mode	Admin mode	
Usage Guide	Clear threshold violations monitored by transceivers	
Example	Clear he threshold violation of the transceiver monitoring on port 21, 25, 26, 28. Switch#clear transceiver threshold-violation interface ethernet 1/0/21;25-26;28	

5.10.2 show transceiver

Command	**show transceiver [interface ethernet <interface-list>] [detail]**	
parameter	**interface-list**	The interface list that the monitoring of the transceiver needs to be shown.
	detail	Show the detailed monitoring of the transceiver.
default	-	
Mode	User mode, admin mode and global mode	
Usage Guide	Displays the transceiver's detailed monitoring information.	
Example	Show the brief DDM information of all ports.	

```
Switch#show transceiver
Interface   Temp（℃）  Voltage（V）  Bias（mA）  RX Power（dBM）  TX Power（dBM）

1/0/25      33          3.31            6.11        -30.54(A-)        -6.01
1/0/26      33          5.00（W+）      6.11        -20.54(W-)         -6.02
```

5.10.3 show transceiver threshold-violation

Command

show transceiver threshold-violation [interface ethernet <interface-list>]

parameter

interface-list	The interface list that the transceiver monitoring needs to be shown.

default

-

Mode

Admin mode and global mode

Usage Guide

Show the transceiver monitoring

Example

Show the transceiver monitoring

Switch(config)#show transceiver threshold-violation interface ethernet 1/0/25-26

```
Ethernet 1/0/25 transceiver threshold-violation information：
Transceiver monitor is enabled. Monitor interval is set to 30 minutes.
The current time is Jan 02 12:30:50 2010.
The last threshold-violation time is Jan 01 1:30:50 2010.
Brief alarm information:
RX loss of signal
RX power low
Detail diagnostic and threshold information:
                        Diagnostic Threshold
                     Realtime Value High Alarm Low Alarm High Warn Low Warn
                     -----------------   -----------    -----------   ------------   ---------
Temperature（℃）  33              70          0            70             0

Voltage（V）         7.31            10.00        0.00          5.00         0.00
Bias current（mA）  3.11             10.30        0.00          5.00         0.00
RX Power（dBM）  -30.54(A-)       9.00         -25.00（-34）9.00        -25.00
TX Power（dBM）  -1.01             9.00          -12.05        9.00         -10.00
Ethernet 1/0/26 transceiver threshold-violation information:
Transceiver monitor is disabled. Monitor interval is set to 30 minutes.
The last threshold-violation doesn't exist.
```

5.10.4 transceiver-monitoring

Command	**transceiver-monitoring {enable | disable}**
parameter	-
default	Disable
Mode	Port mode
Usage Guide	Enable/disable transceiver monitoring
Example	Enable the transceiver monitoring of ethernet1/0/1. Switch(config-if-ethernet1/0/1)#transceiver-monitoring enable

5.10.5 transceiver-monitoring interval

Command	**transceiver-monitoring interval <minutes>** **no transceiver-monitoring interval**
parameter	**minutes** The interval of the transceiver monitoring needs to be set.
default	15 minutes
Mode	Global mode
Usage Guide	sets the interval for transceiver monitoring. No command sets the interval to the default interval of 15 minutes.
Example	Set the interval of the transceiver monitoring as 1 minute. Switch(config)#transceiver-monitoring interval 1

5.10.6 transceiver threshold

Command	**transceiver threshold {default | {temperature | voltage | bias | rx-power | tx-power} {high-alarm | low-alarm | high-warn | low-warn} {<value> | default}}**	
parameter	**default**	Restore the threshold as the default threshold set by the manufacturer. If the monitoring index is not specified, restore all thresholds, if the monitoring index is specified, restore the corresponding threshold only.
	temperature	The monitoring index—temperature
	voltage	The monitoring index—voltage
	bias	The monitoring index—bias current
	rx-power	The monitoring index—receiving power
	tx-power	The monitoring index—sending power
	high-alarm	High-alarm of the monitoring index, namely there is alarm with A+ if exceeding the threshold.
	low-alarm	Low-alarm of the monitoring index, namely there is alarm with Aif exceeding the threshold.
	high-warn	High-warn of the monitoring index, namely there is warning with W+ if exceeding the threshold.
	low-warn	Low-warn of the monitoring index, namely there is warning with W- if exceeding the threshold.
default	The threshold is set by the manufacturer	
Mode	Port mode	
Usage Guide	The range of the threshold parameters is shown for each monitoring index in the following： Temperature: -128.00~128.00 ℃ Voltage: 0.00~7.00 V Bias current: 0.00~140.00 mA x-power: -50.00~9.00 dBM tx-power: -50.00~9.00 dBM The maximum length of the threshold parameter configured by the user is 20 bits. After the user configured a parameter threshold, the threshold set by the manufacturer will be labeled with the bracket when showing the threshold, and decide whether give an alarm according to the user's configuration.	
Example	Configure tx-power threshold of the fiber module, the low-warn threshold is configured as -12 on ethernet1/0/1. Switch(config-if-ethernet1/0/1)#transceiver threshold tx-power low-warn -12	

5.11 LLDP-MED

5.11.1 civic location

Command	**civic location {dhcp server | switch | endpointDev} <***country-code***>** **no civic location**	
parameter	**dhcp server**	Set device type to be DHCP server
	switch	Set device type to be Switch
	endpointDev	Set device type to be LLDP-MED Endpoint
	country-code	Set country code which consist of 2 letters, such as DE or US, it should accord the country code of ISO 3166 standard.
default	No location with Civic Address LCI format is configured on the port.	
Mode	Port mode	
Usage Guide	Configure device type and country code of the location with Civic Address LCI format and enter Civic Address LCI address mode to configure the more detailed location.	
Example	Configure device type as switch and country code as US for the location with Civic Address LCI format on Ethernet 19. Switch(Config-If-Ethernet1/0/19)# civic location switch US Switch(Med-Civic)#	

5.11.2 description-language

Command

{description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo} <*address*>

no {description-language | province-state | city | county | street | locationNum | location | floor | room | postal | otherInfo}

parameter

description-language	language for describing location, such as 'English'
province-state	state, canton, region, province prefecture, and so on, such as 'clara'
city	city, such as 'New York'
county	county, parish, such as 'santa clara'
street	street, such as '1301 Shoreway Road'
locationNum	house number, such as '9'
location	name and occupant of a location, such as 'Carrillo's Holiday Market'
floor	floor number, such as '13'
room	room number, such as '1308'
postal	postal/zip code, such as '10027-1234'
otherInfo	Additional location information, such as 'South Wing'
address	detailed address information, it cannot exceed 250 characters

default

No detailed information of the location with Civic Address LCI is configured on the port.

Mode

Civic Address LCI address mode

Usage Guide

With this command, configure the detailed information of the location with Civic Address LCI on the port, it is able to configure 10 kinds of address types at most.

Example

Configure the detailed location information in Civic Address LCI address mode.

```
Switch(Med-Civic)# city Beijing
Switch(Med-Civic)# street shangdi
```

5.11.3 ecs location

Command	**ecs location <***tel-number***>** **no ecs location**	
parameter	*tel-number*	location characters with ECS ELIN format, such as emergent telephone number, it is character string with the length between 10 and 25.
default	No location with ECS ELIN format is configured.	
Mode	Port mode	
Usage Guide	Length range of the location character string between 10 and 25 with ECS ELIN format.	
Example	Configure the location of ECS ELIN format on port 19. Switch(Config-If-Ethernet1/0/19)# ecs location 880-445-3381	

5.11.4 lldp med fast count

Command	**lldp med fast count <***value***>** **no lldp med fast count**	
parameter	*value*	The number of sending the packets fast, its range from 1 to 10, unit is entries.
default	4	
Mode	Global mode	
Usage Guide	With this command, set the number for sending the packets fast.	
Example	Set the number of quick packages to 5 Switch(config)#lldp med fast count 5	

5.11.5 lldp med trap

Command	**lldp med trap {enable | disable}**
parameter	-
default	Disable
Mode	Port mode
Usage Guide	Enable or disable LLDP-MED TRAP of the port.
Example	Enable LLDP-MED TRAP of the port 19. Switch(Config-If-Ethernet1/0/19)# lldp med trap enable

5.11.6 lldp transmit med tlv all

Command	**lldp transmit med tlv all** **no lldp transmit med tlv all**
parameter	-
default	Port does not enable the function for Sending LLDP-MED TLV.
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED TLV supported by all switches. However, LLDP packets sent by the port without any LLDP-MED TLV after the switch configured the corresponding no command.
Example	Port 19 enables the function for sending LLDP-MED TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv all

5.11.7 lldp transmit med tlv capability

Command	**lldp transmit med tlv capability** **no lldp transmit med tlv capability**
parameter	-
default	The function is disabled for sending LLDP-MED Capability TLV.
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, the sent LLDP packets with LLDP-MED Capability TLV. However, LLDP packets sent by the port without LLDP-MED Capability TLV after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV is the important LLDP-MED TLV, if do not configure the port to send LLDP-MED Capability TLV firstly, other LLDP-MED TLV will not be sent.
Example	Port 19 enables the function for sending LLDP-MED Capability TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv capability

5.11.8 lldp transmit med tlv extendPoe

Command	**lldp transmit med tlv extendPoe** **no lldp transmit med tlv extendPoe**
parameter	-
default	The function is disabled for sending LLDP-MED Extended Power-Via-MDI TLV.
Mode	Port mode
Usage Guide	Configure specified port to send LLDP-MED extended power supply - Via-MDITLV. No command disables the function.
Example	Port 19 enables the function for sending LLDP-MED Extended Power-Via-MDI TLV. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv extendPoe

5.11.9 lldp transmit med tlv location

Command	**lldp transmit med tlv location** **no lldp transmit med tlv location**
parameter	-
default	Disable
Mode	Port Mode
Usage Guide	Configure the specified port to send LLDP-MED Location Identification TLV. After configured this command, if the port has the capability of sending LLDP-MED TLV, the LLDP packets sent from the port will include LLDP-MED Location Identification TLV. Otherwise, the LLDP packets sent from the port will not include LLDP-MED Location Identification TLV by the no command even if the port has the capability of sending LLDP-MED TLV. Notice: Before configuring this function, the capability of sending LLDP-MED Capability TLV must be configured. If the device does not support POE or the POE function of the port is disabled by the command, this TLV will not be sent.
Example	Enable the port 19 to send LLDP-MED Location Identification TLV. Switch(Config-If-Ethernet1/0/19)#lldp transmit med tlv location

5.11.10 lldp transmit med tlv inventory

Command	**lldp transmit med tlv inventory** **no lldp transmit med tlv inventory**
parameter	-
default	The function is disabled for sending LLDP-MED Inventory Management TLVs
Mode	Port mode
Usage Guide	After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Inventory Management TLVs sent by the port. However, LLDP packets without LLDP-MED Inventory Management TLVs sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Inventory Management TLVs, or else the configuration cannot be successful.
Example	Port 19 enables the function for sending LLDP-MED Inventory Management TLVs. Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv inventory

5.11.11 lldp transmit med tlv networkPolicy

Command

lldp transmit med tlv networkPolicy
no lldp transmit med tlv networkPolicy

parameter

-

default

The function is disabled for sending LLDP-MED Network Policy TLV.

Mode

Port mode

Usage Guide

After configuring this command, if the port is able to send LLDP-MED TLV, LLDP packets with LLDP-MED Network Policy TLV sent by the port. However, LLDP packets without LLDP-MED Network Policy TLV sent by the port after the switch configured the corresponding no command. Note: LLDP-MED Capability TLV sent by the port must be configured before sending LLDP-MED Network Policy TLV, or else the configuration cannot be successful.

Example

Port 19 enables the function for sending LLDP-MED Network Policy TLV.

```
Switch(Config-If-Ethernet1/0/19)# lldp transmit med tlv networkPolicy
```

5.11.12 network policy

Command

network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} [status {enable | disable}] [tag {tagged | untagged}] [vid {<*vlan-id***> | dot1p}] [cos <*cos-value*>] [dscp <*dscp-value*>]**

no network policy {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming- video | video-signaling}

parameter

status	Whether the network policy is usable.
enable	Network Policy of the specified application type has been defined, enable is the default value of the network policy.
disable	Network Policy of the specified application type has been defined, disable is the default value of the network policy
tag	Configure the specified application to uses tagged or untagged

	VLAN method
tagged	Configure the flow of the specified application to use the tagged vlan method, here, the fields (such as VLAN ID, Layer2 priority and DSCP value) are take effect
untagged	Configure the flow without tag for the specified application, the fields (such as VLAN ID, Layer2 priority) are ignored, only DSCP value field takes effect. Untagged is the default value of VLAN method.
vid	Configure VLAN ID that the specified application belongs to
vlan-id	Configure the value of VLAN ID, its range from 1 to 4094
dot1p	Configure the specified application to tag the flow by using 802.1p priority, at the same time, use vlan 0 to load the flow.
cos	Configure the priority of Ethernet frame for VLAN
cos-value	Configure the value of Ethernet frame priority for VLAN, its range from 0 to 7, the default value is 5.
dscp	Configure DSCP of VLAN.
dscp-value	DSCP value input by the user, its range from 0 to 63, the default value is 46

default

No network policy is configured on the port.

Mode

Port mode

Usage Guide

User is able to configure the network policy of many kinds on a port, but their application types cannot repeat, and a kind of network policy corresponds to a LLDP-MED network policy TLV. If user configures multi-policy for a port, it will send multi-LLDP-MED network policy TLV to a LLDP packet. If user does not configure any network policy, no LLDP-MED network policy TLV is sent to LLDP packet.

Example

Configure the network policy with the application type of voice on port 19.

Switch(Config-If-Ethernet1/0/19)# network policy voice tag tagged vid 2 cos 6 dscp 23

5.11.13 show lldp

Command	**show lldp [interface ethernet <IFNAME>]**	
parameter	**IFNAME**	Port name
default	-	
Mode	Admin mode	
Usage Guide	Show LLDP and LLDP-MED configurations on the current port.	
Example	Show LLDP and LLDP-MED configuration of the port 19. Switch#show lldp interface ethernet 1/0/19	

```
Port name :Ethernet1/0/19
LLDP Agent Adminstatus : Both
LLDP Operation TLV : default
LLDP Trap Status : disable
LLDP maxRemote :100
LLDP Overflow handle : discard
LLDP interface remote status : Free
MED Optional TLV : capabilities networkPolicy location power inventory
MED Trap Status:Enable
MED TLV Transmit Status:Disable
MED Fast Transmit Status:Disable
```

5.11.14 show lldp neighbors

Command	**show lldp neighbors [interface ethernet <*IFNAME*>]**
parameter	***IFNAME*** Port number; for example :1/0/1
default	-
Mode	Admin mode
Usage Guide	With this command, checking LLDP and LLDP-MED information of the neighbors after the port received LLDP packets sent by the neighbors.
Example	Show the neighbor information on port 1. Switch #show lldp neighbors interface ethernet 1/0/1

```
Port name : Ethernet1/0/1
Port Remote Counter : 1
TimeMark :20
ChassisIdSubtype :4
ChassisId :00-03-0f-00-00-02
PortIdSubtype :Local
PortId :3
PortDesc :Ethernet1/0/1
SysName :switch
SysDesc :switch Device, Compiled Feb 12 17:39:53 2011
SoftWare Version 6.2.30.0
BootRom Version 4.0.1
HardWare Version
Device serial number
Copyright (C) 2001-2011 by Vendor.
All rights reserved
```

5.11.15 show lldp traffic

Command

show lldp traffic

parameter

-

default

-

Mode

Admin Mode.

Usage Guide

After the port received the LLDP packets from the neighbor, this command can be used to view the statistics of the sent and received packets of LLDP and LLDP-MED.

Example

View the statistics of the sent and received packets after the LLDP function is enabled.

```
  Switch(config)#show lldp traffic

PortName Ageouts FramesDiscarded FramesInErrors FramesIn FramesOut
TLVsDiscarded TLVsUnrecognized
----------- -------     ---------------     --------------    --------    ---------     -------------
----------------
Ethernet1/0/1 0     0                    0                     0         7              0
```

5.12 bpdu-tunnel

5.12.1 bpdu-tunnel-protocol

Command

bpdu-tunnel-protocol{stp| gvrp| dot1x| user-defined-protocol <name>}

no bpdu-tunnel-protocol {stp| gvrp| dot1x| user-defined-protocol <name>}

parameter

stp	enable bpdu-tunnel-protocol of stp function in port.
gvrp	enable bpdu-tunnel-protocol of avrp function in port.
dot1x	enable bpdu-tunnel-protocol of dot1x function in port.
name	enable bpdu-tunnel-protocol of neme function in port, the protocol name range from 1 to 32 bytes, and it made up with character, data, underline and the head and tail character can not be underline

default -

Mode Port Mode.

Usage Guide When finished configure bpdu-tunnel-protocol destination MAC address of some protocol, users can enable bpdu-tunnel-protocol function of protocol in port. Stp, gvrp or dot1x function mutex with bpdu-tunnel-protocol function in port, namely, if configured stp, gvrp or dot1x function in port, the bpdu-tunnel-protocol function of the protocol configured failed; if configured bpdu-tunnel-protocol function of this protocol in port, stp, gvrp or dot1x function can not configured in port.

Example Configure bpdu-tunnel-protocol to enable stp protocol in port 1/0/1.

```
Switch(Config-If-Ethernet1/0/1)# bpdu-tunnel-protocol stp
```

5.12.2 bpdu-tunnel-protocol group-mac

Command **bpdu-tunnel-protocol {stp| gvrp| dot1x} {group-mac <mac> | default-group-mac}**

no bpdu-tunnel-protocol {stp| gvrp| dot1x}

parameter

stp	configure bpdu-tunnel-protocol mac of stp protocol;
gvrp	configure bpdu-tunnel-protocol mac of gvrp protocol;
dot1x	configure bpdu-tunnel-protocol mac of dot1x protocol;
mac	bpdu-tunnel-protocol mac address must be multicast address and it can not be protocodl saved address, namely address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac	the default mac address is 01-00-0c-cd-00-02.

default -

Mode Global Mode.

Usage Guide This command must be configured before configure bpdu-tunnel-protocol in port.

Example Configure 01-01-00-0c -00-02 bpdu-tunnel-protocol of stp protocol.

```
Switch(Config)# bpdu-tunnel-protocol stp group-mac 01-01-00-0c -00-02
```

5.12.3 bpdu-tunnel-protocol protocol-mac

Command

bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> {group-mac <mac> | default-group-mac}

no bpdu-tunnel-protocol user-defined-protocol <name>

parameter

name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
protocol-mac <mac>	it is the mac address of protocol;
default-group-mac	The default mac address is 01-00-0c-cd-00-02

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-03 to be the bpdu-tunnel-protocol of mrpp protocol.

```
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol mrpp protocol-mac
00-03-0f-00-00-02 group-mac 01-01-00-0c -00-03
```

5.12.4 bpdu-tunnel-protocol ethernetii

Command

bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type ethernetii protocol-type <type> {group-mac <mac> | default-group-mac}

no bpdu-tunnel-protocol user-defined-protocol <name>

parameter

name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline;
protocol-mac <mac>	it is the mac address of protocol;
type	the value of protocol and the format is xx-xx
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30;
default-group-mac	The default mac address is 01-00-0c-cd-00-02.

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-04 to be the bpdu-tunnel-protocol of lldp protocol.

Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac 01-80-c2-00-00-0e encape-type ethernetii protocol-type 88-cc group-mac 01-01-00-0c -00-04

5.12.5 bpdu-tunnel-protocol snap

Command

bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type snap {oui <oui>| } protocol-type <type> {group-mac <mac> | default-group-mac}
no bpdu-tunnel-protocol user-defined-protocol <name>

parameter

name	it is the protocol name and the protocol name includes 1 to 32characters, and it makes up with character, data and underline, the head and tail character can not be underline
protocol-mac <mac>	it is the mac address of protocol
oui	the value of oui and the format is xx-xx-xx
type	the value of protocol and the format is xx-xx
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
default-group-mac	The default mac address is 01-00-0c-cd-00-02

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-05 to be the bpdu-tunnel-protocol of Apple Talk protocol.

```
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac
00-03-c2-00-00-05 encape-type snap oui 08-00-07 protocol-type 80-9b group-mac
01-01-00-0c -00-05
```

5.12.6 bpdu-tunnel-protocol llc

Command

bpdu-tunnel-protocol user-defined-protocol <name> protocol-mac <mac> encape-type llc dsap <dsap> ssap <ssap> {group-mac <mac> | default-group-mac}

no bpdu-tunnel-protocol user-defined-protocol <name>

parameter

name	it is the protocol name and the protocol name includes 1 to 32 characters, and it makes up with character, data and underline, the head and tail character can not be underline
protocol-mac <mac>	it is the mac address of protocol
dsap	The dsap value of protocol and it ranges from 0 to 255
ssap	The ssap value of protocol and it ranges from 0 to 255;
group-mac <mac>	it is the address of bpdu-tunnel-protocol mac and it must be multicast address, and it is not protocol saved address, namely the address between 01-80-c2-00-00-00 and 01-80-c2-00-00-30
default-group-mac	The default mac address is 01-00-0c-cd-00-02

default

-

Mode

Global Mode

Usage Guide

The command must be configured before bpdu-tunnel-protocol in port.

Example

Configure 01-01-00-0c-00-06 to be the bpdu-tunnel-protocol of NetBIOS protocol.

```
Switch(Config)# bpdu-tunnel-protocol user-defined-protocol lldp protocol-mac
00-03-c2-00-00-06 encape-type llc dsap 240 ssap 224 group-mac 01-01-00-0c -00-06
```

5.13 EEE Energy-saving

5.13.1 eee enable

Command	**eee enable** **no eee enable**
parameter	-
default	-
Mode	Port Mode
Usage Guide	It supports that configure EEE energy-saving function for the appointed port. There is not the EEE energy-saving function on port as default. After configuring the port to enable EEE energy-saving function, the port will enter the energy-saving state if stop to send packets to the port, the state of port is down. When sending packets to the port, the mode will changed from power saving mode to normal mode.
Example	Enable EEE energy-saving function: Switch(config-if-ethernet1/0/1)#eee enable

5.14 LED shut-off

5.14.1 port-led shutoff time-range

Command	**port-led shutoff time-range <***time-range-name***>** **no port-led shutoff**	
parameter	*time-range-name*	it is the name of the time-range defined by user, it is made up by 1 to 64 characters including letters, numbers, underlines. The first and last characters cannot be the underlines
default	-	
Mode	Global Configuration Mode	
Usage Guide	The LED shut-off function of the port can make all the LEDs off according to the configured time-range by user no matter what the link-act status is. It can save power. When there is no configured time-range, the default is all the times; when the range is exceeded, the port LED can be on according to the link-act status	
Example	Configure all the LEDs to be off in t1. switch(config)#: port-led shutoff time-range t1	

Chapter 6 MAC Address Configuration

6.1 MAC Address Table

6.1.1 clear collision-mac-address-table

Syntax	clear collision-mac-address-table
Parameter	none
Default	none
Mode	Admin Mode
Usage	If enable the function of the hash collision mac table that issued ffp (mac-address-table avoid-collision), the mac cannot be cleared.
Example	Clear the hash collision mac table. Switch#clear collision-mac-address-table

6.1.2 clear mac-address-table dynamic

Syntax	clear mac-address-table dynamic [address <mac-addr>] [vlan <vlan-id>] [interface [ethernet | portchannel] <interface-name>]	
Parameter	<mac-addr>	MAC address will be deleted
	<vlan-id>	Vlan id
	<interface-name>	port name for forwarding the MAC packets
Default	None	
Mode	Admin mode.	
Usage	Delete all dynamic address entries which exist in MAC address table, except application, system entries. MAC address entries can be classified according to different sources, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically.	
Example	Delete all dynamic MAC Switch#clear mac-address-table dynamic	

6.1.3 mac-address-learning enable | disable

Syntax	mac-address-learning (enable | disable) (vlan <vlan-id> | interface ethernet <interface-name>)	
Parameter	enable	Enable MAC learning through port
	disable	Disable MAC learning through port
	<vlan-id>	VLAN ID,range:1-4094
	<interface-name>	Port name
Default	all port auto learning mac address	
Mode	Global mode	
Usage	After disabling the MAC address learning function of the port, the port will not be able to automatically learn the MAC address, and the user can manage it by statically adding the MAC address.	
Example	Disable the MAC learning function of port 8 Switch#config Switch(config)#mac-address-learning disable interface ethernet 1/0/8	

6.1.4 mac-address-table aging-time

Syntax	mac-address-table aging-time <0 | aging-time> no mac-address-table aging-time	
Parameter	0	0 to disable aging.
	aging-time	aging-time seconds, range from 10 to 1000000;
Default	Default aging-time is 300 seconds.	
Mode	Global Mode.	
Usage	If no destination address of the packets is same with the address entry in aging-time, the address entry will get aged. The user had better set the aging-time according to the network condition, it usually use the default value.	
Example	Set the aging-time to 600 seconds. Switch#config Switch(config)#mac-address-table aging-time 600	

6.1.5 mac-address-table static | blackhole

Syntax

mac-address-table {static | blackhole} address <mac-addr> vlan <vlan-id> [interface ethernet <interface-name>] | [source | destination | both]

no mac-address-table {static | blackhole | dynamic} [address <mac-addr>] [vlan <vlan-id>] [interface ethernet <interface-name>]

Parameter

static	static entries
blackhole	filter entries, which is for discarding frames from specific MAC address, it can filter source address, destination address or the both. When choose the filter entries, blackhole address can't based on port, and not configure to interface;
dynamic	dynamic address entries
<mac-addr>	MAC address to be added or deleted
<vlan-id>	vlan number
<interface-name>	name of the port transmitting the MAC data packet
source	based on source address filter
destination	based on destination address filter
both	based on source address and destination address filter, the default is both

Default

When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number.

Mode

Global Mode

Usage

In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN.

no mac-address-table command is for deleting all dynamic, static, filter MAC address entries existing in the switch MAC address list, except application, system entries. MAC address entries can be classified according to the different source, the types are as follows: DYNAMIC, STATIC, APPLICATION, SYSTEM. DYNAMIC is the dynamic MAC address entries learned by switch, it can be aged by switch automatically. STATIC is the static MAC address entries (including blackhole entries) added by user. APPLICATION is the static MAC address entries added by application protocol (such as dot1x, security port…). SYSTEM is the additive static MAC address entries according to VLAN interface. When adding STATIC entries, it can cover the conflictive DYNAMIC, except APPLICATION, SYSTEM entries.

After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.

Example

Port 1/0/1 belongs to VLAN200, and establishes address mapping with MAC address 00-03-0f-f0-00-18.

	Switch#config Switch(config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/0/1

6.1.6 l2-address-table static-multicast address

Syntax	l2-address-table static-multicast address {<ip-addr> |<mac-addr>} vlan <vlan-id> interface [ethernet <interface-name>] | port-channel <port-channel-id> no l2-address-table static-multicast (address {<ip-addr> |<mac-addr>} | vlan <vlan-id>) [interface (ethernet <interface-name>] | port-channel <port-channel-id>)]
Parameter	<ip-addr> IP address add or delete IP address <mac-addr> add or delete MAC address <interface-name> port that transfer MAC data packets <port-channel-id> aggregate port name of transfer MAC data packets <vlan-id> VLAN number
Default	When VLAN interface is configured and is up, the system will generate a static address mapping entry of which the inherent MAC address corresponds to the VLAN number
Mode	Global Mode
Usage	In certain special applications or when the switch is unable to dynamically learn the MAC address, users can use this command to manually establish mapping relation between the MAC address and port and VLAN. After configure the static multicast MAC by this command, the multicast MAC traffic will be forwarded to the specified port of the specified VLAN.
Example	Configure a static multicast ip 232.0.0.1, the egress is ehernet 1/0/1. Switch#config Switch(config)# l2-address-table static-multicast address 232.0.0.1 vlan 200 interface ethernet 1/0/1

6.1.7 show collision-mac-address-table

Syntax show collision-mac-address-table

Parameter None

Default None

Mode Global Mode.

Usage If enable the function of the hash collision mac table that issued ffp (mac-address-table avoid-collision), the collision mac which issued ffp use * to sign.

Example Show the hash collision mac table.

```
Switch#config
Switch(config)#show collision-mac-address-table
The max number can be recorded is 200
The max number of collision is 0
The current number recorded is 0

  MAC Address          VLAN    Collision-count
```

6.1.8 show mac-address-table

Syntax show mac-address-table [static | blackhole | aging-time <aging-time> | count] [address <mac-addr>] [vlan <vlan-id>] [count] [interface <interface-name>]

Parameter

static	static entries
blackhole	filter entries
<aging-time>	address aging time
count	entry's number
<mac-addr>	entry's MAC address
<vlan-id>	entry's VLAN number
<interface-name>	entry's interface name

Default MAC address table is not displayed by default

Mode Admin and Configuration Mode.

Usage This command can display various classes of MAC address entries. Users can also use show mac-address-table to display all the MAC address entries.

Example Display all the filter MAC address entries.

```
Switch#show mac-address-table blackhole
```

6.1.9 show l2-address-table multicast

Syntax	show l2-address-table multicast ([count] | [vlan <vlan-id>])
Parameter	<vlan-id> entry's VLAN number,range:1-4094
Default	MAC address table is not displayed by default
Mode	Admin and Configuration Mode.
Usage	This command can display various classes of multicast address entries.
Example	Display all the vlan1 multicast address entries. Switch#show l2-address-table multicast vlan 1 Vlan Address Insert Type Creator Ports ---- -------------------------- ---------- -------------------------------------

6.1.10 clear mac-notification statistics

Syntax	clear mac-notification statistics
Parameter	None
Default	None
Mode	Admin mode
Usage	When this command is used with show command, it is able to check the executive result by show command after executing this command.
Example	Switch#clear mac-notification statistics Switch#

6.1.11 mac-address-table notification

Syntax	mac-address-table notification no mac-address-table notification
Parameter	none
Default	Disable
Mode	Global Mode
Usage	This command is used with trap switch of snmp. When disabling the MAC address notification, other configuration can be shown, but the function is invalid 。
Example	Enable the MAC address notification. Switch#config Switch(config)#mac-address-table notification Switch(config)#

6.1.12 mac-address-table notification history-size

Syntax	mac-address-table notification history-size <0-500> no mac-address-table notification history-size	
Parameter	history-size	data length of sending the notification, its range from 1 to 500
Default	10	
Mode	Global Mode	
Usage	After the global switch is disabled, this command is also able to be configured sequentially.	
Example	Change the maximum history-size to be 256. Switch#config Switch(config)#mac-address-table notification history-size 256	

6.1.13 mac-address-table notification interval

Syntax	mac-address-table notification interval <1-30> no mac-address-table notification interval	
Parameter	interval	interval for sending the notification, unit is second, its range from 0 to 30。
Default	30s	
Mode	Global Mode	
Usage	After the global switch is disabled, this command is also able to be configured sequentially.	
Example	Configure the interval as 30s for sending the MAC address notification Switch#config Switch(config)#mac-address-table notification interval 30	

6.1.14 mac-notification

Syntax

```
mac-notification {added | all | removed}
no mac-notification
```

Parameter

added	added MAC address
all	added and the removed MAC addresses
removed	removed MAC address

Default

No MAC address notification.

Mode

Port mode

Usage

After the global switch is disabled, this command is also able to be configured sequentially.

Example

Send the trap notification after the MAC address is added to Ethernet 1/0/1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# mac-notification added
```

6.1.15 show mac-notification summary

Syntax

```
show mac-notification summary
```

Parameter

none

Default

Do not show the summary.

Mode

Admin mode

Usage

With this command, check the configuration of MAC address and the sending status of MAC notification trap.

Example

```
Switch#show mac-notification summary
MAC address notification:enabled
MAC address snmp traps:disabled
MAC address notification interval = 5
MAC address notification history log size = 10
MAC address added = 0
MAC address removed = 0
MAC address moved = 0
MAC address snmp traps generated = 0
```

6.1.16 snmp-server enable traps mac-notification

Syntax	snmp-server enable traps mac-notification no snmp-server enable traps mac-notification
Parameter	none
Default	Disable trap notification globally.
Mode	Global Mode
Usage	This command is used with MAC notification switch. When the switch is disabled, other configuration can be shown, but the function is invalid.
Example	Enable the trap notification of MAC address Switch#config Switch(config)#snmp-server enable traps mac-notification

Chapter 7 VLAN Configuration

7.1 VLAN

7.1.1 vlan

Syntax	vlan WORD no vlan	
Parameter	WORD	WORD is the VLAN ID to be created/deleted, valid range is 1 to 4094, connect with ';' and '-'.
Default	Only VLAN1 is set by default.	
Mode	Global Mode	
Usage	VLAN1 is the default VLAN and cannot be configured or deleted by the user. The maximal VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.	

Example

Create VLAN100 and enter the configuration mode for VLAN 100.Display the status for the current VLAN;

```
Switch#config
Switch(config)#vlan 100
Switch#show vlan
VLAN Name         Type       Media     Ports
---- ------------ ---------- --------- ----------------------------------------
1    default      Static     ENET      Ethernet1/0/2       Ethernet1/0/3
                                       Ethernet1/0/4       Ethernet1/0/5
                                       Ethernet1/0/6       Ethernet1/0/7
                                       Ethernet1/0/8       Ethernet1/0/9
                                       Ethernet1/0/10      Ethernet1/0/11
                                       Ethernet1/0/12      Ethernet1/0/13
                                       Ethernet1/0/14      Ethernet1/0/15
                                       Ethernet1/0/16      Ethernet1/0/17
                                       Ethernet1/0/18      Ethernet1/0/19
                                       Ethernet1/0/20      Ethernet1/0/21
                                       Ethernet1/0/22      Ethernet1/0/23
                                       Ethernet1/0/24      Ethernet1/0/25
                                       Ethernet1/0/26      Ethernet1/0/27
                                       Ethernet1/0/28
100  VLAN0100     Static     ENET
Switch#
```

7.1.2 name (vlan)

Syntax

name NAME

no name

Parameter

NAME specified name string.

Default

The default VLAN name is vlanXXX, where xxx is VID.

Mode

VLAN Configuration Mode.

Usage

The switch can specify names for different VLANs, making it easier for users to identify and manage VLANs.

Example

Specify the name of VLAN100 as 100

```
Switch#config
Switch(config)# vlan 100
Switch(config-vlan100)#name 100
Switch# show vlan
VLAN Name          Type        Media      Ports
---- ------------ ---------- --------- ----------------------------------------
1     default        Static       ENET        Ethernet1/0/2          Ethernet1/0/3
                                              Ethernet1/0/4          Ethernet1/0/5
                                              Ethernet1/0/6          Ethernet1/0/7
                                              Ethernet1/0/8          Ethernet1/0/9
                                              Ethernet1/0/10         Ethernet1/0/11
                                              Ethernet1/0/12         Ethernet1/0/13
                                              Ethernet1/0/14         Ethernet1/0/15
                                              Ethernet1/0/16         Ethernet1/0/17
                                              Ethernet1/0/18         Ethernet1/0/19
                                              Ethernet1/0/20         Ethernet1/0/21
                                              Ethernet1/0/22         Ethernet1/0/23
                                              Ethernet1/0/24         Ethernet1/0/25
                                              Ethernet1/0/26         Ethernet1/0/27
                                              Ethernet1/0/28
100   100            Static       ENET
Switch#
```

7.1.3 switchport interface

Syntax

switchport interface [ethernet | portchannel] [<interface-name | interface-list>]

no switchport interface [ethernet | portchannel] [<interface-name | interface-list>]

Parameter

ethernet	Ethernet port to be added
portchannel	link-aggregation port to be added
interface-name	port name, such as e1/0/1. If this option is selected, ethernet or portchannel should not be.
interface-list	port list to be added or deleted, ";" and "-" are supported, for example: ethernet1/0/1;3;4-7;8.

Default

A newly created VLAN contains no port by default.

Mode

VLAN Mode

Usage

Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for a time.

Example

Assign Ethernet port 1，3，4-7 of VLAN100.

```
Switch#config
Switch(config)#vlan 100
Switch(config-vlan100)#switchport interface ethernet 1/0/1;3;4-7
Set the port Ethernet1/0/1 access vlan 100 successfully
Set the port Ethernet1/0/3 access vlan 100 successfully
Set the port Ethernet1/0/4 access vlan 100 successfully
Set the port Ethernet1/0/5 access vlan 100 successfully
Set the port Ethernet1/0/6 access vlan 100 successfully
Set the port Ethernet1/0/7 access vlan 100 successfully
Switch#show vlan
VLAN Name         Type       Media     Ports
---- ------------ ---------- --------- ----------------------------------------
1    default      Static     ENET      Ethernet1/0/2         Ethernet1/0/8
                                       Ethernet1/0/9         Ethernet1/0/10
                                       Ethernet1/0/11        Ethernet1/0/12
                                       Ethernet1/0/13        Ethernet1/0/14
                                       Ethernet1/0/15        Ethernet1/0/16
                                       Ethernet1/0/17        Ethernet1/0/18
                                       Ethernet1/0/19        Ethernet1/0/20
                                       Ethernet1/0/21        Ethernet1/0/22
                                       Ethernet1/0/23        Ethernet1/0/24
                                       Ethernet1/0/25        Ethernet1/0/26
                                       Ethernet1/0/27        Ethernet1/0/28
100  VLAN0100     Static     ENET      Ethernet1/0/1         Ethernet1/0/3
                                       Ethernet1/0/4         Ethernet1/0/5
                                       Ethernet1/0/6         Ethernet1/0/7
Switch#
```

7.1.4 switchport forbidden vlan

Syntax

switchport forbidden vlan (WORD | all | add WORD | except WORD | remove WORD)

Parameter

WORD	add the vlanList as forbidden vlan and cover the previous configuration
all	set all VLANs as forbidden vlan
add WORD	add vlanList to the current forbidden vlanList
except WORD	set all VLANs as forbidden vlan except vlanList
Remove WORD	remove vlan specified by vlanList from current forbidden vlanList

Default

Forbidden vlanList is empty

Mode

Port mode

Usage

Tag the corresponding position for forbidden vlanList and clear allow vlanList flags in ports. A port leaves these VLANs if it joins them statically, and it sends message to GVRP module to enable corresponding registered machine of the port to enter forbidden mode.

show running-config display current setting

Example

Port quits the corresponding VLAN and the corresponding registered machine of GVRP to enter forbidden mode.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode hybrid
Switch(config-if-ethernet1/0/1)#switchport forbidden vlan all
Set the port Ethernet1/0/1 mode Hybrid successfully
Switch#show running-config
!
no service password-encryption
!
hostname Switch
sysLocation Default
sysContact Default
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
!
snmp-server enable
!
```

```
!
vlan 1;100
!
Interface Ethernet1/0/1
  switchport mode hybrid
  switchport forbidden vlan 1-4094
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
  switchport mode trunk
  switchport trunk native vlan 100
!
Interface Ethernet1/0/4
!
Interface Ethernet1/0/5
!
Interface Ethernet1/0/6
!
Interface Ethernet1/0/7
!
Interface Ethernet1/0/8
!
Interface Ethernet1/0/9
Switch#
```

7.1.5 switchport mode

Syntax

switchport mode (access | hybrid | trunk | tunnel)

Parameter

access	Access port.
hybrid	Hybrid port.
trunk	Trunk port.
tunnel	Tunnel port.

Default

The port is in Access mode by default.

Mode

Port Mode.

Usage

Ports in trunk mode is called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through. VLAN in different switches can be interconnected with the Trunk ports. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time. Hybrid ports can allow traffic of multiple VLANs to pass through, receive and send the packets of multiple VLANs, used to connect switch, or user's computer. When Hybrid ports and Trunk ports receive the data, the deal way is same, but the deal way is different in sending the data. Because Hybrid ports can allow the packets of multiple VLANs to send with no tag, however, Trunk ports can only allow the packets of the default VLAN to send with no tag. The attribute of ports can not directly convert between Hybrid and Trunk, it must configure to be access at first, then configure to be Hybrid or Trunk. When the Trunk or Hybrid attribute is cancelled, the port attribute restores the default (access) attribute and belongs to vlan1.

show switchport interface display setting

Example

Set port 1 to hybrid mode.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode hybrid
Set the port Ethernet1/0/1 mode Hybrid successfully
Switch(config-if-ethernet1/0/1)#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Hybrid
Port VID :1
Switch(config-if-ethernet1/0/1)#
```

7.1.6 switchport hybrid native vlan

Syntax

switchport hybrid native vlan <vlan-id>

no switchport hybrid native vlan

Parameter

<vlan-id>	VLAN ID (e.g. 100), PVID of Hybrid port.

Default

The default PVID of Hybrid port is 1.

Mode

Port Mode.

Usage

When an untagged frame enters a Hybrid port, it will be added a tag of the native PVID which is set by this command, and is forwarded to the native VLAN.

show switchport interface display setting。

Example

Set the native vlan to 100 for a Hybrid port.

```
Switch#config
Switch(config) # interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#switchport mode hybrid
Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 100
Switch# show switchport interface ethernet 1/0/2

Ethernet1/0/2
Type :Universal
Mode :Hybrid
Port VID :100
Switch#
```

7.1.7 switchport hybrid allowed vlan

Syntax

switchport hybrid allowed vlan (WORD | all | add WORD | except WORD | remove WORD) (tag | untag)

no switchport hybrid allowed vlan

Parameter

WORD	Set vlan List to allowed vlan, and the late configuration will cover the previous configuration;
all	Set all VLANs to allowed vlan;
add WORD	Add vlanList to the existent allowed vlanList;
except WORD	Set all VLANs to allowed vlan except the configured vlanList;
Remove WORD	Delete the specific VLAN of vlanList from the existent allow vlanList;
tag	Join the specific VLAN with tag mode;
untag	Join the specific VLAN with untag mode.

Default

Deny all VLAN traffic to pass.

Mode

Port Mode.

Usage

The user can use this command to set the VLANs whose traffic allowed to pass through the Hybrid port, traffic of VLANs not included are prohibited. The difference between tag and untag mode by setting allowed vlan: set VLAN to untag mode, the frame sent via hybrid port without VLAN tag; set VLAN to tag mode, the frame sent via hybrid port with corresponding VLAN tag. The same VLAN can not be allowed with tag and untag mode by a Hybrid port at the same time. If configure the tag (or untag) allowed VLAN to untag (or tag) allowed VLAN, the last configuration will cover the previous.

show switchport interface display setting。

Example

Set hybrid port allowed vlan 1,100 with tag mode

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode hybrid
Set the port Ethernet1/0/1 mode Hybrid successfully
Switch(config-if-ethernet1/0/1)#switchport hybrid allowed vlan 1;100 tag
set the Hybrid port Ethernet1/0/1 tag allowed vlan successfully
Switch#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Hybrid
Port VID :1
Hybrid tag allowed Vlan: 1;100
Switch#
```

7.1.8 switchport access vlan

Syntax

switchport access vlan <valn-id>

no switchport access vlan

Parameter

< valn-id >	VLAN ID (e.g. 100),valid range is 1 to 4094.

Default

All ports belong to VLAN1 by default.

Mode

Port Mode.

Usage

Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

The "no switchport access vlan" command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

show switchport interface display setting

Example

Add some Access port to VLAN100.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode access
Set the port Ethernet1/0/1 mode Access successfully
Switch(config-if-ethernet1/0/1)# switchport access vlan 100
Set the port Ethernet1/0/1 access vlan 100 successfully
Switch#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Access
Port VID :100
Switch#
```

7.1.9 switchport trunk allowed vlan

Syntax

switchport trunk allowed vlan (WORD | all | add WORD | except WORD | remove WORD) (tag | untag)

no switchport trunk allowed vlan

Parameter

WORD	specified VIDs ,the range from 1 to 4094;
all	all VIDs
add WORD	add assigned VIDs behind allow vlan;
except WORD	all VID add to allow vlan except assigned VIDs;
Remove WORD	delete assigned allow vlan from allow vlan list.

Default

Trunk port allows all VLAN traffic by default.

Mode

Port Mode.

Usage

The user can use this command to set the VLAN traffic allowed to passthrough the Trunk port; traffic of VLANs not included are prohibited.

show switchport interface display setting.

Example

Set Trunk port to allow traffic of VLAN1, 3-5

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport trunk allowed vlan 1;3-5
set the trunk port Ethernet1/0/1 allowed vlan successfully.
Switch#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan: 1;3-5
Switch#
```

7.1.10 switchport trunk native vlan

Syntax

switchport trunk native vlan <vlan-id>

no switchport trunk allowed vlan

Parameter

<vlan-id>	PVID for Trunk port.

Default

The default PVID of Trunk port is 1.

Mode

Port Mode.

Usage

PVID concept is defined in 802.1Q. PVID in Trunk port is used to tag untagged frames. When an untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this VLAN forwarding.

show switchport interface display setting

Example

Set the native VLAN for a Trunk port to 100.

```
Switch#config
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)# switchport trunk native vlan 100
Set the port Ethernet1/0/3 native vlan 100 successfully
Switch#show switchport interface ethernet 1/0/3

Ethernet1/0/3
Type :Universal
Mode :Trunk
Port VID :100
Trunk allowed Vlan: 1-4094
Switch#
```

7.1.11 switchport mode trunk allow-null

Syntax

switchport mode trunk allow-null

Parameter

none

Default

access mode.

Mode

Port mode

Usage

Configure the port as trunk, enable it to leave all VLANs and clear allow-list.

show switchport interface display setting

Example

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mode trunk allow-null
Set the port Ethernet1/0/1 mode Trunk successfully
Switch#show switchport interface ethernet 1/0/1

Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
  switchport mode trunk allow-null
Switch#
```

7.1.12 vlan ingress enable

Syntax

vlan ingress enable

no vlan ingress enable

Parameter

none

Default

Enable VLAN ingress filtering function.

Mode

Port Mode.

Usage

After VLAN ingress filtering is enabled on the port, when the system receives data it will check source port first, and forwards the data to the destination port if it is the VLAN member port, or else drop the data.

show running-config display setting

Example

Disable VLAN ingress rules on the port.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# no vlan ingress enable
Switch# show running-config
!
no service password-encryption
!
hostname Switch
sysLocation Default
sysContact Default
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
snmp-server enable
!
!
vlan 1
!
Interface Ethernet1/0/1
  no vlan ingress enable
!
Interface Ethernet1/0/2
Switch#
```

7.1.13 vlan-translation enable

Syntax	vlan-translation enable no vlan-translation enable
Parameter	none
Default	VLAN translation has not been enabled on the port by default.
Mode	Port Mode.
Usage	vlan-translation and dot1q-tunnel are mutually exclusive, it is recommended to enable vlan-translation on trunk port and manually disable port filtering. show vlan-translation display setting
Example	Enable VLAN translation function on port1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)# vlan-translation enable Switch# show vlan-translation Interface Ethernet1/0/1: vlan-translation is enable, miss drop is not set Switch#

7.1.14 vlan-translation

Syntax	vlan-translation <old-valn-id> to <new-vlan-id> {in | out}
	no vlan-translation <old-valn-id> {in | out}	

Parameter	old-valn-id	original VLAN ID
	new-vlan-id	translated VLAN ID
	in	ingress translation
	out	outgress translation.
Default	There is no VLAN translation relation.	
Mode	Port Mode.	
Usage	The command is for configuring the translation relation of the VLAN translation function. The data packets will be matched according to the configured translation relations, and its VLAN ID will be changed to the one in the configured item once matched, while forward the packets of the original VLAN if not match. This command cannot be used with dot1q-tunnel enable at the same time. show vlan-translation display setting	

Example

Move the VLAN100 data entered from the port1 to VLAN2 after ingress translation.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# vlan-translation enable
Switch(config-if-ethernet1/0/1)#vlan-translation 100 to 2 in
Switch# show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is not set
    vlan-translation 100 to 2 in
Switch#
```

7.1.15 vlan-translation miss drop

Syntax

vlan-translation miss drop {in|out|both}

no vlan-translation miss drop {in|out|both}

Parameter

in	entrance
out	export
both	two-way

Default

Not miss drop when translation failed.

Mode

Port Mode.

Usage

During translate the mapping relation between original VID and present VID, if not configure related translation, the default is not packets miss. After using the command, it will miss data packets when translation failed.

show vlan-translation display setting

Example

set port 1 translation failed and miss packets in entrance.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# vlan-translation enable
Switch(config-if-ethernet1/0/1)#vlan-translation miss drop in
Switch# show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is set in

Switch#
```

7.1.16 dot1q-tunnel enable

Syntax

dot1q-tunnel enable

no dot1q-tunnel enable

Parameter

none

Default

Dot1q-tunnel function disabled on the port by default.

Mode

Port Mode.

Usage

After enabling dot1q-tunnel on the port, data packets without VLAN tag (referred to as tag) will be packed with a tag when entering through the port; those with tag will be packed with an external tag. The TPID in the tag is the global configuration TPID. it default value is 0x8100, and the VLAN ID is the VLAN ID the port belongs to. Data packets with double tags will be forwarded according to MAC address and external tag, till the external tag is removed when transmitted outside from the access port. Since the length of the data packet may be over sized when packed with external tag, it is recommended to use this command associating the Jumbo function. Normally this command is used on access ports. This command can not be used when vlan-translation enabled.

show dot1q-tunnel display setting

Example

Join port1 into VLAN3, enable dot1q-tunnel function.

```
Switch#config
Switch(config)#vlan 3
Switch(config-vlan3)#switchport interface ethernet 1/0/1
Switch(config-vlan3)#exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel enable
Switch# show dot1q-tunnel
Interface Ethernet1/0/1:
dot1q-tunnel is enable

Switch#
```

7.1.17 dot1q-tunnel selective enable

Syntax

dot1q-tunnel selective enable

no dot1q-tunnel selective enable

Parameter

none

Default

Do not enable selective QinQ.

Mode

Port mode

Usage

Enable selective QinQ command should associates with hybrid mode, and it should not be used with dot1q-tunnel enable synchronously.

show running-config display setting

Example

Enable dot1q-tunnel selective enable of port1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective enable
Switch# show running-config
no service password-encryption
hostname Switch
sysLocation Default
sysContact Default
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
snmp-server enable
!
vlan 1;3
!
Interface Ethernet1/0/1
  dot1q-tunnel selective enable
!
Interface Ethernet1/0/2
!
Interface Ethernet1/0/3
!
Switch#
```

7.1.18 dot1q-tunnel selective s-vlan

Syntax

```
dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list>
no dot1q-tunnel selective s-vlan <s-vlan> c-vlan <c-vid-list>
```

Parameter

<s-vlan>	SP VLAN ID
<c-vid-list>	range of user’s VLAN ID.

Default

There is no mapping relation.

Mode

Port mode

Usage

This command is used to configure the mapping relation for selective QinQ. If packets match the mapping relation, they will be tagged with SP vlan tag as the outer VLAN tag.

show running-config display setting

Example

Packets of VLAN 3 through VLAN 5 are tagged with the tag of VLAN 1 as the outer VLAN tag on Ethernet1/0/1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# dot1q-tunnel selective s-vlan 1 c-vlan 3-5
Switch(config-if-Ethernet1/0/1)# dot1q-tunnel selective enable
Switch# show running-config
!
no service password-encryption
!
hostname Switch
sysLocation Default
sysContact Default
username admin privilege 15 password 0 admin
authentication line console login local
snmp-server enable
vlan 1;3
Interface Ethernet1/0/1
  dot1q-tunnel selective s-vlan 1 c-vlan 3-5
  dot1q-tunnel selective enable
Interface Ethernet1/0/2
Interface Ethernet1/0/3
Interface Ethernet1/0/4
Interface Ethernet1/0/5
Interface Ethernet1/0/6
Switch#
```

7.1.19 garp timer join

Syntax	garp timer join <200-500>	
Parameter	<200-500>	millisecond
Default	200 ms	
Mode	Global mode	
Usage	Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error. show garp timer display setting	
Example	Set the value of garp join timer as 210ms. Switch#config Switch(config)# garp timer join 210 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 600 (ms) GARP leaveall timer value is : 10000 (ms) Switch#	

7.1.20 garp timer leave

Syntax	garp timer leave <500-1200>	
Parameter	<500-1200>	millisecond
Default	600ms	
Mode	Global mode	
Usage	Check whether the value satisfy the range. If so, modify the value of garp timer to the specified value, otherwise return a configuration error. show garp timer display setting	
Example	Set the value of garp leave timer as 700ms. Switch#config Switch(config)#garp time leave 700 Switch#show garp timer GARP join timer value is : 210 (ms) GARP leave timer value is : 700 (ms) GARP leaveall timer value is : 10000 (ms) Switch#	

7.1.21 garp timer leaveall

Syntax

garp timer leaveall <5000-60000>

Parameter

<500-60000>	millisecond

Default

10000ms

Mode

Global mode

Usage

Check whether the value satisfy the range. If so, modify the value of garp leaveAll timer to the specified value, otherwise return a configuration error.

show garp timer display setting

Example

Set the value of garp leaveAll as 20000ms.

```
Switch#config
Switch(config)#garp time leaveall 20000
Switch(config)#show garp timer
GARP join timer value is : 210 (ms)
GARP leave timer value is : 700 (ms)
GARP leaveall timer value is : 20000 (ms)

Switch#
```

7.1.22 no garp timer

Syntax

no garp timer (join | leave | leaveall)

Parameter

join	join timer
leave	leave timer
leaveall	leaveAll timer

Default

200 | 600 | 10000 milliseconds for join | leave | leaveall timer respectively.

Mode

Global mode

Usage

Check whether the default value satisfy the range. If so, modify the value of garp join | leave | leaveAll timer to the default value, otherwise return a configuration error.

show garp timer join display setting

Example

Restore garp timer join to the default value.

```
Switch#config
Switch(config)# no garp timer join
Switch(config)# show garp timer join
GARP join timer value is : 200 (ms)

Switch#
```

7.1.23 gvrp(Global)

Syntax

gvrp

no gvrp

Parameter

none

Default

Disabled.

Mode

Global mode

Usage

Enable GVRP function globally and only in this way GVRP module can work normally.

show running-config display setting

Example

Enable GVRP function globally.

```
Switch#config
Switch(config)#gvrp
Switch(config)#show running-config
!
no service password-encryption
!
hostname Switch
sysLocation Default
sysContact Default
!
username admin privilege 15 password 0 admin
!
authentication line console login local
!
snmp-server enable
!
!!
vlan 1
!
gvrp
!
Interface Ethernet1/0/1
Switch#
```

7.1.24 gvrp(Port)

Syntax	gvrp no gvrp
Parameter	none
Default	Disabled
Mode	Port mode
Usage	GVRP function can only be enabled on trunk and hybrid ports, and enabling GVRP will return an error on access port. After GVRP enabled on port, this port will be added to GVRP (i.e. adding corresponding state machine to GVRP of the port). show gvrp port-member display setting
Example	Enable GVRP of port. Switch#config Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode hybrid Set the port Ethernet1/0/1 mode Hybrid successfully Switch(config-if-ethernet1/0/1)#gvrp Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#

7.1.25 private-vlan

Syntax

private-vlan {primary | isolated | community}

no private-vlan

Parameter

primary	set current VLAN to Primary VLAN
isolated	set current VLAN to Isolated VLAN
community	set current VLAN to Community VLAN

Default

Private VLAN is not configured by default.

Mode

VLAN mode

Usage

There are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN. Ports in Primary there are three Private VLANs: Primary VLAN, Isolated VLAN and Community VLAN can communicate with ports of Isolated VLAN and Community VLAN related to this Primary VLAN; Ports in Isolated VLAN are isolated between each other and only communicate with ports in Primary VLAN they related to; ports in Community VLAN can communicate both with each other and with Primary VLAN ports they related to; there is no communication between ports in Community VLAN and port in Isolated VLAN.

Only VLANs containing empty Ethernet ports can be set to Private VLAN, and only the Private VLANs configured with associated private relationships can set the Access Ethernet ports their member ports. Normal VLAN will clear its Ethernet ports when set to Private VLAN.

It is to be noted Private VLAN messages will not be transmitted by GVRP.

show vlan private-vlan display setting

Example

Set VLAN100, 200, 300 to private vlans, with respectively primary, Isolated, Community types.

```
Switch#config
Switch(config)#vlan 100;200;300
Switch(config)#vlan 100
Switch(config-vlan100)#private-vlan primary
Note:This will remove all the access ports from vlan 100
Switch(config-vlan100)#vlan 200
Switch(config-vlan200)#private-vlan isolated
Note:This will remove all the access ports from vlan 200
Switch(config-vlan200)#vlan 300
Switch(config-vlan300)#private-vlan community
Note:This will remove all the access ports from vlan 300
Switch# show vlan private-vlan
VLAN Name           Type        Asso VLAN Ports
---- ------------ ---------- --------- ----------------------------------------
100   VLAN0100      Primary
200   VLAN0200      Isolate
300   VLAN0300      Community
Switch#
```

7.1.26 private-vlan association

Syntax

private-vlan association <secondary-vlan-list>

no private-vlan association

Parameter

<secondary-vlan-list> Sets Secondary VLAN list which is associated to Primary VLAN. There are two types of Secondary VLAN: Isolated VLAN and Community VLAN. Users can set multiple Secondary VLANs by ';'.

Default

There is no Private VLAN association by default.

Mode

VLAN Mode.

Usage

This command can only used for Private VLAN. The ports in Secondary VLANs which are associated to Primary VLAN can communicate to the ports in Primary VLAN.

Before setting Private VLAN association, three types of Private VLANs should have no member ports; the Private VLAN with Private VLAN association can't be deleted. When users delete Private VLAN association, all the member ports in the Private VLANs whose association is deleted are removed from the Private VLANs.

show vlan private-vlan display setting

Example

Associate Isolated VLAN200 and Community VLAN300 to Primary VLAN100.

```
Switch#config
Switch(config)# vlan 100
Switch(config-vlan100)#private-vlan association 200;300
Set vlan 100 associated vlan successfully
Switch(config-vlan100)#show vlan private-vlan
VLAN Name           Type        Asso VLAN Ports
---- ------------ ---------- --------- ----------------------------------------
100   VLAN0100      Primary      200   300
200   VLAN0200      Isolate      100
300   VLAN0300      Community    100
Switch#
```

7.1.27 show dot1q-tunnel

Syntax

Show dot1q-tunnel

Parameter

none

Default

None.

Mode

Admin and Configuration Mode.

Usage

This command is used for displaying the information of the ports at dot1q-tunnel state.

Example

Display current dot1q-tunnel state.

```
Switch#show dot1q-tunnel
Interface Ethernet1/0/1:
    dot1q-tunnel is enable

Switch#
```

7.1.28 show garp timer

Syntax

Show garp timer [join | leave | leaveall]

Parameter

join	join timer
leave	leave timer
leaveall	leaveAll timer

Default

200|600|10000 milliseconds for join | leave | leaveAll timer respectively.

Mode

Admin mode

Usage

Show the corresponding value of the timer specified in the command.

Example

Show the value of all garp timers currently.

```
Switch# show garp timer
GARP join timer value is : 200 (ms)
GARP leave timer value is : 600 (ms)
GARP leaveall timer value is : 10000 (ms)

Switch#
```

7.1.29 show gvrp fsm information

Syntax

show gvrp fsm information interface (ethernet | port-channel | IFNAME)

Parameter

ethernet	physical port
port-channel	aggregate port
IFNAME	port name

Default

MT for registered machine and VO for request state machine.

Mode

Admin mode

Usage

Show the corresponding state of all registered machines and request state machines.

Example

Show the state of all state machines.

```
Switch# show gvrp fsm information interface ethernet 1/0/1


VA:Very anxious Active member,   AA:Anxious Active member,   QA:Quiet Active member
VP:Very anxious Passive member,   AP:Anxious Passive member,   QP:Quiet Passive member
VO:Very anxious Observer,   AO:Anxious Observer,   QO:Quiet Observer
LA:Leaving Acitve member,   LO:leaving Observer
IN:In,   LV:Leaving,   MT:Empty
INR:In Registration fixed,   LVR:Leaveing Registration fixed,   MTR:Empty Registration fixed
INF:In, registration forbidden,  LVF:Leaveing, registration forbidden,  MTF:Empty, registration
forbidden

Ethernet1/0/1 gvrp fsm information:
Index      VLANID        Applicant        Registrar
-----      ------        ---------        ---------
1          1             Qa               MT
Switch#
```

7.1.30 show gvrp leaveAll fsm information

Syntax

show gvrp leaveAll fsm information interface (ethernet | port-channel | IFNAME)

Parameter

ethernet	physical port
port-channel	aggregate port
IFNAME	port name

Default

Passive

Mode

Admin mode

Usage

Check the state of leaveAll state machine

Example

Show the state of leaveAll state machine on port.

```
Switch# show gvrp fsm information interface ethernet 1/0/1
Interface                    LeaveAll fsm
---------                  ------------
Ethernet1/0/1                Passive
Switch#
```

7.1.31 show gvrp leavetimer running information

Syntax

show gvrp leavetimer running information [vlan <1-4094> |]interface (ethernet | port-channel | IFNAME)

Parameter

<1-4094>	Vlan tag
ethernet	physical port
port-channel	aggregate port
IFNAME	port name

Default

leavetimer is disabled.

Mode

Admin mode

Usage

Show running state and expiration time of each leave timer.

Example

Show running state and expiration time of each leave timer on current port.

```
Switch# show gvrp leavetimer running information interface ethernet 1/0/1
VLANID       running state          expired time
------       -------------          ------------
Switch#
```

7.1.32 show gvrp port-member

Syntax	show gvrp [active |] port-member	
Parameter	active	port is in active state
Default	GVRP is disabled on port.	
Mode	Admin mode	
Usage	Show all ports (enable GVRP) saved in GVRP.	
Example	Show all ports with GVRP enabled. Switch#show gvrp port-member Ports which were enabled gvrp included: Ethernet1/0/1 Switch#	

7.1.33 show gvrp port registerd vlan

Syntax	show gvrp port [dynamic | static] registerd vlan interface (Ethernet | port-channel | IFNAME)	
Parameter	dynamic	dynamic registration
	static	static registration
	Ethernet	physical port
	port-channel	aggregate port
	port IFNAME	port name
Default	No dynamic or static registration VLANs on port.	
Mode	Admin mode	
Usage	Show the corresponding VLANs of the registered machines by dynamic or static registration.	
Example	Show all dynamic or static registration VLANs on current port. Switch#show gvrp port registerd vlan interface ethernet 1/0/1 Current port dynamic registerd vlan included: Current port static registerd vlan included: Switch#	

7.1.34 show gvrp timer running information

Syntax	show gvrp timer (join | leaveall) running information interface (ethernet | port-channel | IFNAME)	
Parameter	join	join timer
	leaveall	leaveAll timer
	Ethernet	physical port
	port-channel	aggregate port
	port IFNAME	port name
Default	Join timer is disabled and leaveAll timer is enabled	
Mode	Admin mode	
Usage	Check running state of join|leaveAll timer on port.	
Example	Show running state and expiration time of each timer. Switch#show gvrp timer join running information interface ethernet 1/0/1 Current port's jointimer running state is: UP Current port's jointimer expired time is: 0.2 s Switch#	

7.1.35 show gvrp vlan registerd port

Syntax	show gvrp vlan <1-4094> registerd port	
Parameter	<1-4094>	Vlan tag
Default	No ports with specified VLAN registered.	
Mode	admin mode	
Usage	none	
Example	Show all ports with current VLAN registered. Switch#show gvrp vlan 100 registerd port Ethernet1/0/3（T） Ethernet1/0/4（T） Ethernet1/0/5（T） Ethernet1/0/6（T） Ethernet1/0/7（T） Ethernet1/0/8（T） Ethernet1/0/9（T） Ethernet1/0/10（T） Switch#	

7.1.36 show vlan

Syntax

show vlan [brief | summary] [id <vlan-id>] [name <vlan-name>] [internal usage [id <vlan-id> | name <vlan-name>]]

Parameter

brief	brief information;
summary	VLAN statistics
<vlan-id>	for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094;
<vlan-name>	is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.

Default

none

Mode

Admin Mode and Configuration Mode.

Usage

If no <vlan-id> or <vlan-name> is specified, then information for all VLANs in the switch will be displayed.

Example

Display the status for the current VLAN; display statistics for the current VLAN.

```
Switch#show vlan
VLAN Name         Type       Media     Ports
---- ------------ ---------- --------- ----------------------------------------
1    default      Static     ENET      Ethernet1/0/2        Ethernet1/0/3
                                       Ethernet1/0/4        Ethernet1/0/5
                                       Ethernet1/0/6        Ethernet1/0/7
                                       Ethernet1/0/8        Ethernet1/0/9
                                       Ethernet1/0/10       Ethernet1/0/11
                                       Ethernet1/0/12       Ethernet1/0/13
                                       Ethernet1/0/14       Ethernet1/0/15
                                       Ethernet1/0/16       Ethernet1/0/17
                                       Ethernet1/0/18       Ethernet1/0/19
                                       Ethernet1/0/20       Ethernet1/0/21
                                       Ethernet1/0/22       Ethernet1/0/23
                                       Ethernet1/0/24       Ethernet1/0/25
                                       Ethernet1/0/26       Ethernet1/0/27
                                       Ethernet1/0/28
Switch#show vlan summary
The max. Vlan entries: 4094

Existing Vlan:
Universal Vlan:
1
```

```
Private Vlan:
100     200     300

Total Existing Vlan:4
Switch#
```

displayed information	Explanation
VLAN	VLAN ID
Name	VLAN name
Type	VLAN type, statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN

7.1.37 show vlan-translation

Syntax show vlan-translation

Parameter None

Default none

Mode Admin and Configuration Mode.

Usage Display the information of all the ports at VLAN-translation state.

Example Display current VLAN translation state information.

```
Switch#show vlan-translation
Interface Ethernet1/0/1:
    vlan-translation is enable, miss drop is not set
```

7.1.38 vlan-translation n-to-1

Syntax

vlan-translation n-to-1 <WORD> to <new-vlan-id>

no vlan-translation n-to-1 <WORD>

Parameter

<WORD>	original VLAN ID, its range from 1 to 4094, connect them with ‘;’ and ‘-’. If there are two VLANs with different range are translated into different VLAN ID in the same port, two VLAN ranges should not be superposed.
<new-vlan-id>	translated VLAN ID,its range from 1 to 4094.

Default

Disable

Mode

Port mode

Usage

Multi-to-One VLAN translation is used to network edge to map multiple VLANs to one VLAN of backbone network. When data traffic returns from backbone network to network edge, it will restore VLAN of network edge to implement Multi-to-One VLAN translation and save VLAN resource of backbone network. Note: When using this function, the device must establish the original and the translated VLAN firstly, and enabling the downlink port of this function and the uplink port for connecting backbone network, which must be join in the original and the translated VLAN with tagged mode. This function should not be used with dot1q-tunnel and VLAN translation at the same time Note: Multi-to-One VLAN translation should be enabled after MAC learning.

show vlan-translation n-to-1 display setting ◦

Example

On Ethernet 1/0/1, translate the data traffic from VLAN with the range between 1 to 5 into VLAN 100, and translate the data traffic (belongs to VLAN with the range between 1 to 5) out from VLAN100 into the corresponding VLAN ID, connect the uplink port of the backbone network as Ethernet 1/0/5.

```
Switch#config
Switch(config)#vlan 1;5;100
Switch(config)#vlan 2-4
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#switchport mode trunk
Set the port Ethernet1/0/1 mode Trunk successfully
Switch(config-if-ethernet1/0/1)#vlan-translation n-to-1 1-5 to 100
Switch(config-if-ethernet1/0/1)#interface ethernet 1/0/5
Switch(config-if-ethernet1/0/5)#switchport mode trunk
Set the port Ethernet1/0/5 mode Trunk successfully
Switch#show vlan-translation n-to-1
Ethernet1/0/1:
vlan-translation n-to-1 enable
  vlan-translation n-to-1 1-5 to 100
```

7.1.39 show vlan-translation n-to-1

Syntax

show vlan-translation n-to-1 <interface-name>

Parameter

<interface-name> Specify the name of the port which will be shown. If there is no parameter, show all port configurations with this function.

Default

There is no Multi-to-One VLAN translation information.

Mode

Admin mode.

Usage

If appointed vlan when show, it will display the n-to-1 translation of specified vlan, if not appointed vlan, it will display all n-to-1 information.

Example

Show all port configurations with Multi-to-One VLAN translation function.

```
Switch#show vlan-translation n-to-1
Ethernet1/0/1:
vlan-translation n-to-1 enable
  vlan-translation n-to-1 1-5 to 100
```

7.1.40 dynamic-vlan mac-vlan prefer

Syntax

dynamic-vlan mac-vlan prefer

Parameter

None

Default

MAC-based VLAN is preferred by default.

Mode

Global Mode.

Usage

Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN.IP-subnet-based VLAN.Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. After the IP-subnet-based VLAN is set to be preferred and the user wish to restore to preferring the MAC-based VLAN, please use this command.

show dynamic-vlan prefer display setting ◦

Example

Set the MAC-based VLAN preferred.

```
Switch#config
Switch(config)#dynamic-vlan mac-vlan prefer
Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan
```

7.1.41 dynamic-vlan subnet-vlan prefer

Syntax

dynamic-vlan subnet-vlan prefer

Parameter

None

Default

MAC-based VLAN is preferred by default.

Mode

Global Mode.

Usage

Configure the preference of dynamic-vlan on switch. The default priority sequence is MAC-based VLAN. IP-subnet-based VLAN. Protocol-based VLAN, namely the preferred order when several dynamic VLAN is available. This command is used to set to preferring the IP-subnet-based VLAN.

show dynamic-vlan prefer display setting。

Example

Set the IP-subnet-based VLAN preferred.

```
Switch#config
Switch(config)#dynamic-vlan subnet-vlan prefer
Switch(config)#show dynamic-vlan prefer
IP Subnet Vlan
Mac Vlan/Voice Vlan
Protocol Vlan
```

7.1.42 mac-vlan vlan

Syntax

mac-vlan vlan <vlan-id>

no mac-vlan vlan <vlan-id>

Parameter

<vlan-id> <vlan-id> is the number of the specified VLAN.

Default

No MAC VLAN is configured by default.

Mode

Global Mode.

Usage

Set specified VLAN for MAC VLAN.

show mac-vlan display setting.

Example

Set VLAN100 to MAC VLAN.

```
Switch#config
Switch(config)#mac-vlan vlan 100
Switch#show vlan
VLAN Name         Type       Media     Ports
---- ------------ ---------- --------- ----------------------------------------
1    default      Static     ENET      Ethernet1/0/1          Ethernet1/0/2
                                       Ethernet1/0/3          Ethernet1/0/4
                                       Ethernet1/0/5          Ethernet1/0/6
                                       Ethernet1/0/7          Ethernet1/0/8
```

```
                                              Ethernet1/0/9        Ethernet1/0/10
                                              Ethernet1/0/11       Ethernet1/0/12
                                              Ethernet1/0/13       Ethernet1/0/14
                                              Ethernet1/0/15       Ethernet1/0/16
                                              Ethernet1/0/17       Ethernet1/0/18
                                              Ethernet1/0/19       Ethernet1/0/20
                                              Ethernet1/0/21       Ethernet1/0/22
                                              Ethernet1/0/23       Ethernet1/0/24
                                              Ethernet1/0/25       Ethernet1/0/26
                                              Ethernet1/0/27       Ethernet1/0/28
100    VLAN0100        UserDynam    ENET
```

7.1.43 mac-vlan

Syntax	mac-vlan mac <mac-addrss> <mac-mask> vlan <vlan-id> priority <priority-id> no mac-vlan {mac <mac-addrss> <mac-mask>|all}	
Parameter	<mac-addrss>/<mac-mask>	mac-address/mac-mask format:XX-XX-XX-XX-XX-XX
	<vlan-id>	vlan-id is the ID of the VLAN with a valid range of 1~4094
	<priority-id>	priority-id is the level of priority and is used in the VLAN tag with a valid range of 0~7
Default	No MAC address joins the VLAN by default.	
Mode	Global Mode	
Usage	With this command user can add specified MAC address to specified VLAN. If there is a non VLAN label data packet enters from the switch port from the specified MAC address, it will be assigned with specified VLAN ID so sent enter specified VLAN. Their belonging VLAN are the same no matter which port did they enter through. The command does not have any interfere on the VLAN label data packet. show mac-vlan display setting	
Example	Add network device of MAC address as 00-03-0f-11-22-33 to VLAN 100. Switch#config Switch(config)#mac-vlan vlan 100 Switch(config)#mac-vlan mac 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff vlan 100 priority 0 Switch#show mac-vlan Mac-Address Mac-Mask VLAN_ID Priority ----------------- ----------------- ------- -------- 00-03-0f-11-22-33 ff-ff-ff-ff-ff-ff 100 0	

7.1.44 protocol-vlan

Syntax

protocol-vlan mode (ethernetII | snap) etype <etype-id> vlan <vlan-id> [priority <priority-id>]

protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id> vlan <vlan-id>

no protocol-vlan (mode ((ethernetII | snap) etype <etype-id>) | all}

no protocol-vlan mode llc dsap <dsap-id> ssap <ssap-id>

Parameter

<etype-id>	etype-id is the type of the packet protocol, with a valid range of 1536~65535;
<vlan-id>	vlan-id is the ID of VLAN, the valid range is 1~4094。
<priority-id>	priority-id is the priority, the range is 0~7
<dsap-id>/<ssap-id>	dsap-id is Dsap ID，ssap-id is Ssap ID，the range is 0-255

Default

No protocol joined the VLAN by default

Mode

Global Mode

Usage

The command adds specified protocol into specified VLAN. If there is any non VLAN label packet from specified protocol enters through the switch port, it will be assigned with specified VLAN ID and enter the specified VLAN. No matter which port the packets go through, their belonging VLAN is the same. The command will not interfere with VLAN labeled data packets. It is recommended to configure ARP protocol together with the IP protocol or else some application may be affected.

show protocol -vlan display setting。

Example

Assign the IP protocol data packet encapsulated by the EthernetII to VLAN200

```
Switch#config
Switch(config)#protocol-vlan mode ethernetII etype 1536 vlan 200
Switch#show protocol-vlan
Protocol_Type                           VLAN_ID        Priority
----------------------------       -------       --------
mode ethernetii etype 0x600               200            0
mode ethernetii etype 0x60e                 1            7
mode snap etype 0x613                       1            1
mode llc dsap 0x1    ssap 0x1               1            0
```

7.1.45 show dynamic-vlan prefer

Syntax show dynamic-vlan prefer

Parameter None

Default Mac Vlan/Voice Vlan

Mode Admin Mode and Configuration Mode.

Usage Display the dynamic VLAN preference.

Example Display current dynamic VLAN preference.

```
Switch#show dynamic-vlan prefer
Mac Vlan/Voice Vlan
IP Subnet Vlan
Protocol Vlan
```

7.1.46 show mac-vlan interface

Syntax show mac-vlan interface

Parameter None

Default None

Mode Admin Mode and other configuration Mode.

Usage Display the ports of enabling MAC-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example Display the ports of enabling MAC-based VLAN currently.

```
Switch#show mac-vlan
Ports
-----------------------------------------
  Ethernet1/0/1(A)      Ethernet1/0/2(A)
  Ethernet1/0/3(A)      Ethernet1/0/4(A)
  Ethernet1/0/5(A)      Ethernet1/0/6(A)
  Ethernet1/0/7(A)      Ethernet1/0/8(A)
  Ethernet1/0/9(A)      Ethernet1/0/10(A)
  Ethernet1/0/11(A)     Ethernet1/0/12(A)
  Ethernet1/0/13(A)     Ethernet1/0/14(A)
  Ethernet1/0/15(A)     Ethernet1/0/16(A)
  Ethernet1/0/17(A)     Ethernet1/0/18(A)
  Ethernet1/0/19(A)     Ethernet1/0/20(A)
  Ethernet1/0/21(A)     Ethernet1/0/22(A)
  Ethernet1/0/23(A)     Ethernet1/0/24(A)
  Ethernet1/0/25(A)     Ethernet1/0/26(A)
  Ethernet1/0/27(A)     Ethernet1/0/28(A)
```

7.1.47 show protocol-vlan

Syntax	show protocol-vlan
Parameter	None
Default	None
Mode	Admin Mode and Configuration Mode
Usage	Display the configuration of Protocol-based VLAN on the switch.

Example

Display the configuration of the current Protocol-based VLAN.

```
Switch#show protocol-vlan
Protocol_Type                          VLAN_ID        Priority
----------------------------     -------       --------
mode ethernetii etype 0x600             200             0
mode ethernetii etype 0x60e               1             7
mode snap etype 0x613                     1             1
mode llc dsap 0x1    ssap 0x1             1             0
```

7.1.48 show subnet-vlan

Syntax	show subnet-vlan
Parameter	None
Default	None
Mode	Admin Mode and other Configuration Mode.
Usage	Display the configuration of the IP-subnet-based VLAN on the switch.

Example

Display the configuration of the current IP-subnet-based VLAN.

```
Switch#show subnet-vlan
IP-Address              Mask                      VLAN_ID        Priority
----------------      ----------------      -------       --------
192.168.5.2            255.255.255.0                100             0
```

7.1.49 show subnet-vlan interface

Syntax show subnet-vlan interface

Parameter None

Default None

Mode Admin Mode and other Configuration Mode.

Usage Display the port of enabling IP-subnet-based VLAN, the character in the bracket indicate the ports mode, A means Access port, T means Trunk port, H means Hybrid port.

Example Display the port of enabling IP-subnet-based VLAN currently.

```
Switch#show subnet-vlan interface
Ports
----------------------------------------
 Ethernet1/0/1(A)     Ethernet1/0/2(A)
 Ethernet1/0/3(A)     Ethernet1/0/4(A)
 Ethernet1/0/5(A)     Ethernet1/0/6(A)
 Ethernet1/0/7(A)     Ethernet1/0/8(A)
 Ethernet1/0/9(A)     Ethernet1/0/10(A)
 Ethernet1/0/11(A)    Ethernet1/0/12(A)
 Ethernet1/0/13(A)    Ethernet1/0/14(A)
 Ethernet1/0/15(A)    Ethernet1/0/16(A)
 Ethernet1/0/17(A)    Ethernet1/0/18(A)
 Ethernet1/0/19(A)    Ethernet1/0/20(A)
 Ethernet1/0/21(A)    Ethernet1/0/22(A)
 Ethernet1/0/23(A)    Ethernet1/0/24(A)
 Ethernet1/0/25(A)    Ethernet1/0/26(A)
 Ethernet1/0/27(A)    Ethernet1/0/28(A)
```

7.1.50 subnet-vlan

Syntax

subnet-vlan ip-address <ipv4-addrss> mask <subnet-mask> vlan <vlan-id> priority <priority-id>

no subnet-vlan {ip-address <ipv4-addrss> mask <subnet-mask> | all}

Parameter

<ipv4-addrss>	ipv4-address is the IPv4 address shown in dotted decimal notation; the valid range of each section is 0~255;
<subnet-mask>	subnet-mask is the subnet mask code shown in dotted decimal notation; the valid range of each section is 0~255;
<vlan-id>	vlan-id is the VLAN ID with a valid range of 1~4094
<priority-id>	priority-id is the priority applied in the VLAN tag with a valid range of 0~7;

Default

No IP subnet joined the VLAN by default.

Mode

Global Mode.

Usage

This command is used for adding specified IP subnet to specified VLAN. When packet without VLAN label and from the specified IP subnet enters through the switch port, it will be matched with specified VLAN id and enters specified VLAN. These packets will always come to the same VLAN no matter through which port did they enter. This command will not interfere with VLAN labeled data packets.

show subnet-vlan display setting.

Example

Add the network equipment with IP subnet of 192.168.1.1/24 to VLAN 300

```
Switch#config
Switch(config)#vlan 300
Switch(config-vlan300)#exit
Switch(config)#subnet-vlan ip-address 192.168.1.1 mask 255.255.255.0 vlan 300 priority 0
Switch(config)#show subnet-vlan
IP-Address                 Mask                          VLAN_ID          Priority
----------------         ----------------         -------        --------
192.168.1.1                255.255.255.0                   300               0
```

7.1.51 switchport mac-vlan enable

Syntax

switchport mac-vlan enable

no switchport mac-vlan enable

Parameter

none

Default

The MAC-base VLAN function is enabled on the port by default.

Mode

Port Mode.

Usage

After adding a MAC address to specified VLAN, the MAC-based VLAN function will be globally enabled. This command can disable the MAC-based VLAN function on specified port to meet special user applications.

show mac-vlan interface display setting。

Example

Disable the MAC-based VLAN function on port1.

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no switchport mac-vlan enable
Switch(config-if-ethernet1/0/1)#show mac-vlan interface
Ports
----------------------------------------
  Ethernet1/0/2(A)     Ethernet1/0/3(A)
  Ethernet1/0/4(A)     Ethernet1/0/5(A)
  Ethernet1/0/6(A)     Ethernet1/0/7(A)
  Ethernet1/0/8(A)     Ethernet1/0/9(A)
  Ethernet1/0/10(A)    Ethernet1/0/11(A)
  Ethernet1/0/12(A)    Ethernet1/0/13(A)
  Ethernet1/0/14(A)    Ethernet1/0/15(A)
  Ethernet1/0/16(A)    Ethernet1/0/17(A)
  Ethernet1/0/18(A)    Ethernet1/0/19(A)
  Ethernet1/0/20(A)    Ethernet1/0/21(A)
  Ethernet1/0/22(A)    Ethernet1/0/23(A)
  Ethernet1/0/24(A)    Ethernet1/0/25(A)
  Ethernet1/0/26(A)    Ethernet1/0/27(A)
  Ethernet1/0/28(A)
```

7.1.52 switchport subnet-vlan enable

Syntax

switchport subnet-vlan enable

no switchport subnet-vlan enable

Parameter

none

Default

The IP-subnet-based VLAN is enabled on the port by default.

Mode

Port Mode.

Usage

After adding the IP subnet to specified VLAN, the IP-subnet-based VLAN function will be globally enabled. This command can disable the IP-subnet-based VLAN function on specified port to meet special user applications.

show subnet-vlan interface display setting.

Example

Disable the IP-subnet-based VLAN function on port2.

```
Switch#config
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#no switchport subnet-vlan enable
Switch(config-if-ethernet1/0/2)#show subnet-vlan interface
Ports
----------------------------------------
  Ethernet1/0/1(A)     Ethernet1/0/3(A)
  Ethernet1/0/4(A)     Ethernet1/0/5(A)
  Ethernet1/0/6(A)     Ethernet1/0/7(A)
  Ethernet1/0/8(A)     Ethernet1/0/9(A)
  Ethernet1/0/10(A)    Ethernet1/0/11(A)
  Ethernet1/0/12(A)    Ethernet1/0/13(A)
  Ethernet1/0/14(A)    Ethernet1/0/15(A)
  Ethernet1/0/16(A)    Ethernet1/0/17(A)
  Ethernet1/0/18(A)    Ethernet1/0/19(A)
  Ethernet1/0/20(A)    Ethernet1/0/21(A)
  Ethernet1/0/22(A)    Ethernet1/0/23(A)
  Ethernet1/0/24(A)    Ethernet1/0/25(A)
  Ethernet1/0/26(A)    Ethernet1/0/27(A)
  Ethernet1/0/28(A)
```

7.1.53 show voice-vlan

Syntax

show voice-vlan

Parameter

None

Default

None

Mode

Admin Mode and other Configuration Mode.

Usage

Display Voice VLAN Configuration.

Example

Display the Current Voice VLAN Configuration.

```
Switch#show subnet-vlan
IP-Address                  Mask                        VLAN_ID        Priority
----------------       ----------------       -------        --------
192.168.5.2                255.255.255.0                  100               0
```

7.1.54 switchport voice-vlan enable

Syntax

switchport voice-vlan enable

no switchport voice-vlan enable

Parameter

none

Default

Voice VLAN is enabled by default.

Mode

Port Mode.

Usage

When voice equipment is added to the Voice VLAN, the Voice VLAN is enabled globally by default. This command disables Voice VLAN on specified port to meet specified application of the user. show voice-vlan display setting。

Example

Disable the Voice VLAN function on port2.

```
Switch#config
Switch(config)# interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)# no switchport voice-vlan enable
Switch(config-if-ethernet1/0/2)# show voice-vlan
Voice VLAN ID:100
Ports
----------------------------------------
  Ethernet1/0/1(A)    Ethernet1/0/3(A)
  Ethernet1/0/4(A)    Ethernet1/0/5(A)
  Ethernet1/0/6(A)    Ethernet1/0/7(A)
  Ethernet1/0/8(A)    Ethernet1/0/9(A)
  Ethernet1/0/10(A)   Ethernet1/0/11(A)
  Ethernet1/0/12(A)   Ethernet1/0/13(A)
  Ethernet1/0/14(A)   Ethernet1/0/15(A)
  Ethernet1/0/16(A)   Ethernet1/0/17(A)
  Ethernet1/0/18(A)   Ethernet1/0/19(A)
  Ethernet1/0/20(A)   Ethernet1/0/21(A)
  Ethernet1/0/22(A)   Ethernet1/0/23(A)
  Ethernet1/0/24(A)   Ethernet1/0/25(A)
  Ethernet1/0/26(A)   Ethernet1/0/27(A)
  Ethernet1/0/28(A)
Voice name          Mac-Address           Mask                  Priority
---------------     -----------------     -----------------     --------
```

7.1.55 voice-vlan

Syntax

voice-vlan mac <mac-address> mask <mac-mask> priority <priority-id> [name <voice-name>]

no voice-vlan {mac <mac-address> mask <mac-mask> | name <voice-name> | all}

Parameter

<mac-address>	Mac-address is the voice equipment MAC address, shown in ”xx-xx-xx-xx-xx-xx” format;
<mac-mask>	mac-mask is the last eight digit of the mask code of the MAC address, the valid values are: 0xff, 0xfe, 0xfc, 0xf8, 0xf0, 0xe0, 0xc0,0x80, 0x0;
<priority-id>	priority-id is the priority of the voice traffic, the valid range is 0–7;
<voice-name>	the voice-name is the name of the voice equipment, which is to facilitate the equipment management;

Default

This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.

Mode

Global Mode.

Usage

This command will add a specified voice equipment into the Voice VLAN, if a non VLAN labeled data packet from the specified voice equipment enters through the switch port, then no matter through which port the packet enters, it will belongs to Voice VLAN. The command will not interfere with the packets of VLAN labels.

show voice-vlan display setting.

Example

Add the 256 sets of voice equipments of the R&D department with MAC address ranging from 00-03-0f-11-22-00 to 00-03-0f-11-22-ff to the Voice VLAN.

```
Switch#config
Switch(config)#vlan 100
Switch(config-vlan100)#exit
Switch(config)#voice-vlan vlan 100
Switch(config)#voice-vlan mac 00-03-0f-11-22-00 mask 0 priority 5 name R&D
Switch(config)#show voice-vlan
Voice VLAN ID:100
Ports
----------------------------------------
  Ethernet1/0/1(A)      Ethernet1/0/3(A)
  Ethernet1/0/4(A)      Ethernet1/0/5(A)
  Ethernet1/0/6(A)      Ethernet1/0/7(A)
  Ethernet1/0/8(A)      Ethernet1/0/9(A)
  Ethernet1/0/10(A)     Ethernet1/0/11(A)
  Ethernet1/0/12(A)     Ethernet1/0/13(A)
  Ethernet1/0/14(A)     Ethernet1/0/15(A)
  Ethernet1/0/16(A)    Ethernet1/0/17(A)
  Ethernet1/0/18(A)    Ethernet1/0/19(A)
  Ethernet1/0/20(A)    Ethernet1/0/21(A)
  Ethernet1/0/22(A)    Ethernet1/0/23(A)
  Ethernet1/0/24(A)    Ethernet1/0/25(A)
  Ethernet1/0/26(A)    Ethernet1/0/27(A)
  Ethernet1/0/28(A)
Voice name             Mac-Address              Mask                      Priority
---------------      -----------------      -----------------      --------
R&D                     00-03-0f-11-22-00      00-00-00-00-00-00                 5
```

7.1.56 voice-vlan vlan

Syntax

voice-vlan vlan <vlan-id>

no voice-vlan

Parameter

<vlan-id>	Vlan id is the number of the specified VLAN.

Default

No Voice VLAN is configured by default.

Mode

Global Mode.

Usage

Set specified VLAN for Voice VLAN, There can be only one Voice VLAN at the same time. The voice VLAN can not be applied concurrently with MAC-based VLAN.

show voice-vlan display setting.

Example

Set VLAN100 to Voice VLAN.

```
Switch#config
Switch(config)#vlan 100
Switch(config-vlan100)#exit
Switch(config)#voice-vlan vlan 100
Switch(config)#show voice-vlan
Voice VLAN ID:100
Ports
----------------------------------------
  Ethernet1/0/1(A)      Ethernet1/0/3(A)
  Ethernet1/0/4(A)      Ethernet1/0/5(A)
  Ethernet1/0/6(A)      Ethernet1/0/7(A)
  Ethernet1/0/8(A)      Ethernet1/0/9(A)
  Ethernet1/0/10(A)     Ethernet1/0/11(A)
  Ethernet1/0/12(A)     Ethernet1/0/13(A)
  Ethernet1/0/14(A)     Ethernet1/0/15(A)
  Ethernet1/0/16(A)     Ethernet1/0/17(A)
  Ethernet1/0/18(A)     Ethernet1/0/19(A)
  Ethernet1/0/20(A)     Ethernet1/0/21(A)
  Ethernet1/0/22(A)     Ethernet1/0/23(A)
  Ethernet1/0/24(A)     Ethernet1/0/25(A)
  Ethernet1/0/26(A)     Ethernet1/0/27(A)
  Ethernet1/0/28(A)
Voice name           Mac-Address           Mask                   Priority
---------------      -----------------     -----------------      --------
```

Chapter 8 Anti-ring Protocol

8.1 MSTP

8.1.1 abort

Command	abort
parameter	-
default	-
Mode	MSTP Region Mode
Usage Guide	This command is to quit MSTP region mode without saving the current configuration. The previous MSTP region configuration is valid.
Example	Quit MSTP region mode without saving the current configuration. Switch(Config-Mstp-Region)#abort Switch(config)#

8.1.2 exit

Command	**exit**
parameter	-
default	-
Mode	MSTP Region Mode
Usage Guide	This command is to quit MSTP region mode with saving the current configuration.
Example	Quit MSTP region mode with saving the current configuration. Switch(Config-Mstp-Region)#exit Switch(config)#

8.1.3 instance vlan

Command	**instance <*instance-id*> vlan <*vlan-list*>** **no instance <*instance-id*> [vlan <*vlan-list*>]**	
parameter	***instance-id***	sets the instance number. The valid range is from 0 to 64
	vlan-list	sets consecutive or non-consecutive VLAN numbers. “-” refers to consecutive numbers, and “;” refers to non-consecutive numbers
default	Before creating any Instances, there is only the instance 0, and VLAN 1~4094 all belong to the instance 0.	
Mode	MSTP Region Mode	
Usage Guide	This command sets the mappings between VLANs and instances. Only if all the mapping relationships and other attributes are same, the switches are considered in the same MSTP region. Before setting any instances, all the VLANs belong to the instance 0. MSTP can support maximum 64 MSTIs (except for CISTs). CIST can be treated as MSTI 0. All the other instances are considered as instance 1 to 64.	
Example	Map VLAN1-10 and VLAN 100-110 to Instance 1. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110	

8.1.4 Name

Command	**name <*name*>** **no name**	
parameter	***name***	is the MSTP region name. The length of the name should be less than 32 characters
default	Default MSTP region name is the MAC address of this bridge.	
Mode	MSTP Region Mode	
Usage Guide	This command is to set MSTP region name. The bridges with same MSTP region name and same other attributes are considered in the same MSTP region.	
Example	Set MSTP region name to mstp-test. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#name mstp-test	

8.1.5 revision-level

Command	**revision-level <*level*>** **no revision-level**	
parameter	***level***	is revision level. The valid range is from 0 to 65535
default	The default revision level is 0.	
Mode	MSTP Region Mode	
Usage Guide	This command is to set revision level for MSTP configuration. The bridges with same MSTP revision level and same other attributes are considered in the same MSTP region.	
Example	Set revision level to 2000. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)# revision-level 2000	

8.1.6 spanning-tree

Command	**spanning-tree** **no spanning-tree**
parameter	-
default	MSTP is not enabled by default.
Mode	Global Mode and Port Mode
Usage Guide	If the MSTP is enabled in global mode, the MSTP is enabled in all the ports except for the ports which are set to disable the MSTP explicitly
Example	Enable the MSTP in global mode, and disable the MSTP in the interface1/0/2. Switch(config)#spanning-tree Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#no spanning-tree

8.1.7 spanning-tree cost

Command

spanning-tree cost <*cost*>

no spanning-tree cost

parameter

cost	sets path cost. The valid range is from 1 to 200,000,000.

default

By default, the port cost is relevant to the port bandwidth.

For the aggregation ports, the default costs are as below:	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost	默认端口
10Mbps	N	2000000/N	2000000
100Mbps	N	200000/N	200000/N
1GMbps	N	20000/N	20000/N

Mode

Port Mode

Usage Guide

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of port and the designated port of the instance.

Example

On the port1/0/2, set the port cost is 3000000.

```
Switch(Config-If-Ethernet1/0/2)#spanning-tree cost 3000000
```

8.1.8 spanning-tree digest-snooping

Command	**spanning-tree digest-snooping** **no spanning-tree digest-snooping**
parameter	-
default	Don't use the authentication string of partner port.
Mode	Port Mode
Usage Guide	According to MSTP protocol, the region authentication string is generated by MD5 algorithm with public authentication key, intstance ID, VLAN ID. Some manufactory don't use the public authentication key, this causes the incompatibility. After the command is executed the port can use the authentication string of partner port, realize compatibility with these manufactories equipment. Because the authentication string is related to instance ID and VLAN ID, the command may cause recognizing the equipment that with different instance and VLAN relation as in the same region. Before the command is executed, make sure that instance and VLAN relation is accord for all the equipment. If there are more than one equipment connected, all the connected ports should execute this command.
Example	Configure the authentication string of partner port. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree digest-snooping Switch(Config-If-Ethernet1/0/2)#

8.1.9 spanning-tree format

Command	**spanning-tree format {standard | privacy | auto}** **no spanning-tree format**	
parameter	**standard**	The packet format provided by IEEE
	privacy	Privacy packet format, which is compatible with CISCO equipments.
	auto	Auto identified packet format, which is determined by checking the format of the received packets.
default	Auto Packet Format.	
Mode	Port Mode	
Usage Guide	As the CISCO has adopted the packet format different with the one provided by IEEE, while many companies also adopted the CISCO format to be CISCO compatible, we have to provide support to both formats. The standard format is originally the one provided by IEEE, and the privacy packet format is CISCO compatible. In case we are not sure about which the packet format is on partner, the AUTO configuration will be preferred so to identify the format by the packets they sent. The AUTO packet format is set by default in the concern of better compatibility with previous products and the leading companies. The packet format will be privacy format before receiving the partner packet when configured to AUTO. When the format is not AUTO and the received packet format from the partner does not match the configured format, we set the state of the port which receives the unmatched packet to DISCARDING to prevent both sides consider themselves the root which leads to circuits. When the AUTO format is set, and over one equipment which is not compatible with each other are connected on the port (e.g. a equipment running through a HUB or Transparent Transmission BPDU is connected with several equipments running MSTP), the format alter counts will be recorded and the port will be disabled at certain count threshold. The port can only be re-enabled by the administrator.	
Example	Configure port message format as the message format of IEEE. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree format standard Switch(Config-If-Ethernet1/0/2)#	

8.1.10 spanning-tree forward-time

Command	**spanning-tree forward-time <*time*>** **no spanning-tree forward-time**	
parameter	***time***	is forward delay time in seconds. The valid range is from 4 to 30
default	The forward delay time is 15 seconds by default	
Mode	Global Mode	
Usage Guide	When the network topology changes, the status of the port is changed from blocking to forwarding. This delay is called the forward delay. The forward delay is co working with hello time and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly。 2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)	
Example	In global mode, set MSTP forward delay time to 20 seconds. Switch(config)#spanning-tree forward-time 20	

8.1.11 spanning-tree hello-time

Command	**spanning-tree hello-time <*time*>** **no spanning-tree hello-time**	
parameter	***time***	is Hello time in seconds. The valid range is from 1 to 10
default	Hello Time is 2 seconds by default	
Mode	Global Mode	
Usage Guide	This command is used to set the interval bpdu switch sending, command "no spanning-tree hello-time" restore default configuration.Hello time is the interval that the switch sends BPDUs. Hello time is co working with forward delay and max age. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly. 2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)	
Example	Set MSTP hello time to 5 seconds in global mode. Switch(config)#spanning-tree hello-time 5	

8.1.12 spanning-tree link-type p2p

Command	**spanning-tree link-type p2p {auto | force-true | force-false}** **no spanning-tree link-type**	
parameter	**auto**	sets auto-negotiation
	force-true	forces the link as point-to-point type
	force-false	forces the link as non point-to-point type.
default	The link type is auto by default; The MSTP detects the link type automatically.	
Mode	Port Mode	
Usage Guide	For configuring port link types, command "no spanning-tree link-type" restore default configuration.When the port is full-duplex, MSTP sets the port link type as point-to-point; When the port is half-duplex, MSTP sets the port link type as shared.	
Example	Force the port 1/0/7-8 as point-to-point type. Switch(config)#interface ethernet 1/0/7-8 Switch(Config-Port-Range)#spanning-tree link-type p2p force-true	

8.1.13 spanning-tree maxage

Command	**spanning-tree maxage <*time*>** **no spanning-tree maxage**	
parameter	***time***	is max aging time in seconds. The valid range is from 6 to 40.
default	The max age is 20 seconds by default.	
Mode	Global Mode	
Usage Guide	this command is used to configure bpdu maximum aging time, command "no spanning-tree maxage" restore default configuration.The lifetime of BPDU is called max age time. The max age is co working with hello time and forward delay. The parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly. 2 * (Bridge_Forward_Delay - 1.0 seconds) >= Bridge_Max_Age Bridge_Max_Age >= 2 * (Bridge_Hello_Time + 1.0 seconds)	
Example	In global mode, set max age time to 25 seconds. Switch(config)#spanning-tree maxage 25	

8.1.14 spanning-tree max-hop

Command	**spanning-tree max-hop <*hop-count*>** **no spanning-tree max-hop**	
parameter	***hop-count***	sets maximum hops. The valid range is from 1 to 40
default	The max hop is 20 by default.	
Mode	Global Mode	
Usage Guide	This command is used to set BPDU maximum number of hops, and the command "**no spanning-tree max-hop**" is used to restore the default configuration.The MSTP uses max-age to count BPDU lifetime. In addition, MSTP also uses max-hop to count BPDU lifetime. The max-hop is degressive in the network. The BPDU has the max value when it initiates from MSTI root bridge. Once the BPDU is received, the value of the max-hop is reduced by 1. When a port receives the BPDU with max-hop as 0, it drops this BPDU and sets itself as designated port to send the BPDU.	
Example	Set max hop to 32. Switch(config)#spanning-tree max-hop 32	

8.1.15 spanning-tree mcheck

Command	**spanning-tree mcheck**
parameter	-
default	The port is in the MSTP mode by default
Mode	Port Mode
Usage Guide	If a network which is attached to the current port is running IEEE 802.1D STP, the port converts itself to run in STP mode. The command is used to force the port to run in the MSTP mode. But once the port receives STP messages, it changes to work in the STP mode again. This command can only be used when the switch is running in IEEE802.1s MSTP mode. If the switch is running in IEEE802.1D STP mode, this command is invalid.
Example	Force the port 1/0/2 to run in the MSTP mode. Switch(Config-If-Ethernet1/0/2)#spanning-tree mcheck

8.1.16 spanning-tree mode

Command	**spanning-tree mode {mstp | stp | rstp}** **no spanning-tree mode**	
parameter	**mstp**	sets the switch in IEEE802.1s MSTP mode
	stp	sets the switch in IEEE802.1D STP mode
	rstp	sets the switch in IEEE802.1D RSTP mode
default	The switch is in the MSTP mode by default	
Mode	Global Mode	
Usage Guide	This command is used to configure the spanning tree mode and the command "**no spanning-tree mode**" is used to restore the default mode.When the switch is in IEEE802.1D STP mode, it only sends standard IEEE802.1D BPDU and TCN BPDU. It drops any MSTP BPDUs.	
Example	Set the switch in the STP mode. Switch(config)#spanning-tree mode stp	

8.1.17 spanning-tree mst configuration

Command	**spanning-tree mst configuration** **no spanning-tree mst configuration**
parameter	-
default	-
Mode	Global Mode
Usage Guide	Whether the switch is in the MSTP region mode or not, users can enter the MSTP mode, configure the attributes, and save the configuration. When the switch is running in the MSTP mode, the system will generate the MST configuration identifier according to the MSTP configuration. Only if the switches with the same MST configuration identifier are considered as in the same MSTP region.
Example	Enter MSTP region mode. Switch(config)#spanning-tree mst configuration Switch(Config-Mstp-Region)#

8.1.18 panning-tree mst cost

Command

spanning-tree mst <*instance-id*> cost <*cost*>

no spanning-tree mst <instance-id> cost

parameter

instance-id	sets the instance ID. The valid range is 0-64
cost	sets path cost, different cost formats have different ranges. For the default dot1t mode the valid range is 1-200,000,000, and for dot1d is 1-65535.

default

By default, the port cost is relevant to the port bandwidth.

Port Type	Default Path Cost	Suggested Range
10Mbps	2000000	2000000-20000000
100Mbps	200000	200000-2000000
1GMbps	20000	20000-200000

For the aggregation ports, the default costs are as below:

Port Type	Allowed Number Of Aggregation Ports	Default Port Cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1GMbps	N	20000/N

Port Speed	Port Type	Port Cost	
		802.1D-2008	802.1T
0		65535	200000000
10Mbps	Half- duplex Full- duplex aggregation link with 2 ports aggregation link with 3 ports	100 99 95 95 95	2,000,000 1,999,999 1,000,000 666,666 500,000

	aggregation link with 4 ports		
100Mbps	Half- duplex Full- duplex aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	19 18 15 15 15	200,000 199,999 100,000 66,666 50,000
1000Mbps	Full- duplex aggregation link with 2 ports aggregation link with 3 ports aggregation link with 4 ports	4 3 3 3	20,000 10,000 6,666 5,000

Mode

Port Mode

Usage Guide

By setting the port cost, users can control the cost from the current port to the root bridge in order to control the elections of root port and the designated port of the instance.

Example

On the port1/0/2, set the MSTP port cost in the instance 2 to 3000000.

Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 2 cost 3000000

8.1.19 spanning-tree cost-format

Command	**spanning-tree cost-format {dot1d | dot1t}**
	-
default	count path-cost with dot1t format.
Mode	Global mode.
Usage Guide	There are two formats about cost value: they are dot1d marked on IEEE802.1d-2008 and dot1t marked on IEEE802.1t, but path-cost ranges of them are different, dot1d range from 1 to 65535, and dot1t range from 1 to 200,000,000.
Example	Set the cost format in global mode. Switch(config)#spanning-tree cost-format dot1d

8.1.20 spanning-tree mst loopguard

Command	**spanning-tree [mst <instance-id>] loopguard** **no spanning-tree [mst <instance-id>] loopguard**	
parameter	**instance-id**	MSTP instance ID.
default	Disable loopguard function	
Mode	Port Mode	
Usage Guide	The command can avoid root port or alternate port to be changed as designated port due to invalid unilateralism link. When the receiving timer is time, the configured port with loopguard is set as block state.	
Example	Configure port 1/0/2 as loopguard mode for instance 0. Switch(Config)#interface ethernet 1/0/2 Switch(Config-Ethernet-1/0/2)#spanning-tree mst 0 loopguard Switch(Config-Ethernet-1/0/2)#	

8.1.21 spanning-tree mst port-priority

Command	**spanning-tree mst <*instance-id*> port-priority <*port-priority*>** **no spanning-tree mst <*instance-id*> port-priority**	
parameter	***instance-id***	sets the instance ID. The valid range is from 0 to 64
	port-priority	sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32…240.
default	The default port priority is 128	
Mode	Port Mode	
Usage Guide	By setting the port priority, users can control the port ID of the instance in order to control the root port and designated port of the instance. The lower the value of the port priority is, the higher the priority is.	
Example	Set the port priority as 32 on the port 1/0/2 for the instance 1. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 1 port-priority 32	

8.1.22 spanning-tree mst priority

Command	**spanning-tree mst <*instance-id*> priority <*bridge-priority*>** **no spanning-tree mst <*instance-id*> priority**	
parameter	***instance-id***	sets instance ID. The valid range is from 0 to 64;
	port-priority	sets the switch priority. The valid range is from 0 to 61440. The value should be the multiples of 4096, such as 0, 4096, 8192…61440
default	The default bridge priority is 32768	
Mode	Global Mode	
Usage Guide	By setting the bridge priority, users can change the bridge ID for the specified instance. And the bridge ID can influence the elections of root bridge and designated port for the specified instance.	
Example	Set the priority for Instance 2 to 4096. Switch(config)#spanning-tree mst 2 priority 4096	

8.1.23 spanning-tree mst rootguard

Command	**spanning-tree [mst <*instance-id*>] rootguard** **no spanning-tree [mst <*instance-id*>] rootguard**
parameter	***instance-id*** MSTP instance ID
default	Disable rootguard function
Mode	Port Mode
Usage Guide	The command is used in Port Mode, if the port is configured to be a rootguand port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked).If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.
Example	Enable rootguard function for port 1/0/2 in instance 0. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree mst 0 rootguard Switch(Config-If-Ethernet1/0/2)#

8.1.24 spanning-tree portfast

Command	**spanning-tree portfast [bpdufilter | bpduguard] [recovery <30-3600>]** **no spanning-tree portfast**
parameter	**bpdufilter** configure the border port mode as BPDU filter **bpduguard** configure the border port mode as BPDU guard **recovery** configure the border port can be recovered automatically after implement bpduguard violation operation **<30-3600>** the recovery time, do not recover it by default
default	All the ports are non-boundary ports by default when enabling MSTP

Mode	Port Mode
Usage Guide	Set the current port as boundary port, and BPDU filter. BPDU guard as specified mode or default mode; the command "no spanning-tree portfast" sets the current port as non-boundary port. When a port is set to be a boundary port, the port converts its status from discarding to forwarding without bearing forward delay. Once the boundary port receives the BPDU, the port becomes a non-boundary port.
Example	Configure the border port mode as BPDU guard, the recovery time as 60s. Switch(config)#interface ethernet 1/0/2 Switch(Config-If-Ethernet1/0/2)#spanning-tree portfast bpduguard recovery 60 Switch(Config-If-Ethernet1/0/2)#

8.1.25 spanning-tree port-priority

Command	**spanning-tree port-priority <*port-priority*>** **no spanning-tree port-priority**	
parameter	***port-priority***	sets port priority. The valid range is from 0 to 240. The value should be the multiples of 16, such as 0, 16, 32, 48…240
default	The default port priority is 32768	
Mode	Port Mode	
Usage Guide	By setting the port priority to designated port. The lower the value of the port priority is, the higher the priority is.	
Example	Set the port priority as 4096 on the port 1. Switch(Config-If-Ethernet1/0/1)#spanning-tree port-priority 4096	

8.1.26 spanning-tree priority

Command	**spanning-tree priority <*bridge-priority*>** **no spanning-tree priority**	
parameter	***bridge-priority***	is the priority of the bridging switch. Its value should be round times of 4096 between 0 and 61440, such as 0, 4096, 8192… 61440.
default	Default priority is 32768	
Mode	Global Mode	
Usage Guide	The bridge ID can be altered by changing the priority of the switch. Further, the priority information can also be used for voting of the root bridge and the specified ports. The bridge priority value of the switch is smaller, however the priority is higher.	
Example	Configure the priority is 4096. Switch(config)#spanning-tree priority 4096	

8.1.27 spanning-tree rootguard

Command	**spanning-tree rootguard** **no spanning-tree rootguard**
parameter	-
default	Port is non-root port
Mode	Port Mode
Usage Guide	The command is used in Port Mode, if the port is configured to be a rootguand port, it is forbidden to be a MSTP root port. If superior BPDU packet is received from a rootguard port, MSTP did not recalculate spanning-tree, and just set the status of the port to be root_inconsistent (blocked). If no superior BPDU packet is received from a blocked rootguard port, the port status will restore to be forwarding. The rootguard function can maintain a relative stable spanning-tree topology when a new switch is added to the network.
Example	Set the port 1 is root port. Switch(Config-If-Ethernet1/0/1)#spanning-tree rootguard

8.1.28 spanning-tree tcflush (Global mode)

Command	**spanning-tree tcflush {enable| disable| protect}** **no spanning-tree tcflush**	
parameter	**enable**	The spanning-tree flush once the topology changes.
	disable	The spanning tree don't flush when the topology changes.
	protect	the spanning-tree flush not more than one time every ten seconds.
default	Enable	
Mode	Global mode	
Usage Guide	Configure the spanning-tree flush mode once the topology changes. "**no spanning-tree tcflush**" restores to default setting. According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.	
Example	Configure the spanning-tree flush mode once the topology changes is not flush to TC. Switch(config)#spanning-tree tcflush disable Switch(config)#	

8.1.29 spanning-tree tcflush (Port mode)

Command	**spanning-tree tcflush {enable| disable| protect}** **no spanning-tree tcflush**	
parameter	**enable**	The spanning-tree flush once the topology changes
	disable	The spanning tree don't flush when the topology changes
	protect	the spanning-tree flush not more than one time every ten seconds
default	Default enable mode	
Mode	Port Mode	
Usage Guide	Configure the spanning-tree flush mode for port once the topology changes. "**no spanning-tree tcflush**" restores to default setting. According to MSTP, when topology changes, the port that send change message clears MAC/ARP table (FLUSH). In fact it is not needed for some network environment to do FLUSH with every topology change. At the same time, as a method to avoid network assault, we allow the network administrator to configure FLUSH mode by the command.	
Example	Configure the spanning-tree flush mode once the topology change is not flush to TC. Switch(config)#spanning-tree tcflush disable	

8.1.30 spanning-tree transmit-hold-count

Command	**spanning-tree transmit-hold-count <*tx-hold-count-value*>** **no spanning-tree transmit-hold-count**	
parameter	***tx-hold-count-value***	ranging from 1 to 20, the default value is 10
default	10	
Mode	Global Mode	
Usage Guide	Set the max number for sending BPDU within the Hello Time interval to control BPDU flow. The variable is used to whole MST bridge.	
Example	Set the max transmit-hold-count as 20. Switch(config)#spanning-tree transmit-hold-count 20	

8.1.31 show mst-pending

Command	**show mst-pending**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	In the MSTP region mode, display the configuration of the current MSTP region such as MSTP name, revision, VLAN and instance mapping.

Example

Display the configuration of the current MSTP region.

```
Switch(config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#show mst-pending
Name switch
Revision 0
Instance Vlans Mapped
----------------------------------
00 1-29, 31-39, 41-4093
03 30
04 40
05 4094
----------------------------------
Switch(Config-Mstp-Region)#
```

8.1.32 show spanning-tree

Command	**show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]**	
	instance-id	sets interface list
	interface-list	sets the instance ID. The valid range is from 0 to 64
	detail	sets the detailed spanning-tree information
default	-	
Mode	Admin and Configuration Mode	
Usage Guide	This command can display the MSTP information of the instances in the current bridge.	
Example	Display the bridge MSTP.	

```
Switch#sh spanning-tree
*********************************** Process 0 ***********************************
                      -- MSTP Bridge Config Info --

Standard        :   IEEE 802.1s
Bridge MAC      :   00:1f:ce:10:b0:1b
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3

############################ Instance 0 ############################
Self Bridge Id     : 32768.00:1f:ce:10:b0:1b
Root Id                : this switch
Ext.RootPathCost : 0
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID        : 0
Current port list in Instance 0:
Ethernet1/0/12 Ethernet1/0/20 (Total 2)

    PortName          ID        ExtRPC     IntRPC    State Role        DsgBridge
DsgPort
-------------- -------- --------- --------- ---    ---- ------------------ --------
Ethernet1/0/12 128.012             0             0 FWD    DSGN 32768.001fce10b01b
128.012
Ethernet1/0/20 128.020             0             0 FWD    DSGN 32768.001fce10b01b
128.020
```

Display information	describe
MSTP Bridge Config Info	
Standard	STP version
Bridge MAC	Bridge MAC address
Bridge Times	Max Age, Hello Time and Forward Delay of the bridge
Force Version	Version of STP
Instance 0	
Self Bridge Id	The priority and the MAC address of the current bridge for the current instance
Root Id	The priority and the MAC address of the root bridge for the current instance
Ext.RootPathCost	Total cost from the current bridge to the root of the entire network
Int.RootPathCost	Cost from the current bridge to the region root of the current instance
Root Port ID	Root port of the current instance on the current bridge
Current port list in Instance 0	
PortName	Port name
ID	Port priority and port index
ExtRPC	Port cost to the root of the entire network
IntRPC	Cost from the current port to the region root of the current instance
State Role	Port status of current instance
DsgBridge	Upward designated bridge of the current port in the current instance
DsgPort	Upward designated port of the current port in the current instance

8.1.33 show spanning-tree mst config

Command	**show spanning-tree mst config**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	In the Admin mode, this command can show the parameters of the MSTP configuration such as MSTP name, revision, VLAN and instance mapping.
Example	Display the configuration of the MSTP on the switch.

```
Switch#show spanning-tree mst config

Name
Revision        0
Instance        Vlans Mapped
---------------------------------
00               1-4094
---------------------------------
```

8.1.34 spanning-tree process

Command	**spanning-tree process <process-id>** **no spanning-tree process <process-id>**
parameter	**process-id** the range is 1-31
default	-
Mode	Global Mode
Usage Guide	Create the new mstp process. Multiple mstp processes can be configured on one device and each process is standalone. The process 0 exists only as default.
Example	Create the new mstp process 1.

```
Switch(config)#spanning-tree process 1
```

8.1.35 spanning-tree tc-notify process0

Command	**spanning-tree tc-notify process0** **no spanning-tree tc-notify process0**
parameter	-
default	-
Mode	mstp process mode
Usage Guide	When there is a change in mstp process N, the device will receive the tc packet, at the same time, the process N will notify tc to the instance in mstp process 0 on the shared link. It makes the process 0 refresh the table entry for ensuring the traffic not to break off.
Example	Configure to notify TC of process 1 to process 0. Switch(Config-Mstp-Process-1)#spanning-tree tc-notify process0

8.1.36 spanning-tree binding-process

Command	**spanning-tree binding-process <process-id>** **no spanning-tree binding-process <process-id>**
parameter	**process-id** the range is 1-31.
default	All the ports belong to process 0
Mode	Port Mode
Usage Guide	Configure the port to join the appointed mstp process N. The port will enter into process N from the process 0. This command is mutually exclusive to the shared port configuration command (link-share).
Example	Add the Ethernet1/0/2 into process 1. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1

8.1.37 spanning-tree binding-process link-share

Command	**spanning-tree binding-process < process-id > link-share** **no spanning-tree binding-process < process-id > link-share**
parameter	**process-id** the range is 1-31
default	The port is only in the mstp calculating of process 0
Mode	Port Mode
Usage Guide	Configure the port belong to the shared port of process N. Except for process 0, the configured port can be in the mstp calculating of multiple processes, but the port status can be only configured by process 0. This command can be configured for more than once.
Example	Configure the Ethernet1/0/2 as the shared port of process 1 and 0. Switch(Config-If-Ethernet1/0/2)#spanning-tree binding-process 1 link-share

8.2 ERPS Configuration

8.2.1 ethernet tcn-propagation erps

Command

ethernet tcn-propagation erps to {erps | stp}

no ethernet tcn-propagation erps to

parameter

erps	topology changing sends the R-APS event packets to notify the connection ring of this device
stp	topology changing sends the stp packets to notify the stp topology connected to this device

default

ERPS ring topology changing only takes effect in this ring but does not send the notification packets

Mode

Global Mode

Usage Guide

Configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other ERPS rings; if configured stp method, it will send the stp packets outward.

Example

Configure to send R-APS event notification to the interconnection ring after the topology changing.

```
Switch(config)#ethernet tcn-propagation erps to erps
```

Configure to send STP notification to the interconnection ring after the topology changing.

```
Switch(config)#ethernet tcn-propagation erps to stp
```

Delete the topology changing transmission notification method.

```
Switch(config)#no ethernet tcn-propagation erps to
```

8.2.2 erps-ring

Command	**erps-ring <** ***ring-name*** **>** **no erps-ring <** ***ring-name*** **>**	
parameter	***ring-name***	the ERPS ring name created. The maximum character number is 64 and it is made up with letters, numbers and the underlines. The first and last character cannot be the underline
default	Do not configure any ERPS ring.	
Mode	Global Mode	
Usage Guide	Create a ERPS ring and enter ERPS ring configuration mode. enter ERPS ring configuration mode if the ERPS ring already exists. no command delete ERPS ring.	
Example	Create the ERPS ring of ring1 Switch(config)#erps-ring 1 Switch(config-erps-ring)# Delete the EPRS ring of ring1 Switch(config)#no erps-ring 1	

8.2.3 version

Command	**version {v1 | v2}** **no version**	
parameter	**v1**	means to support v1 which is released in 2008-06 and the amendment (2009-04)
	v2	means to support v2 which is released in 2010-03 and the amendment (2010-06)
default	**V2**	
Mode	ERPS Ring Configuration Mode	
Usage Guide	This command is used to configure the supporting version of the ERPS loop, no the	

command is restored to the default state of the v2.

If configured ERPS ring to support v1, this ring will not support multi-instance. ERPS ring instance does not support the management commands of MS, FS, etc. and the non-revertive switch is not effective. It only support revertive switch.

If configured ERPS ring to support v1, the instance of this ring will deal with the ERPS packets according to the v1 format. Package the R-APS packets and resolve the fields according to v1 format. The fields defined by v2 will not be dealt.

Example

Configure the ERPS ring of ring1 to support v1

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#version v1
```

Delete v1 supported by the ERPS ring of ring1

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#no version
```

8.2.4 open-ring

Command

open-ring

no open-ring

parameter

-

default

Default Configuration ERPS Subrings

Mode

ERPS Ring Configuration Mode

Usage Guide

If the ERPS ring instance has been configured on the ring, there will be the message of "**Cann't config open-ring on ERPS ring whitch has ERPS instance, please delete ERPS instance firstly!**" Otherwise, enter into the next step. Configure this ERPS ring type as sub ring.

Example

Configure the ERPS ring of ring1 as sub ring of open type.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#open-ring
```

Delete the configuration of the sub ring of open type.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no open-ring
```

8.2.5 raps-virtual-channel

Command

raps-virtual-channel {with | without}

parameter

with	the R-APS virtual channel is existed in this ERPS ring
without	the R-APS virtual channel is not existed in this ERPS ring

default

The R-APS virtual channel is not existed in ERPS ring

Mode

ERPS Ring Configuration Mode

Usage Guide

Configure if there is the R-APS virtual channel in ERPS ring according to the configuration.

Inputting: Success or error. If there is not R-APS virtual channel on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R-APS channel and the data channel will be blocked at the same time.

Example

Configure that there is R-APS virtual channel in the ERPS sub ring of ring1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#raps-virtual-channel with
```

8.2.6 erps-ring

Command

erps-ring <ring-name> port0 [port1]

no erps-ring <ring-name> port0

parameter

ring-name	ERPS ring name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines
port1-none	there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node

default

Do not configure port0 on ERPS ring

Mode

Port Mode

Usage Guide

this command is used to configure the port as the port of the specified ERPS ring.
If this ERPS ring is not open-ring type, the port1-none cannot be configured.
Check if the ERPS ring configuration is integral; if it is integral, check if the ERPS instance
configuration is integral; if it is integral, activate the instance as active and run the protocol.

Example

Configure e 1/0/1 as the port0 of ERPS ring1

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#erps-ring ring1 port0
```

Delete the e 1/0/1 as port0 of ERPS ring1

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#no erps-ring ring1 port0
```

8.2.7 failure-detect

Command

{port0 | port1} failure-detect {cc | physical-link-or-cc} domain <domain-name> service {< ma-name > | number < ma-num > | pvlan < vlan-id >} mep
<mep-id> rmep<rmep-id>
no {port0 | port1} failure-detect

parameter

{port0 | port1}	parameter selection. Port0 means the fault detection type of port0. Port1 means the fault detection type ofport1
{cc|physical-link-or-cc}	parameter selection. cc means that the ERPS ring port detection is cc report fault. physical-link-or-cc means that the ERPS ring port detection is cc report fault and physical link fault.
<domain-name>	the cfm domain name of ERPS ring port detection
< ma-name >	the service name that cfm belongs to of ERPS ring port detection.
<mep-id>	the local mep id that cfm monitored of ERPS ring port detection
<rmep-id>	the remote mep id that cfm monitored of ERPS ring port detection

default

ERPS ring port only detects the physical link fault as default

Mode

ERPS Ring Configuration Mode

Usage Guide

Configure the fault detection type of ERPS ring ports. If it is detected as cc type, the maintenance domain, maintenance set that cc belongs to and the monitoring link (it is conditioned with (mep-id, rmep-id)) should be appointed. The premise of this configuration is that the corresponding ring port has been joined into ERPS ring. The no command deletes
the fault detection type of ERPS ring ports.
Configure the fault detection type of ERPS ring ports as the appointed type. If the type is cc,
save the configured md, ma, mep and rmep information to use for matching after receiving
the cfm fault notification.

Example

Configure the detection type of ERPS ring1 port0as cc.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#port0 failure-defect cc domain domain1 service serivice1 mep 1 rmep 2
```

Delete this configuration.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no port0 failure-defect
```

8.2.8 erps-instance

Command

erps-instance <instance-id>
no erps-instance <instance-id>

parameter

instance-id	id of ERPS ring, the range is 1 to 48

default

Do not configure any ERPS ring instance

Mode

ERPS Ring Configuration Mode

Usage Guide

Create the ERPS ring instance and enter into the ERPS ring instance configuration Mode.
If the ERPS ring supports v1, there will be the message of “Doesn't support multiple ERPS instance capability on the ring running version 1!” when configured more than one

ERPS instance.

Example

Configure the ERPS ring instance 1 on ERPS ring1.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#
```

Delete the ERPS ring instance 1 on ERPS ring1.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#no erps-instance 1
```

8.2.9 description

Command

description <instance-name>
no description <instance-name>

parameter

instance-name	ERPS instance name, the maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.

default

Do not configure the ERPS instance name as default

Mode

ERPS Instance Configuration Mode

Usage Guide

Configure the description string for the ERPS instance.

Example

Configure the ERPS instance1 name on ring1 as instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# description instance1
```

Delete this name of instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)# no description
```

8.2.10 ring-id

Command

ring-id <ring-id>
no ring-id <ring-id>

parameter

ring-id	ERPS ring id and the range is 1 to 64

default

The MAC address is 01-19-A7-00-00-01 as default

Mode

ERPS Instance Configuration Mode.

Usage Guide

Configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. If ERPS ring supports v1, ring-id only can be configured as 1. The no command configures it not to carry the ring-id, it means that the MAC is 01-19-A7-00-00-01.

Example

Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 to carry the ring-id 2.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#ring-id 2
```

Configure the last byte of R-APS packets destination MAC address sent by ERPS ring1 instance2 not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01.

```
Switch(config)#erps-ring 1
Switch(config-erps-ring)#erps-instance 2
Switch(config-erps-ring-inst-2)#no ring-id
```

8.2.11 rpl

Command

rpl {port0 | port1} {owner | neighbour}
no rpl {port0 | port1}

parameter

{port0 | port1}	ERPS ring member ports
{owner | neighbour}	**Owner**：RPL owner **Neighbour**：RPL owner

default

None, it is the ordinary transmission node type.

Mode	ERPS Instance Configuration Mode
Usage Guide	Configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. The no command configures the member port of ERPS ring instance as the ordinary transmission port member.
Example	Configure the port0 of ERPS ring1 instance1 as RPL owner node. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)# rpl port0 owner

8.2.12 non-revertive

Command	**non-revertive** **no non-revertive**
parameter	-
default	ERPS ring instance supports the revertive as default
Mode	ERPS Instance Configuration Mode
Usage Guide	Configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring.
Example	Configure the ERPS ring1 instance1 to support the non-revertive. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#non-revertive

8.2.13 guard-timer

Command	**guard-timer <guard-times>** **no guard-timer**
parameter	**guard-times** the interval is 10ms and the range is 10ms to 2s
default	500ms
Mode	ERPS Instance Configuration Mode
Usage Guide	Configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the Request/State="1110" are except) will be dropped. The no command configures the guard timer as the default value.
Example	Configure the guard timer of ERPS ring1 instance1 as 1s. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)guard-timer 100

8.2.14 holdoff-timer

Command	**holdoff –timer <holdoff-times>** **no holdoff -timer**
parameter	**holdoff-times** the interval is 1s and the range is 0 to 10s
default	0s
Mode	ERPS Instance Configuration Mode
Usage Guide	This command is used to configure the delay timer, and the default configuration is restored in the form of No
Example	Configure the Holdoff timer of ERPS ring1 instance1 as 5s. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#holdoff –timer 5

8.2.15 wtr-timer

Command	**wtr-timer <wtr-times>** **no wtr-timer**	
parameter	**wtr-times**	the interval is 1min and the range is from 1 to 12min
default	5min	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. The no command configures the WTR timer as the default.	
Example	Configure the WTR timer of ERPS ring1 instance1 as 10min. Switch(config)#erps-ring 1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#wtr-timer 10	

8.2.16 protected-instance

Command	**protected-instance <instance-list>** **no protected-instance <instance-list>**	
parameter	**instance-list**	the MSTP instance list protected by ERPS ring instance, such as i, j-k. The number of the instances in the list is not limited.
default	ERPS ring instance does not protect any MSTP instance	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance.	
Example	Configure the protection instance of ERPS ring1 instance1 as instance 2. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#protected-instance 2	

8.2.17 raps-mel

Command	**raps-mel <level-value>** **no raps-mel**	
parameter	**level-value**	the level value of APS packets, range is from 0 to 7
default	Level is 7	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the level of R-APS channel of ERPS ring instance as the appointed level. If configured successfully, the mel field of the R-APS packet sent by this ERPS ring instance will be added as the appointed level and only the R-APS packets with the level that is larger than or same as the appointed level can be allowed passing by, or notify the error. The no command configures the level as the default of 7. The MEL field in the protocol packets is used to detect if the current packet can pass by.	
Example	Configure the level of R-APS channel of ERPS ring1 instance1 as 5. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)raps-mel 5	

8.2.18 control-vlan

Command	**control-vlan <vlan-id>** **no control-vlan**	
parameter	**vlan-id**	vlan id of R-APS packets, range is from 2 to 4094
default	Do not configure any control vlan	
Mode	ERPS Instance Configuration Mode	
Usage Guide	Configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. The no command deletes the control vlan.	

Example

Configure the control vlan of ERPS ring1 instance1 as vlan10.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)control-vlan 10
```

8.2.19 forced-switch

Command

forced-switch {port0 | port1}

parameter

port0	means to run the forced switch configuration on port0 of the ring node
port1	means to run the forced switch configuration on port1 of the ring node

default

No forced switch in ERPS ring instance

Mode

ERPS Instance Configuration Mode

Usage Guide

Run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting.

If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node;

If this instance configuration is not integral, it is on the status of unactive, there will be the message of "The request is rejected because the ERP instance in unactive state!" otherwise, enter into the next step;

Example

Run the forced switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#force-switch port0
```

8.2.20 manual-switch

Command

manual-switch {port0 | port1}

parameter

port0	means to run the manual switch configuration on port0 of the ring node
port1	means to run the manual switch configuration on port1 of the ring node

default

No manual switch in ERPS ring instance

Mode

ERPS Instance Configuration Mode

Usage Guide

Run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance.

If this instance configuration is not integral, it is on the status of unactive, there will be the message of "The request is rejected because the ERP instance in unactive state!" otherwise,

enter into the next step;

Example

Run the manual switch configuration on the port0 of ERPS ring1 instance1.

```
Switch(config)#erps-ring ring1
Switch(config-erps-ring)#erps-instance 1
Switch(config-erps-ring-inst-1)#manual-switch port0
```

8.2.21 clear command

Command	**clear command**
parameter	-
default	No clear command in ERPS ring instance.
Mode	ERPS Instance Configuration Mode
Usage Guide	Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery. If the forced or manual switch command has existed on the node of this ring instance, clear the switch command and keep the block status of the data channel and R-APS channel of the blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the higher level request happens on the ring (such as SF); If the local forced or manual switch has existed on the node of this ring instance, clear the command and then receive the R-APS (NR) packets whose node ID is larger than the local node ID. Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports.
Example	Run clear configuration on ERPS ring1 instance1. Switch(config)#erps-ring ring1 Switch(config-erps-ring)#erps-instance 1 Switch(config-erps-ring-inst-1)#clear command

8.2.22 show erps ring

Command	**show erps ring {<ring-name> | brief}**	
parameter	**ring-name**	ERPS ring name
	brief	Show the ERPS ring main information
default	-	
Mode	Admin Mode	
Usage Guide	Read the ERPS ring information.	

Example

show all the ERPS rings information.

```
Switch#show erps ring brief
ethernet tcn-propagation erps to none.
Ring-Name                                                              Ring-topo
Port0            Port1            Version    Inst-Coun
t
------------------------------------------------------------------------------------
------------
--
ring1                                                              major-ring      -
-                V2          0
```

8.2.23 show erps instance

Command	**show erps instance [ring <ring-name> [instance <instance-id>]]**	
parameter	**ring-name**	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances information.
default	-	
Mode	Admin Mode	
Usage Guide	Show the ERPS ring instance information.	

Example

Show all the ERPS ring instances information.

```
Switch#show erps instance
ERPS Ring: 1
  Instance: 1
  Description: -
  Protected Instance: -
  Revertive mode: revertive
  R-APS MEL: 7
```

```
R-APS Virtual-Channel: with
Control Vlan: -
Ring ID: 1
Guard Timer(10ms): 50
Holdoff Timer(seconds): 0
WTR Timer(min): 5
------------------------------------------
Port        Role                 Port-Status
------------------------------------------
Port0       common                 blocked
Port1       common                 blocked
```

Display content	analyze
Description	ERPS ring instance name
Protected Instance	MSTP instance protected by ERPS ring instance
Revertive mode	ERPS ring link mode: revertive, non-revertive
R-APS MEL	Level of R-APS channel, package R-APS packets
R-APS Virtual-Channel	If the ERPS ring is the sub ring, the R-APS virtual channel of the inherited ring: with, without
Ring ID	The ring-id number carried by the packets sent by ERPS ring instance, range is from 1 to 64.
Contral Vlan	R-APS channel vlan, package R-APS packet of tag
WTR_Timer	Wait to Restore timer, range is from 1 to 12min
Guard_Timer	Guard timer, range is from 10ms to 2s
Holdoff_Timer	Holdoff timer, range is from 0 to 10
Port	ERPS ring port information: port0, port1
Role	ERPS ring node roles: RPL Owner, RPL neighbor, Common
Port-Status	Blocked: port is in block status forwarding: port is in forwarding status

8.2.24 show erps status

Command

show erps status [ring <ring-name> [instance <instance-id>]]

parameter

ring-name	ERPS ring name
instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show all the ERPS ring instances status information.

default

-

Mode

Admin Mode

Usage Guide

Show the status information of ERPS ring instance.

Example

Show all the ERPS ring instances status information.

```
Switch#show erps status
ERPS ring: 1 instance: 1 status:
Active: 0
Node State: -
Time last topology change:Jan 00 00:00:00 1900
-------------------------------------------------------------------------------
Port        Interface          Port-Status      Signal-Status      R-APS-NodeId
BPR
-------------------------------------------------------------------------------
Port0    -              -              -               -                     -
Port1    -              -              -               -                     -

ERPS ring: 1 instance: 2 status:
Active: 0
Node State: -
Time last topology change:Jan 00 00:00:00 1900
-------------------------------------------------------------------------------
Port        Interface          Port-Status      Signal-Status      R-APS-NodeId
BPR
-------------------------------------------------------------------------------
Port0    -              -              -               -                     -
Port1    -              -              -               -                     -
```

Display content	analyze

Active	Current active status of ERPS ring instance: 1, 0
Node State	Current status of ERPS ring instance: Idle, Protection, Forced-switch, Manual-switch, Pending
Time last topology change	Topology switching last time
Port-Status	Blocked: the port is in block status Forwarding: the port is in forwarding status
Signal-Status	ERPS ring port fault status: Non-failed: no fault Failed: fault happened
R-APS-NodeId	The node ID information is the last bit of the MAC address
BPR	The block link information carried by the receiving last R-APS saved by ERPS ring port, it is port0 or port1 which was blocked.

8.2.25 show erps statistics

Command

show erps statistics [ring <ring-name> [instance <instance-id>]]

parameter

ring-name	ERPS ring name
instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, show the statistic information of all the ERPS ring instances of this device.

default

-

Mode

Admin Mode

Usage Guide

Show the statistic information of ERPS ring instance.

Example

Show the statistic information of ERPS ring instance.

```
Switch#show erps statistics
Statistics for ERPS ring: 1 instance 1:
R-APS     Port0(Tx/Rx)                Port1(Tx/Rx)
-----------------------------------------------------------
```

```
NR:        0             /0                 0            /0
NR,RB:    0             /0                 0            /0
SF:        0             /0                 0            /0
MS:        0             /0                 0            /0
FS:        0             /0                 0            /0
EVENT:    0             /0                 0            /0
---------------------------------------------------------
TOTAL:    0             /0                 0            /0

Statistics for ERPS ring: 1 instance 2:
R-APS     Port0(Tx/Rx)                 Port1(Tx/Rx)
---------------------------------------------------------
NR:        0             /0                 0            /0
NR,RB:    0             /0                 0            /0
SF:        0             /0                 0            /0
MS:        0             /0                 0            /0
FS:        0             /0                 0            /0
EVENT:    0             /0                 0            /0
---------------------------------------------------------
TOTAL:    0             /0                 0            /0
```

8.2.26 clear erps statistics

Command	**clear erps statistics [ring <ring-name> [instance <instance-id>]]**	
parameter	**ring-name**	ERPS ring name
	instance-id	ID of ERPS ring instance, range is from 1 to 48. If it is not appointed, clear the statistic information of all the ERPS ring instances of this device
default	-	
Mode	Admin Mode	
Usage Guide	Clear the statistic information of ERPS.	
Example	Clear the statistic information of ERPS ring1 instance1. Switch#clear erps statistics ring 1 instance 1	

Chapter 9 QOS and Flow-based Redirection

9.1 QOS

9.1.1 accounting

Syntax	Accounting no accounting
Parameter	none
Default	Do not set statistic function.
Mode	Policy map configuration mode
Usage	Set statistic function for the classified traffic. After enable this function, add statistic function to the traffic of the policy class map, the messages can only red or green when passing policy. When print statistic information, in packets means classify packets numbers and not support the classify of color.
Example	Count the packets which satisfy c1 rule. Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#accounting Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit Switch(config)#

9.1.2 class

Syntax	class <class-map-name> [insert-before <class-map-name>] no class <class-map-name>	
Parameter	<class-map-name>	<class-map-name> is the class map name used by the class.
	insert-before <class-map-name>	insert-before <class-map-name> insert a new configured class to the front of a existent class to improve the priority of the new class.
Default	No policy class is configured by default.	

Mode	Policy map configuration mode
Usage	Associates a class to a policy map and enters the policy class map mode; the no command deletes the specified class. Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and nexthop configuration can be performed on packet traffic classified by class map.
Example	After add a policy class map c1 to the policy map, add a policy class map c2 and insert it to the front of c1. Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#class-map c2 Switch(config-classmap-c2)#exit Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#class c2 insert-before c1 Switch(config-policymap-p1-class-c2)#exit

9.1.3 class-map

Syntax	class-map <class-map-name> no class-map <class-map-name>	
Parameter	<class-map-name>	class map name
Default	No class map is configured by default.	
Mode	Global Mode	
Usage	Creates a class map and enters class map mode; the no command deletes the specified class map.	
Example	Creating and then deleting a class map named “c1”. Switch#config Switch(config)#class-map c1 Switch(config-classmap-c1)#exit Switch(config)#no class-map c1	

9.1.4 clear mls qos statistics

Syntax	clear mls qos statistics (interface [ethernet] <interface-name>) | (vlan <vlan-id>)	
Parameter	<vlan-id>	VLAN ID
	<interface-name>	interface name
Default	Do not set action.	
Mode	Admin Mode	
Usage	Clear accounting data of the specified ports or VLAN Policy Map. If there are no parameters, clear accounting data of all policy map.	
Example	Clear the Policy Map statistic of VLAN 100. Switch#clear mls qos statistics vlan 100	

9.1.5 drop

Syntax	drop no drop
Parameter	none
Default	None
Mode	Policy class map configuration mode
Usage	Drop the specified packet after configure this command.
Example	Drop the packet which satisfy c1. Switch#config Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#drop Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit

9.1.6 match

Syntax	match (access-group <acl-index-or-name> | ip dscp <dscp-list> | ip precedence <ip-precedence-list> | ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list>) no match {access-group | ip dscp | ip precedence| ipv6 access-group| ipv6 dscp | ipv6 flowlabel | vlan | cos)	
Parameter	<acl-index-or-name>	match specified IP ACL, MAC ACL or IPv6 standard ACL or MAC-IP ACL, the parameters are the number or name of the ACL;
	<dscp-list>	match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the range is 0~63;
	<ip-precedence-list>	match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0~7;
	ipv6 access-group <acl-index-or-name>	match specified IPv6 ACL, the parameter is the number or name of the IPv6 ACL;
	<flowlabel-list>	match specified IPv6 flow label, the parameter is IPv6 flow label value, the range is 0~1048575;
	<vlan-list>	match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the range is 1~4094;
	<cos-list>	match specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS, the range is 0~7;
Default	No match standard by default	
Mode	Class-map Mode	
Usage	Configure the match standard of the class map; the no form of this command deletes the specified match standard. Only one match standard can be configured in a class map. When configuring the match ACL, permit rule as the match option, apply Policy Map action. Deny rule as the excluding option, do not apply Policy Map action. (The deny rule is not supported issuing in PBR, please pay attention to avoid it.) If configure another match rule after one was configured, the operation fails, but configure the same match rule will cover the previous.	
Example	Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0. Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit	

9.1.7 mls qos aggregate-policy

Syntax	mls qos aggregate-policy <policer_name> <bits_per_second> burst-group <normal_burst_bytes> no mls qos aggregate-policy <policer_name>	
Parameter	<policer_name>	it is the aggregate policy name.
	<bits_per_second>	it define the information rate, namely CIR, the unit is kbit per second, and it ranges from 1 to 10000000;
	<normal_burst_bytes>	it define the committed burst size, namely CBS, the unit is kilobyte, and it ranges from 1 to 8192, when the CBS more than the maximum of chips , it uses the biggest value that chip support to set hardware, CLI have not notice information;
Default	The default is no policy action.	
Mode	Global Mode	
Usage	Define a aggregate policy command. The no command delete mode configuration. It only supports single cylinder configuration, when configuring, if configured CBS, not support configure color, green packets only supports transmit, red packets only supports drop.	
Example	Set 10000 as CIR, CBS is 512. Switch (config)#policy burst 1 512 Switch(config)# mls qos aggregate-policy 1 1000 burst-group 1	

9.1.8 mls qos cos

Syntax	mls qos cos <default-cos> no mls qos cos	
Parameter	<default-cos>	default CoS value for the port, the valid range is 0 to 7
Default	The default CoS value is 0	
Mode	Port Configuration Mode	
Usage	Configures the default CoS value of the port; the “no mls qos cos” command restores the default setting. Configure the default CoS value for switch port. In default configuration, the message ingress cos from this port are default value whether the message with tag. If the message without tag, the message cos value for tag is enactmented.	
Example	Setting the default CoS value of ethernet port 1/0/1 to 7, i.e., packets coming in through this port will be assigned a default CoS value of 7 if no CoS value present . Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos cos 7	

9.1.9 mls qos map

Syntax

mls qos map (cos-intp <intp1…intp8> | cos-dp <dp1…dp8> | dscp-intp <in-dscp list> to <intp> | dscp-dp <in-dscp list> to <dp> | dscp-dscp <in-dscp list> to <out-dscp>)

no mls qos map (cos-intp | cos-dp | dscp-intp | dscp-dp | dscp-dscp)

Parameter

cos-intp <intp1…intp8>	defines the mapping from CoS to intp (queue) value, <intp1..intp8> are 8 intp value corresponding to the 0 to 7 CoS value, each intp value is delimited with space, ranging from 0 to 7;
cos-dp<dp1…dp8>	defines the mapping from cos to intp (queue), <dp1…dp8> is 8 drop priority and it corresponding to the Cos value from 0 to 7, every drop priority is separated by space, and it ranges from 0 to 2;
dscp-intp	defines the mapping from DSCP to intp (queue).
dscp-dp	defines the mapping from dscp to drop priority.
dscp-dscp	defines the mapping from entrance dscp to export dscp, <in-dscp list> is the input dscp value, the most is 8 and it separated by space from each other, and it ranges from 0 to 63, <out-dscp> is output dscp value and it ranges from 0 to 63.

Default

Default mapping values are:

Default CoS-TO-INTP Map

COS:	0	1	2	3	4	5	6	7
INTP:	0	1	2	3	4	5	6	7

Default CoS-TO-DP Map

CoS	0	1	2	3	4	5	6	7
DP	0	0	0	0	0	0	0	0

Default DSCP-TO-INTP Map

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

Default DSCP-TO-DP Map

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	0	0
1:	0	0	0	0	0	0	0	0	0	0
2:	0	0	0	0	0	0	0	0	0	0

```
3:      0   0   0   0   0   0   0   0   0   0
4:      0   0   0   0   0   0   0   0   0   0
5:      0   0   0   0   0   0   0   0   0   0
6:      0   0   0   0
Default DSCP-TO-DSCP Map
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:      0   1   2   3   4   5   6   7   8   9
1:      10  11  12  13  14  15  16  17  18  19
2:      20  21  22  23  24  25  26  27  28  29
3:      30  31  32  33  34  35  36  37  38  39
4:      40  41  42  43  44  45  46  47  48  49
5:      50  51  52  53  54  55  56  57  58  59
6:      60  61  62  63
```

Mode	Global Mode
Usage	INTP means the chip internal priority setting. Because of the internal DSCP value have 64 and the chip internal priority (queue) only 8, the dscp-intp mapping need 8 continuum internal dscp mapping to the same INTP.
Example	Setting the CoS-to-INTP mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7。 Switch(config)#mls qos map cos-intp 0 1 2 3 4 5 6 7

9.1.10 mls qos queue algorithm

Syntax	mls qos queue algorithm (sp | wrr | wdrr) no mls qos queue algorithm	
Parameter	sp	The strict priority, the queue number of bigger, then the priority is higher
	wrr	Select wrr algorithm
	wdrr	Select wdrr algorithm.
Default	WRR	
Mode	Port Configuration Mode	
Usage	After configure this command, the queue management algorithm is set.	
Example	Setting the queue management algorithm as sp. switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mls qos queue algorithm sp	

9.1.11 mls qos queue wdrr weight

Syntax	mls qos queue wdrr weight <weight1..weight8> no mls qos queue wdrr weight	
Parameter	<weight1..weight8>	defines the queue weight, in Kbytes. For WDRR algorithm, this configuration is valid, but for SP algorithm, it is invalid. When the weight is 0, this queue adopts SP algorithm to manage, and WDRR algorithm turns into SP+WDRR algorithm. range:0-32767
Default	The queue weight is 10 20 40 80 160 320 640 1280.	
Mode	Port Configuration Mode	
Usage	If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWDRR. When removing the queue, the system will manage SP queue at first, then manage WDRR queue, SP queue executes the strict priority management mode, WDRR queue executes the weight rotation management mode.	
Example	Configure the queue weight as 10 10 20 20 40 40 80 80. Switch(interface-ethernet1/0/1)#mls qos queue wdrr weight 10 10 20 20 40 40 80 80	

9.1.12 mls qos queue wrr weight

Syntax	mls qos queue wrr weight <weight1..weight8> no mls qos queue wrr weight	
Parameter	<weight1..weight8>	defines the queue weight, range: 0-127
Default	The queue weight is 1 2 3 4 5 6 7 8。	
Mode	Port Configuration Mode	
Usage	If the queue weight is configured as 0, it uses SP algorithm to manage, while WRR turns into SWDRR. When removing the queue, the system will manage SP queue at first, then manage WDRR queue, SP queue executes the strict priority management mode, WDRR queue executes the weight rotation management mode.	
Example	Configure the queue weight as 127 8 9 6 3 4 2 0。 Switch(interface-ethernet1/0/1)#mls qos queue wrr weight 127 8 9 6 3 4 2 0	

9.1.13 mls qos queue bandwidth

Syntax	mls qos queue <queue-id> bandwidth <maximum-bandwidth> no mls qos queue <queue-id> bandwidth	
Parameter	<queue-id>	queue ID to configure the bandwidth guarantee, the different chip supports the different queue count, the range is different too, and the ranging from 1 to 8.
	<maximum-bandwidth>	maximum-bandwidth, ranging from 0 to 128000, when input 0, it means the max-bandwidth function is not take effect. The minimum-bandwidth must not bigger than maximum-bandwidth.
Default	The queue bandwidth have no guarantee	
Mode	Port Configuration Mode	
Usage	The minimum-bandwidth guarantee and maximum-bandwidth limit can be configured at the different or same queue. The queue bandwidth pledge for egress is relative to management mode, for example: one port is the strict priority-queue, the highest priority is queue 8 now, it will satisfy this queue traffic when block is happened. But if user want the lower priority of queue having bandwidth, it can remain bandwidth via this command, the lower priority queue's minimum-bandwidth will be satisfied at first, then the excess bandwidth is managed according to SP.	
Example	Configure the maximum-bandwidth is 128kbps for ethernet1/0/2 queue1. Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# mls qos queue 1 bandwidth 128	

9.1.14 mls qos trust

Syntax	mls qos trust (cos | dscp) no mls qos trust (cos | dscp)	
Parameter	dscp	configures the port to trust DSCP status
	cos	configures the COS port to trust status.
Default	the default is trust COS value.	
Mode	Port Configuration Mode	
Usage	Configures the current port trust; the no command disables the current trust status of the port. trust dscp mode: Set the intp field based dscp-to-intp mapping. trust cos mode: Set the intp field based cos-to-intp mapping.	
Example	Set trust dscp of port 1/0/1, not trust cos. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ehternet1/1)# mls qos trust dscp Switch(config-if-ehternet1/1)#no mls qos trust cos	

9.1.15 Policy burst

Syntax	policy burst <burst_group> <normal_burst_bytes>	
Parameter	<burst_group>	burst_group id ranges from 1 to 2
	<normal_burst_bytes>	The committed burst size – CBS (Committed Burst Size), in byte, ranging from 1 to 8192. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;
Default	The default of normal_burst_bytes is 1024.	
Mode	Global Mode	
Usage	Configure burst-group in global mode and it supports 2 burst-group, then it can use burst-group in strategy classify table mode. It can return default configuration by set 1024 as default value.	
Example	Set burst-group 1 to define CBS as 512 bits Switch(config)#policy burst 1 512	

9.1.16 Policy

Syntax	policy <bits_per_second> burst-group <burst-group-id> no policy	
Parameter	<bits_per_second>	The committed information rate – CIR (Committed Information Rate), in Kbps, ranging from 1 to 10000000;
	<burst-group-id>	It is CBS burst-group id and it ranges from 1 to 2.
Default	No policy action.	
Mode	Policy class map configuration mode	
Usage	Support non-aggregate policy command of double color, the no command delete mode configuration. Configure information rate in policy class map configuration mode. Not support the color configuration and the default green packets is transmit, red packets drop.	
Example	Set information rate 1000 in policy class map configuration mode, the CBS is 512, the more than cir rate will send and do nothing for packets. Switch(config)#policy burst 1 512 Switch(config)#class-map cm Switch(config-classmap-cm)#match cos 0 Switch(config-classmap-cm)#exit Switch(config)#policy-map 1 Switch(config-policymap-1)#class cm Switch(config-policymap-1-class-cm)# policy 1000 burst-group 1	

9.1.17 Policy aggregate

Syntax	policy aggregate <aggregate-policy-name> no policy aggregate <aggregate-policy-name>
Parameter	<aggregate-policy-name> <aggregate-policy-name> is the policy set name.
Default	No policy is configured by default
Mode	Policy class map configuration mode
Usage	Police Map reference aggregate policy, applies an aggregate policy to classified traffic; the no command deletes the specified aggregate policy. The same policy set can be referred to by different policy class maps.
Example	Create class-map, the match rule is the cos value is 0; policy-map is 1, enter the policy map mode, set the Policy and choose the color policy for the current list. Switch(config)#class-map cm Switch(config-classmap-cm)#match cos 0 Switch(config-classmap-cm)#exit Switch(config)#policy-map 1 Switch(config-policymap-1)#class cm Switch(config-policymap-1-class-cm)#policy aggregate color

9.1.18 Policy-map

Syntax	policy-map <policy-map-name> no policy-map <policy-map-name>
Parameter	<policy-map-name> policy map name.
Default	No policy map is configured by default.
Mode	Global Mode
Usage	Creates a policy map and enters the policy map mode; the "no policy-map <policy-map-name>" command deletes the specified policy map. Policy class map opertion can be done in policy map configuration mode.
Example	Creating and deleting a policy map named "p1". 。 Switch(config)#policy-map p1 Switch(config-policymap-p1)#exit Switch(config)#no policy-map p1

9.1.19 service-policy input

Syntax	service-policy input <policy-map-name> no service-policy input {<policy-map-name>}	
Parameter	input <policy-map-name>	input <policy-map-name> applies the specified policy map to the ingress direction of switch port. no command will delete all the policy maps applied on the ingress direction of the port if there is not the specified policy map name.
Default	No policy map is bound to port by default.	
Mode	Port Configuration Mode	
Usage	Applies a policy map to the specified port; the no command deletes the specified policy map applied to the port or deletes all the policy maps applied on the ingress direction of the port . Only one policy map can be applied to each direction of each port or VLAN interface.	
Example	Bind policy p1 to ingress Ethernet port1/1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#service-policy input p1	

9.1.20 service-policy input vlan

Syntax	service-policy input <policy-map-name> vlan <vlan-list> no service-policy input {<policy-map-name>} vlan < vlan-list>	
Parameter	input <policy-map-name>	input <policy-map-name> applies the specified policy map to the ingress direction of switch VLAN interface.
	vlan < vlan-list>	vlan <vlan-list> the vlan list of binding policy map.
Default	No policy map is bound to VLAN interface by default.	
Mode	Global Mode	
Usage	Applies a policy map to the specified VLAN interface; the no command deletes the specified policy map applied to the VLAN interface or deletes all the policy maps applied in the ingress direction of the vlan interface . Only one policy map can be applied to each direction of each port or VLAN interface. 。	
Example	Bind policy p1 to ingress of VLAN interface 2-4,6 Switch(config)#service-policy input p1 vlan 2-4;6	

9.1.21 set

Syntax	set (ip dscp <new-dscp> | ip precedence <new-precedence> | internal priority <new-inp> | drop precedence <new-dp> | cos <new-cos>) no set (ip dscp | ip precedence | internal priority | drop precedence | cos)	
Parameter	ip dscp <new-dscp>	new DSCP value, do not distinguish v4 and v6.
	ip precedence <new-precedence>	new IP Precedence.
	cos <new-cos>	new IP Precedence.
Default	Not assigning by default.	
Mode	Policy Class-map Mode	
Usage	Assign a new DSCP, IP Precedence for the classified traffic; the no form of this command delete assigning the new values. Only the classified traffic which matches the matching standard will be assigned with the new values.	
Example	Set the IP Precedence of the packets matching c1 class rule to 3. Switch(config)#policy-map p1 Switch(Config-PolicyMap-p1)#class c1 Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3 Switch(Config-PolicyMap-p1-Class-c1)#exit Switch(Config-PolicyMap-p1)#exit	

9.1.22 show class-map

Syntax	show class-map [<class-map-name>]	
Parameter	[<class-map-name>]	class map name
Default	None	
Mode	Admin Mode.	
Usage	Displays all configured class-map or specified class-map information.	
Example	Switch#show class-map Class map name:cm, used by 1 time(s) match cos: 0 Class map name:color, used by 0 time(s)	

```
match cos: 0
```

Displayed information	Explanation
Class map name:c1	Name of the Class map
used by 1 times	Used times
match acl name:1	Classifying rule for the class map

9.1.23 show policy-map

Syntax	show policy-map [<policy-map-name>]
Parameter	<policy-map-name> policy map name
Default	None
Mode	Admin Mode.
Usage	Displays all configured policy-map or specified policy-map information.

Example

```
Switch#show policy-map
Policy Map 1, used by 0 time(s)
  Class Map name: cm

Policy Map p1, used by 0 time(s)
  Class Map name: c1
    drop
    set ip precedence 3
        policy CIR: 2000 CBS: 512
    conform-action:
     transmit
    exceed-action:
     drop
```

Displayed information	Explanation
Policy map name:c1	Name of policy map
Class Map name: c1	Class Map name
policy 20000 512	Policy implemented
used by 0 port	Number of port that use the policy

9.1.24 show mls qos interface

Syntax

show mls qos {interface [<interface-id>] [policy | queuing] | vlan <vlan-id>} | [begin | include | exclude <regular-expression>]

Parameter

<interface-id>	port ID
<vlan-id>	VLAN ID
<regular-expression>	Regular expression

Default

None

Mode

Admin Mode.

Usage

Displays QoS configuration information on a port.

There is only red or green when packets passing police. In the print information, in packets means classify packets numbers and not supports the statistic information of color.

Example

```
Switch#show mls qos interface ethernet 1/0/1
Ethernet1/0/1:
Default COS: 0
Trust: DSCP
Attached Policy Map for Ingress: p1

Egress Internal-Priority-TO-Queue map:
INTP:   0    1    2    3    4    5    6    7
  -----------------------------------------
Queue:  0    1    2    3    4    5    6    7

Queue Algorithm: WRR
Queue weights:
Queue       1      2      3      4      5      6      7      8
  ------------------------------------------------------
WrrWeight   1      2      3      4      5      6      7      8
WdrrWeight 10     10     20     20     40     40     80     80

Bandwidth Guarantee Configuration:
Queue     1        2        3        4        5        6        7        8
  ------------------------------------------------------------------
MinBW(K) 0        0        0        0        0        0        0        0
MaxBW(K) 0        0        0        0        0        0        0        0
```

Displayed information	Explanation

Ethernet1/0/1	Port name
default cos:0	Default CoS value of the port
Trust: COS	The trust state of the port
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap. If there is no Accounting for Class Map, show NA
in-profile	Total in-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
out-profile	Total out-profile data packets match this ClassMap. If there is no Accounting for Class Map, show NA
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR，WDDR or PQ queue out method
Queue weights	Queue weights Configuration
Bandwidth Guarantee Configuration	Bandwidth Guarantee Configuration

```
Switch(config)#show mls qos interface ethernet 1/0/1 queuing
Ethernet1/0/1:

Egress Internal-Priority-TO-Queue map:
INTP:   0    1    2    3    4    5    6    7
  ----------------------------------------
Queue:  0    1    2    3    4    5    6    7

Queue Algorithm: WRR
Queue weights:
Queue         1      2      3      4      5      6      7      8
  ----------------------------------------------------
WrrWeight    1      2      3      4      5      6      7      8
WdrrWeight  10     10     20     20     40     40     80     80

Bandwidth Guarantee Configuration:
Queue      1         2         3         4         5         6         7         8
  ----------------------------------------------------------------
MinBW(K)   0         0         0         0         0         0         0         0
MaxBW(K)   0         0         0         0         0         0         0         0
```

Displayed information	Explanation
Internal-Priority-TO-Queue map::	Internal-Priority to queue mapping
Queue Algorithm:	WRR, WDDR or PQ queue out method
Queue weights	Queue weights configuration
Bandwidth Guarantee Configuration	Bandwidth Guarantee Configuration

```
Switch # show mls qos interface ethernet 1/0/1 policy
Ethernet1/0/1:
Attached Policy Map for Ingress: p1
```

Displayed information	Explanation
Ethernet1/0/1	Port name
Attached Policy Map for Ingress: p1	Policy name bound to port
ClassMap	ClassMap name
classified	Total data packets match this ClassMap.
in-profile	Total in-profile data packets match this ClassMap.
out-profile	Total out-profile data packets match this ClassMap.

9.1.25 show mls qos

Syntax	show mls qos in (interface <interface-name> policy) | (vlan <vlan-id>)	
Parameter	<interface-name>	port name.
	<vlan-id>	VLAN ID
Default	None	
Mode	Admin Mode.	
Usage	Show the policy configuration information of the in direction of port or vlan. Show the policy configuration information of the in direction.	
Example	Show the policy configuration information of the in direction. Switch#show mls qos in interface ethernet1/0/1 policy Ethernet1/0/1: Attached Policy Map for Ingress: p1	

9.1.26 show mls qos maps

Syntax

show mls qos maps [cos-intp | cos-dp | dscp-intp | dscp-dp | dscp-dscp] | [begin | include | exclude <regular-expression>]

Parameter

cos-intp	The mapping from ingress L2 CoS to internal priority
cos-dp	The mapping from ingress L2 CoS to drop priority
dscp-intp	The mapping from ingress DSCP to internal priority
dscp-dp	The mapping from ingress DSCP to drop priority
dscp-dscp	The mapping from outgress internal to DSCP priority

Default

None

Mode

Admin and Configuration Mode.

Usage

Display the map configuration information of QoS.

Example

Display configuration information of the mapping table.

```
Switch#show mls qos maps


Ingress COS-TO-Internal-Priority map:
COS:   0    1    2    3    4    5    6    7
  ----------------------------------------
INTP: 0    1    2    3    4    5    6    7



Ingress DSCP-TO-Internal-Priority map:
d1 : d2   0    1    2    3    4    5    6    7    8    9
0:         7    1    7    7    7    0    7    7    7    1
1:         1    1    1    1    1    1    2    1    2    2
2:         2    2    2    2    3    1    3    3    3    3
3:         3    3    4    1    4    4    4    4    4    4
4:         5    1    5    5    5    5    5    5    6    1
5:         6    6    6    6    6    6    7    1    7    7
6:         7    7    7    7



Ingress COS-TO-Drop-Precedence map:
COS:   0    1    2    3    4    5    6    7
  ----------------------------------------
DP:    0    0    0    0    0    0    0    0
```

```
Ingress DSCP-TO-DSCP map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:        0   1   2   3   4   5   6   7   8   9
1:       10  11  12  13  14  15  16  17  18  19
2:       20  21  22  23  24  25  26  27  28  29
3:       30  31  32  33  34  35  36  37  38  39
4:       40  41  42  43  44  45  46  47  48  49
5:       50  51  52  53  54  55  56  57  58  59
6:       60  61  62  63


Ingress DSCP-TO-Drop-Precedence map:
d1 : d2  0   1   2   3   4   5   6   7   8   9
0:        0   0   0   0   0   0   0   0   0   0
1:        0   0   0   0   0   0   0   0   0   0
2:        0   0   0   0   0   0   0   0   0   0
3:        0   0   0   0   0   0   0   0   0   0
4:        0   0   0   0   0   0   0   0   0   0
5:        0   0   0   0   0   0   0   0   0   0
6:        0   0   0   0
```

9.1.27 show mls qos vlan

Syntax	show mls qos vlan <v-id>	
Parameter	<v-id>	VLAN ID
Default	None	
Mode	Admin Mode.	
Usage	Display configuration information of the QOS VLAN.	

Example

```
Switch#show mls qos vlan 1
Vlan 1:
Attached Policy Map for Ingress: 1
Classmap classified(in packets)
c1 0
Rule ID classified(in packets)
```

9.1.28 show mls qos aggregate-policy

Syntax	show mls qos aggregate-policy [<aggregate-policy-name>]
Parameter	<aggregate-policy-name> aggregate policy name
Default	None
Mode	Admin mode and configuration mode.
Usage	Display all configured aggregate-policy or appointed aggregate-policy information.
Example	Switch#show mls qos aggregate-policy a2 aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop Not used by any policy map

Displayed information	Explanation
aggregate policy a2 CIR: 1000 CBS: 1024 conform-action: transmit exceed-action: drop	The configuration of aggregate policy.
Not used by any Policy Map	The referenced times of aggregate policy.

9.1.29 transmit

Syntax	transmit no transmit
Parameter	none
Default	Do not set the action.
Mode	Policy class map configuration mode
Usage	Send the packet directly after configure this command.
Example	Send the packet which satisfy c1. Switch#config Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#transmit Switch(config-policymap-p1-class-c1)#exit Switch(config-policymap-p1)#exit

9.1.30 access-group redirect to interface Ethernet

Syntax	access-group <aclname> redirect to interface [ethernet] <IFNAME> no access-group <aclname> redirect	
Parameter	<aclname>	name of the flow , only supports digital standard IP ACL, digital extensive IP ACL, nomenclatural standard IP ACL, nomenclatural extensive IP ACL, digital standard MAC ACL, digital extensive MAC ACL, nomenclatural standard MAC ACL, nomenclatual extensive MAC, digital standard IPv6 ACL, and nomenclatural standard IPv6 ACL. Parameters of Timerange and Portrange cannot be set in ACL; the type of ACL should be Permit.
	<IFNAME>	<IFNAME> the destination port of redirection
Default	None	
Mode	Port Configuration Mode	
Usage	Specify flow-based redirection; “no access-group <aclname> redirect” command is used to delete flow-based redirection. Flow-based redirection function enables the switch to transmit the data frames meeting some special condition to another specified port. Notice: Redirect does not support redirect flow to the port.	
Example	Redirecting the frames whose source IP is 192.168.1.111 received from port 1 to port 6 Switch(config)#access-list 1 permit host 192.168.1.111 Switch(config)# interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#access-group 1 redirect to interface ethernet 1/0/6	

9.1.31 show flow-based-redirect

Syntax	show flow-based-redirect [interface [ethernet] <IFNAME>]	
Parameter	<IFNAME>	display the information of the flow-based redirection configured in the ports listed in the interface-list.
Default	none	
Mode	Admin Mode and Configuration Mode.	
Usage	This command is used to display the information of current flow-based redirection in the system/port	
Example	Switch(config)#show flow-based-redirect Flow-based-redirect config on interface Ethernet1/0/1: RX flow (access-list 1) is redirected to interface Ethernet1/0/6	

9.1.32 add

Syntax	add s-vid <new-vid> no add s-vid	
Parameter	s-vid <new-vid>	s-vid <new-vid> appointed VID of tunnel VLAN Tag.
Default	The default is not add tag.	
Mode	Policy classify table configuration mode	
Usage	Add specified tunnel tag for data packets of mapped classify table, the no command cancel configuration. After configured the command, add appointed tunnel tag or inner tag for packets of mapping classify table. When use QinQ function, the data packets that sent only have inner VLAN Tag or no Tag, it needs add s-vid commands to add appointed tunnel VLAN Tag, otherwise data have not tunnel VLAN in switch.	
Example	Add a VLAN Tag that VID is 2 to satisfied c1 classify rule packets. Switch#config Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c1 Switch(config-policymap-p1-class-c1)#add s-vid 2	

9.1.33 match

Syntax	match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list>| ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <cos-list> }
	no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan | cos }}	

Parameter	access-group <acl-index-or-name>	match the specified IP ACL or MAC–IP ACL or standard IPV6 ACL, the parameters are the number or name of ACL
	ip dscp <dscp-list>	match the specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values, the ranging is 0 to 63
	ip precedence <ip-precedence-list>	match the specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0 to 7
	ipv6 access-group <acl-index-or-name>	match the specified IPv6 ACL, the parameter is the number or name of IPv6 ACL
	ipv6 flowlabel <flowlabel-list>	match the specified IPv6 flow label, the parameter is IPv6 flow label value, the ranging is 0 to 1048575

	vlan <vlan-list>	match the specified VLAN ID of the external VLAN Tag, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs, the ranging is 1 to 4094
	cos <cos-list>	match the specified CoS value, the parameter is a CoS list consisting of maximum 8 CoS values, the ranging is 0 to 7
Default	There is no match standard.	
Mode	Class-map Mode	
Usage	Configure the match standard of the class map; the no command deletes the specified match standard. Only one match standard can be configured in a class map. When configuring the ACL match, permit rule is the match option, it will apply Policy Map action. Deny rule is the excluding option, it does not apply Policy Map action. If it has been configured other match rule, the operation is failure, but configuring the same match rule will cover the previous.	
Example	Create a class-map named c1, and configure the class rule of the class-map to match packets with IP Precedence of 0. Switch(config)#class-map c1 Switch(config-classmap-c1)#match ip precedence 0 Switch(config-classmap-c1)#exit	

9.1.34 service-policy

Syntax	service-policy <policy-map-name> in no service-policy <policy-map-name> in	
Parameter	<policy-map-name>	The specified policy-map name of flexible QinQ
Default	No policy map is bound to port	
Mode	Port Configuration Mode	
Usage	Bind the specified policy of flexible QinQ to the ingress of the port, the no command cancels the binding. Only one policy map can be bound to each port, the function takes effect after the policy map is bound to a port. At present, do not support the configuration with add commend and delete command in policy.	
Example	Apply policy-map p1 (p1 corresponds with the action that modify s-vid) to Ethernet port 1/0/1 for flexible QinQ. Switch(config-if-ethernet1/0/1)#dot1q-tunnel enable Switch(config-if-ethernet1/0/1)#service-policy p1 in	

9.1.35 set

Syntax	set {s-vid <new-vid> | cos <cos-list> | drop-precedence <dp-list> | internal-priority <inp-list> | ip {dscp <dscp-list> | precedence <pri-list>} | s-tpid <tpid-list> }
	no set{s-vid | cos | drop-precedence | internal-priority | ip {dscp | precedence} | s-tpid }	

Parameter	<new-vid>	modify tunnel VID of VLAN Tag
	<cos-list>	modify cos value of packets
	<dp-list>	modify drop priority
	<inp-list>	modify inner priority
	<dscp-list> <pri-list>	modify ip dscp value or precedence value
	<tpid-list>	modify tunnel tpid value of packets
Default	Do not modify the value.	
Mode	Policy class map configuration mode	
Usage	Assign the new cos and vid value to the packets which match the class map, no command cancels the operation. Only modify the new value again for the classified flow that correspond the match standard.	
Example	Set an external VLAN Tag' VID as 3 for the packet which satisfy c2 class rule. Switch(config)#policy-map p1 Switch(config-policymap-p1)#class c2 Switch(config-policymap-p1-class-c2)#set s-vid 3 Switch(config-policymap-p1-class-c2)#exit	

Chapter 10 Layer 3 Interface and ARP

10.1 Layer 3 Interface

10.1.1 description

Command	**description <*text*>** **no description**	
parameter	***text***	is the description information of VLAN interface, the length should not exceed 256 characters
default	Do not configure	
Mode	VLAN interface mode	
Usage Guide	The description information of VLAN interface behind description and shown under the configured VLAN.	
Example	Configure the description information of VLAN interface as test vlan. Switch(config)#interface vlan 2 Switch(config-if-vlan2)#description test vlan	

10.1.2 interface vlan

Command	**interface vlan <*vlan-id*>** **no interface vlan <*vlan-id*>**	
parameter	***vlan-id***	is the VLAN ID of the established VLAN, ranging from 1 to 4094.
default	No Layer 3 interface is configured upon switch shipment.	
Mode	Global Mode	
Usage Guide	this command is used to create the 3-layer interface, no the command is used to delete the 3-layer interface.	
Example	Create a VLAN interface (layer 3 interface). Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#	

10.1.3 no interface IFNAME

Command	**no interface IFNAME**	
parameter	**IFNAME**	Interface Name
default	-	
Mode	Global mode	
Usage Guide	This command is used to delete the layer 3 interface. It can deal with the situation that the interface name is spelt in special way. IFNAME can match multiple ways, such as vlan1, Vlan1, v1, V1 and etc.	
Example	Delete interface vlan1. (config)# no interface vlan1	

10.1.4 show ip route

Command

show ip route [database]

parameter

database is database information.

default

-

Mode

Admin Mode

Usage Guide

Show kernal routing table, include: routing type, destination network, mask, next-hop address, interface, etc.

Example

shows the routing table.

```
Switch#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

C       127.0.0.0/8 is directly connected, Loopback    tag:0
Total routes are : 1 item(s)
```

Display information	describe
C –connected	Direct route, namely the segment directly connected with the layer 3 switch
S –static	Static route, the route manually configured by users
R - RIP derived	RIP route, acquired by layer 3 switch through the RIP protocol.
O - OSPF derived	OSPF route, acquired by layer 3 switch through the OSPF protocol
A- OSPF ASE	Route introduced by OSPF
B- BGP derived	BGP route, acquired by the BGP protocol.

10.2 IPv4/v6 configuration

10.2.1 clear ip traffic

Command	**clear ip traffic**
parameter	-
default	-
Mode	Admin Mode.
Usage Guide	Clear the statistic information of receiving and sending packets for IP kernel protocol, including the statistic of receiving packets, sending packets and dropping packets and the error information of receiving and sending packets for IP protocol, ICMP protocol, TCP protocol and UDP protocol.
Example	Clear statistic information of IP protocol. Switch#clear ip traffic

10.2.2 clear ipv6 neighbor

Command	**clear ipv6 neighbors**
parameter	-
default	-
Mode	Admin Mode.
Usage Guide	This command can not clear static neighbor
Example	Clear neighbor list. Switch#clear ipv6 neighbors

10.2.3 ip address

Command	**ip address <*ip-address*> <*mask*> [secondary]** **no ip address [<*ip-address*> <*mask*>] [secondary]**	
parameter	***ip-address***	is IP address, dotted decimal notation;
	mask	is subnet mask, dotted decimal notation;
	secondary	indicates that the IP address is configured as secondary IP address.
default	The system default is no IP address configuration.	
Mode	VLAN interface configuration mode	
Usage Guide	This command configures IP address on VLAN interface manually. If optional parameter secondary is not configured, then it is configured as the primary IP address of VLAN interface; if optional parameter secondary is configured, then that means the IP address is the secondary IP address of VLAN. One VLAN interface can only have one primary IP address and more than one secondary IP addresses. Primary IP and Secondary IP all can be used on SNMP/Web/Telnet management. Furthermore, the switch also provides BOOTP/DHCP manner to get IP address.	
Example	The IP address of switch VLAN1 interface is set to 192.168.1.10/24. Switch(Config-if-Vlan1)#ip address 192.168.1.10 255.255.255.0	

10.2.4 ip default-gateway

Command	**ip default-gateway <A.B.C.D>** **no ip default-gateway <A.B.C.D>**	
parameter	**A.B.C.D**	is gateway address, for example 10.1.1.10.
default	There is no default gateway.	
Mode	Global mode.	
Usage Guide	Configure the default gateway of the router to specify the default next hop address to which the packets will be sent.	
Example	Specifies the default gateway.Switch(config)# ip default-gateway 10.1.1.10	

10.2.5 ipv6 address

Command	**ipv6 address <ipv6-address|prefix-length> [eui-64]** **no ipv6 address <ipv6-address|prefix-length> [eui-64]**	
parameter	**ipv6-address**	is the prefix of IPv6 address, parameter
	prefix-length	is the prefix length of IPv6 address, which is between 3-128
	eui-64	means IPv6 address is generated automatically based on eui64 interface identifier of the interface.
default	-	
Mode	Interface Configuration Mode	
Usage Guide	IPv6 address prefix cannot be multicast address or any other specific IPv6 address, and different layer 3 interfaces cannot configure the same address prefix. For global unicast address, the length of the prefix must be greater than or equal to 3. For site-local address and link-local address, the length of the prefix must be greater than or equal to 10.	
Example	Configure an IPv6 address on VLAN1 Layer 3 interface: the prefix is 2001:3f:ed8::99 and the length of the prefix is 64. Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64	

10.2.6 ipv6 nd dad attempts

Command	**ipv6 nd dad attempts <*value*>** **no ipv6 nd dad attempts**	
parameter	***value***	is the Neighbor Solicitation Message number sent in succession by Duplicate Address Detection and the value of <value> must be in 0-10, NO command restores to default value 1.
default	The default request message number is 1	
Mode	Interface Configuration Mode	
Usage Guide	When configuring an IPv6 address, it is required to process IPv6 Duplicate Address Detection, this command is used to configure the ND message number of Duplicate Address Detection to be sent, value being 0 means no Duplicate Address Detection is executed.	
Example	The Neighbor Solicitation Message number sent in succession by interface when setting Duplicate Address Detection is 3. Switch(Config-if-Vlan1)# ipv6 nd dad attempts 3	

10.2.7 ipv6 nd ns-interval

Command	**ipv6 nd ns-interval <*seconds*>** **no ipv6 nd ns-interval**	
parameter	***seconds***	is the time interval of sending Neighbor Solicitation Message, <seconds> value must be between 1-3600 seconds, no command restores the default value 1 second.
default	The default Request Message time interval is 1 second.	
Mode	Interface Configuration Mode	
Usage Guide	The value to be set will include the situation in all routing announcement on the interface. Generally, very short time interval is not recommended.	
Example	Set Vlan1 interface to send out Neighbor Solicitation Message time interval to be 8 seconds. Switch(Config-if-Vlan1)#ipv6 nd ns-interval 8	

10.2.8 ipv6 neighbor

Command	**ipv6 neighbor <*ipv6-address*> <*hardware-address*> interface <*interface-type interface-name*>** **no ipv6 neighbor <*ipv6-address*>**	
parameter	***ipv6-address***	is static neighbor IPv6 address
	hardware-address	is static neighbor hardware address
	interface-type	is Ethernet type,
	interface-name	is Layer 2 interface name
default	There is not static neighbor table entry	
Mode	Interface Configuration Mode	
Usage Guide	IPv6 address and multicast address for specific purpose and local address cannot be set as neighbor.	

Example

Set static neighbor 2001:1:2::4 on port E1/0/1, and the hardware MAC address is 00-03-0f-89-44-bc.

```
Switch(Config-if-Vlan1)#ipv6 neighbor 2001:1:2::4 00-03-0f-89-44-bc interface Ethernet
1/0/1
```

10.2.9 show ip interface

Command	**show ip interface [<*ifname*> | vlan <*vlan-id*>] brief**	
parameter	***ifname***	Interface name
	vlan-id	VLAN ID
default	Show all brief information of the configured layer 3 interface when no parameter is specified.	
Mode	All modes.	
Usage Guide	This command is used to view brief information on the configured Layer 3 interface.	

Example

view brief information on vlan1 interface configuration.

```
Switch#show ip interface vlan 1 brief
Index      Interface              IP-Address       Protocol
11001       Vlan1                   192.168.2.1      up
```

10.2.10 show ip traffic

Command	**show ip traffic**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Display statistics for IP, ICMP, TCP, UDP packets received/sent.

Example

Displays statistics for IP packets.

```
Switch#show ip traffic
IP statistics:
Rcvd: 3249810 total, 3180 local destination
0 header errors, 0 address errors
0 unknown protocol, 0 discards
Frags: 0 reassembled, 0 timeouts
0 fragment rcvd, 0 fragment dropped
0 fragmented, 0 couldn't fragment, 0 fragment sent
Sent: 0 generated, 3230439 forwarded
0 dropped, 0 no route
ICMP statistics:
Rcvd: 0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
Sent: 0 total 0 errors 0 time exceeded
0 redirects, 0 unreachable, 0 echo, 0 echo replies
0 mask requests, 0 mask replies, 0 quench
0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
TcpActiveOpens 0, TcpAttemptFails 0
TcpCurrEstab 0, TcpEstabResets 0
TcpInErrs 0, TcpInSegs 3180
TcpMaxConn 0, TcpOutRsts 3
TcpOutSegs 0, TcpPassiveOpens 8
TcpRetransSegs 0, TcpRtoAlgorithm 0
TcpRtoMax 0, TcpRtoMin 0
UDP statics:
UdpInDatagrams 0, UdpInErrors 0
```

UdpNoPorts 0, UdpOutDatagrams 0

Display content	describe
IP statistics：	IP packet statistics
Rcvd: 3249810 total, 3180 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be fragmented, number of fragments sent, etc.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics：	ICMP packet statistics.
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

10.2.11 show ipv6 interface

Command	**show ipv6 interface {brief|<*interface-name*>}**	
parameter	**brief**	is the brief summarization of IPv6 status and configuration
	interface-name	is Layer 3 interface name
default	-	
Mode	Admin and Configuration Mode	
Usage Guide	If only brief is specified, then information of all L3 is displayed, and you can also specify a specific Layer 3 interface.	
Example	View information ipv6 the vlan1 interface.	

```
Switch#show ipv6 interface Vlan1
Vlan1 is up, line protocol is up, dev index is 2004
Device flag 0x1203(UP BROADCAST ALLMULTI MULTICAST)
IPv6 is enabled
Link-local address(es):
fe80::203:fff:fe00:10 PERMANENT
Global unicast address(es):
3001::1 subnet is 3001::1/64 PERMANENT
Joined group address(es):
ff02::1
ff02::16
ff02::2
ff02::5
ff02::6
ff02::9
ff02::d
ff02::1:ff00:10
ff02::1:ff00:1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts is 1
ND managed_config_flag is unset
ND other_config_flag is unset
ND NS interval is 1 second(s)
ND router advertisements is disabled
ND RA min-interval is 200 second(s)
ND RA max-interval is 600 second(s)
ND RA hoplimit is 64
ND RA lifetime is 1800 second(s)
ND RA MTU is 0
```

ND advertised reachable time is 0 millisecond(s)

ND advertised retransmit time is 0 millisecond(s)

Display content	describe
Vlan1	Layer 3 interface name
[up/up]	Layer 3 interface status
dev index	Internal index No.
fe80::203:fff:fe00:10	Automatically configured IPv6 address of Layer 3 interface
3001::1	Configured IPv6 address of Layer 3 interface

10.2.12 show ipv6 route

Command **show ipv6 route [database]**

parameter **database** is router database

default -

Mode Admin and Configuration Mode

Usage Guide **show ipv6 route** only shows IPv6 kernal routing table (routing table in tcpip), database shows all routers except the local router.

Example Display IPv6 Routing Table.

```
Switch#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
        I - IS-IS, B - BGP
Timers: Uptime

C     ::1/128 via ::, Loopback, 02:55:37    tag:0
```

Display content	describe
IPv6 Routing Table	IPv6 routing table status
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,I - IS-IS, B - BGP > - selected route	Abbreviation display sign of every entry

10.2.13 show ipv6 neighbors

Command

show ipv6 neighbors [{vlan|ethernet} interface-number | interface-name | address <*ipv6address*>]

parameter

{vlan|ethernet} interface-number	specify the lookup based on interface
ipv6address	specifies the lookup based on IPv6 address. It displays the whole neighbor table entry if without parameter.

default

-

Mode

Admin and Configuration Mode

Usage Guide

Displays neighbor table information. If there are no parameters, the entire neighbor table entry is displayed.

Example

Check ipv6 Neighbor Table Information.

```
Switch#show ipv6 neighbors
IPv6 neighbour unicast items: 2, valid: 1, matched: 1, incomplete: 0, delayed: 0,
         manage items: 0
IPv6  Address                                Hardware  Addr            Interface
Port                  State          Age-time(sec)
fe80::d8e4:a662:88e4:dc24                        00-e0-4c-21-00-34          Vlan1
Ethernet1/0/18         reachable        563

IPv6 neighbour table: 1 entries
```

Display content	describe
IPv6 Addres	Neighbor IPv6 address
Hardware Addr	Neighbor MAC address
Interface	Exit interface name
Port	Exit interface name
State	Neighbor status (reachable. statle. delay. probe. permanent. incomplete. unknow)

10.2.14 show ipv6 traffic

Command **show ipv6 traffic**

parameter -

default -

Mode Admin and Configuration Mode

Usage Guide Display IPv6 transmit packet statistics.

Example Display IPv6 transmit packet statistics.

```
Switch#show ipv6 traffic
IPv6 statistics:
  Rcvd:   27 total, 21 local destination
          0 header errors, 0 address errors
          0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
          0 fragment rcvd, 0 fragment dropped
          0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:   24 generated, 0 forwarded
          0 dropped, 0 no route
ICMPv6 statistics:
  Rcvd:   21 total, 0 errors
          0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
          0 echo requests, 0 echo replies
          0 group queries, 0 group responses, 0 group reduces
          0 router solicits, 0 router adverts, 0 redirects
          9 neighbor solicits, 12 neighbor adverts
  Sent:   24 total, 0 errors
          0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems
          0 echo requests, 0 echo replies
          0 group queries, 0 group responses, 0 group reduces
          0 router solicits, 0 router adverts, 0 redirects
          9 neighbor solicits, 9 neighbor adverts
TCP statistics:
  Rcvd:   0 total segments, 0 errors
  Sent:   0 total segments, 0 retransmitted segments
UDP statics:
  Rcvd:   0 total, 0 errors, 0 no port
  Sent:   0 total
```

Display content	describe
IPv6 statistics:	IPv6 data report statistics
Rcvd: 27 total, 21 local destination 0 header errors, 0 address errors 0 unknown protocol, 0 discards	IPv6 received packets statistics
Frags: 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	IPv6 fragmenting statistics
Sent: 24 total, 0 errors 0 unreachable, 0 too big, 0 time exceeded, 0 parameter problems 0 echo requests, 0 echo replies 0 group queries, 0 group responses, 0 group reduces 0 router solicits, 0 router adverts, 0 redirects 9 neighbor solicits, 9 neighbor adverts	IPv6 sent packets statistics

10.2.15 ip route

Command

ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>l<*prefix-length*>} {<*gateway-address*> | null0} [<*distance*>]

no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]

parameter

ip-prefix	Routing destination address, for example :1.1.1.1
mask	Routing destination address subnet mask, for example :255.255.255.0
prefix-length	Routing destination address prefix
gateway-address	Address IP next hop, for example :1.1.1.1
null0	Forwarding interface
distance	Routing priority, size range :1-255

default

Default static routing has a priority of 1

Mode

Global mode.

Usage Guide

This command can be used to configure switch static routing. both the address and the forwarding interface are available by specifying the next hop IP the routing packet when configuring the next hop of the static route.

Example

Add static routing to the switch.

```
Switch(config)#ip route 192.168.2.8/24 null0
```

10.3 ARP Configuration

10.3.1 arp

Command	**arp <*ip_address*> <*mac_address*> {interface [ethernet] <*portName*>}** **no arp <*ip_address*>**	
parameter	***ip_address***	is the IP address, at the same field with interface address
	mac_address	is the MAC address
	ethernet	stands for Ethernet port
	portName	for the name of layer2 port
default	No static ARP entry is set by default.	
Mode	VLAN Interface Mode	
Usage Guide	Static ARP entries can be configured in the switch.	
Example	Configuring static ARP for interface VLAN1. Switch(Config-if-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 interface eth 1/0/2	

10.3.2 clear arp-cache

Command	**clear arp-cache**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	this command is used to clear the arp table.
Example	Clear the arp table. Switch#clear arp-cache

10.3.3 clear arp traffic

Command	**clear arp traffic**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	Clear the switch ARP message statistics. box switches, this command only clears the statistics of APP messages received and sent from the current card.
Example	Clear switch ARP message statistics. Switch#clear arp traffic

10.3.4 show arp

Command	**show arp [<*ipaddress*>] [<*vlan-id*>] [<*hw-addr*>] [type {static | dynamic}] [count] [vrf word]**	
parameter	***ipaddress***	is a specified IP address
	vlan-id	Vlan id
	hw-addr	for entry of specified MAC address
	static	for static ARP entry
	dynamic	for dynamic ARP entry
	count	displays number of ARP entries
	vrf word	is the specified vrf name
default	-	
Mode	Admin Mode	
Usage Guide	Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.	

Example

Displays the current ARP table content information.

```
Switch#show arp
ARP Unicast Items: 7, Valid: 7, Matched: 7, Verifying: 0, Incomplete: 0, Failed: 0, None: 0
Address    Hardware Addr       Interface          Port              Flag
50.1.1.6   00-0a-eb-51-51-38   Vlan50     Ethernet1/0/11     Dynamic
50.1.1.9   00-00-00-00-00-09   Vlan50     Ethernet1/0/1      Static
150.1.1.2   00-00-58-fc-48-9f   Vlan150    Ethernet1/0/4      Dynamic
```

Display content	describe
Total arp items	Total number of ARP entries.
Valid	ARP entry number matching the filter conditions and attributing the legality states.
Matched	ARP entry number matching the filter conditions.
Verifying	ARP entry number at verifying again validity for ARP
InCompleted	ARP entry number have ARP request sent without ARP reply.
Failed	ARP entry number at failed state.
None	ARP entry number at begin-found state.
Address	IP address of ARP entries.
Hardware Address	MAC address of ARP entries.
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) port corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

10.3.5 show arp traffic

Command	**show arp traffic**
parameter	-
default	-
Mode	Admin and Config Mode
Usage Guide	Display statistics information of received and sent APP messages.
Example	Displays current ARP statistics.

```
Switch#show arp traffic
ARP statistics:
  Rcvd:   0 request, 0 response
  Sent:   0 request, 0 response
```

10.4 ARP Scanning Prevention

10.4.1 anti-arpscan enable

Command	**anti-arpscan enable** **no anti-arpscan enable**
parameter	-
default	Disable ARP scanning prevention function.
Mode	Global configuration mode
Usage Guide	When remotely managing a switch with a method like telnet, users should set the uplink port as a Super Trust port before enabling anti-ARP-scan function, preventing the port from being shutdown because of receiving too many ARP messages. After the anti-ARP-scan function is disabled, this port will be reset to its default attribute, that is, Untrust port.
Example	Enable the ARP scanning prevention function of the switch. Switch(config)#anti-arpscan enable

10.4.2 anti-arpscan port-based threshold

Command	**anti-arpscan port-based threshold <*threshold-value*>** **no anti-arpscan port-based threshold**
parameter	***threshold-value*** rate threshold, ranging from 2 to 200.
default	10 packets /second.
Mode	Global Configuration Mode
Usage Guide	the threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.
Example	Set the threshold of port-based ARP scanning prevention as 10 packets/second. Switch(config)#anti-arpscan port-based threshold 10

10.4.3 anti-arpscan ip-based threshold

Command	**anti-arpscan ip-based threshold <*threshold-value*>** **no anti-arpscan ip-based threshold**
parameter	***threshold-value*** rate threshold, ranging from 1 to 200.
default	3 packets/second.
Mode	Global configuration mode
Usage Guide	The threshold of port-based ARP scanning prevention should be larger than the threshold of IP-based ARP scanning prevention, or, the IP-based ARP scanning prevention will fail.
Example	Set the threshold of IP-based ARP scanning prevention as 6 packets/second. Switch(config)#anti-arpscan ip-based threshold 6

10.4.4 anti-arpscan trust

Command	**anti-arpscan trust [port | supertrust-port]** **no anti-arpscan trust [port | supertrust-port]**
parameter	-
default	By default all the ports are non- trustful.
Mode	Port configuration mode
Usage Guide	If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed, but the non- trustful IP of this port will still be checked. If a port is set as a super trusted port, then neither the port nor the IP of the port will be dealt with. If the port is already closed by ARP scanning prevention, it will be opened right after being set as a trusted port.
Example	Set port ethernet 4/5 of the switch as a trusted port. Switch(Config-If-Ethernet4/5)# anti-arpscan trust port

10.4.5 anti-arpscan trust ip

Command	**anti-arpscan trust ip <*ip-address*> [<*netmask*>]** **no anti-arpscan trust ip <*ip-address*> [<*netmask*>]**	
parameter	***ip-address***	Configure trusted IP address
	netmask	Net mask of the IP.
default	By default all the IP are non-trustful. Default mask is 255.255.255.255	
Mode	Global configuration mode	
Usage Guide	If a port is configured as a trusted port, then the ARP scanning prevention function will not deal with this port, even if the rate of received ARP messages exceeds the set threshold, this port will not be closed. If the port is already closed by ARP scanning prevention, its traffic will be recovered right immediately.	
Example	Set 192.168.1.0/24 as trusted IP Switch(config)#anti-arpscan trust ip 192.168.1.0 255.255.255.0	

10.4.6 anti-arpscan recovery enable

Command	**anti-arpscan recovery enable** **no anti-arpscan recovery enable**
parameter	-
default	Enable the automatic recovery function
Mode	Global configuration mode
Usage Guide	If the users want the normal state to be recovered after a while the port is closed or the IP is disabled, they can configure this function.
Example	Enable the automatic recovery function of the switch. Switch(config)#anti-arpscan recovery enable

10.4.7 anti-arpscan recovery time

Command	**anti-arpscan recovery time <*seconds*>** **no anti-arpscan recovery time**
parameter	***seconds*** Automatic recovery time, in second ranging from 5 to 86400.
default	300s
Mode	Global configuration mode
Usage Guide	this command is used to configure automatic recovery time, no command is used to restore default configuration.
Example	Set the automatic recovery time as 3600 seconds. Switch(config)#anti-arpscan recovery time 3600

10.4.8 anti-arpscan log enable

Command	**anti-arpscan log enable** **no anti-arpscan log enable**
parameter	-
default	Enable ARP scanning prevention log function.
Mode	Global configuration mode
Usage Guide	After enabling ARP scanning prevention log function, users can check the detailed information of ports being closed or automatically recovered by ARP scanning prevention or IP being disabled and recovered by ARP scanning prevention. The level of the log is "Warning".
Example	Enable ARP scanning prevention log function of the switch. Switch(config)#anti-arpscan log enable

10.4.9 anti-arpscan trap enable

Command

anti-arpscan trap enable
no anti-arpscan trap enable

parameter

-

default

Disable ARP scanning prevention SNMP Trap function.

Mode

Global configuration mode

Usage Guide

After enabling ARP scanning prevention SNMP Trap function, users will receive Trap message whenever a port is closed or recovered by ARP scanning prevention, and whenever IP t is closed or recovered by ARP scanning prevention.

Example

Enable ARP scanning prevention SNMP Trap function of the switch.

```
Switch(config)#anti-arpscan trap enable
```

10.4.10 show anti-arpscan

Command

show anti-arpscan [trust [ip | port | supertrust-port] |prohibited [ip | port]]

parameter

-

default

Display every port to tell whether it is a trusted port and whether it is closed. If the port is closed, then display how long it has been closed. Display all the trusted IP and disabled IP.

Mode

Admin Mode

Usage Guide

Use “show anti-arpscan trust port” if users only want to check trusted ports. The reset follow the same rule.

Example

Check the operating state of ARP scanning prevention function after enabling it.

```
Switch#show anti-arpscan
Total port: 28
Name                Port-property    beShut    shutTime(seconds)
Ethernet1/0/1     untrust           N          0
```

```
Ethernet1/0/2      untrust          N          0
Ethernet1/0/3      untrust          N          0
Ethernet1/0/4      trust            N          0
Ethernet1/0/5      trust            N          0
Ethernet1/0/6      untrust          N          0
Ethernet1/0/7      untrust          N          0
Ethernet1/0/8      untrust          N          0
Ethernet1/0/9      untrust          N          0
Ethernet1/0/10     untrust          N          0
Ethernet1/0/11     untrust          N          0
Ethernet1/0/12     untrust          N          0
Ethernet1/0/13     untrust          N          0
Ethernet1/0/14     untrust          N          0
Ethernet1/0/15     untrust          N          0
Ethernet1/0/16     untrust          N          0
Ethernet1/0/17     untrust          N          0
Ethernet1/0/18     untrust          N          0
Ethernet1/0/19     untrust          N          0
Ethernet1/0/20     untrust          N          0
Ethernet1/0/21     untrust          N          0
Ethernet1/0/22     untrust          N          0
Ethernet1/0/23     untrust          N          0
Ethernet1/0/24     untrust          N          0
Ethernet1/0/25     untrust          N          0
Ethernet1/0/26     untrust          N          0
Ethernet1/0/27     untrust          N          0
Ethernet1/0/28     untrust          N          0

No prohibited IP.

Trust IP:
192.168.1.0        255.255.255.0
```

10.5 Preventing ARP Spoofing

10.5.1 ip arp-security updateprotect

Command	**ip arp-security updateprotect** **no ip arp-security updateprotect**
parameter	-
default	ARP table automatic update.
Mode	Global Mode/ Interface configuration.
Usage Guide	Forbid ARP table automatic update, the ARP packets conflicting with current ARP item (e.g. with same IP but different MAC or port) will be dropped, the others will be received to update aging timer or create a new item; so, the current ARP item keep unchanged and the new item can still be learned.
Example	Automatic update of ARP table is prohibited. Switch(Config-if-Vlan1)#ip arp-security updateprotect. Switch(config)#ip arp-security updateprotect

10.5.2 ip arp-security learnprotect

Command	**ip arp-security learnprotect** **no ip arp-security learnprotect**
parameter	-
default	ARP learning enabled.
Mode	Global Mode/ Interface Configuration
Usage Guide	This command is for preventing the automatic learning and updating of ARP. Unlike ip arp-security updateprotect, once this command implemented, there will still be timeout even if the switch keeps sending Request/Reply messages.
Example	Prohibit IPv4 version of the ARP learning function. Switch(config)# ip arp-security learnprotect

10.5.3 ip arp-security convert

Command	**ip arp-security convert**
parameter	-
default	-
Mode	Global Mode/ Interface configuration
Usage Guide	This command will convert the dynamic ARP entries to static ones, which, in combination with disabling automatic learning, can prevent ARP binding. Once implemented, this command will lose its effect.
Example	To change all dynamic ARP to static ARP. Switch(config)#ip arp -security convert

10.5.4 clear ip arp dynamic

Command	**clear ip arp dynamic**
parameter	-
default	-
Mode	Interface Configuration
Usage Guide	This command will clear dynamic entries before binding ARP. Once implemented, this command will lose its effect.
Example	Clear all dynamic ARP. on the interface. Switch(Config-if-Vlan1)#clear ip arp dynamic

10.5.5 clear ipv6 nd dynamic

Command	**clear ipv6 nd dynamic**
parameter	-
default	-
Mode	Vlan Interface Mode
Usage Guide	It used in dynamic table when use ND bind function to clear. After executeit, the command will be useless.
Example	Clear all dynamic ND. in ports. Switch(Config-if-Vlan1)#clear ipv6 nd dynamic

10.6 ARP GUARD

10.6.1 arp-guard ip

Command	**arp-guard ip <addr>** **no arp-guard ip <addr>**	
parameter	**Addr**	is the protected IP address, in dotted decimal notation
default	There is no ARP GUARD address by default	
Mode	Port configuration mode	
Usage Guide	After configuring the ARP GUARD address, the ARP messages received from the ports configured ARP GUARD will be filtered. If the source IP addresses of the ARP messagse match the ARP GUARD address configured on this port, these messages will be judged as ARP cheating messages, which will be directly dropped instead of sending to the CPU of the switch or forwarding. 16 ARP GUARD addresses can be configured on each port.	
Example	Configure the ARP GUARD address on port ethernet1/0/1 as 100.1.1.1 switch(config)#interface ethernet1/0/1 switch(Config-If-Ethernet 1/0/1)#arp-guard ip 100.1.1.1	

10.7 Gratuitous ARP Configuration

10.7.1 ip gratuitous-arp

Command	**ip gratuitous-arp [<*interval-time*>]** **no ip gratuitous-arp**
parameter	***interval-time*** is the update interval for gratuitous ARP with its value limited between 5 and 1200 seconds and with default value as 300 seconds.
default	Gratuitous ARP is disabled by default.
Mode	Global configuration mode and vlan interface configuration mode
Usage Guide	When configuring gratuitous ARP in global configuration mode, all the Layer 3 interfaces in the switch will be enabled to send gratuitous ARP request. If gratuitous ARP is configured in interface configuration mode, then only the specified interface is able to send gratuitous ARP requests. When configuring the gratuitous ARP, the update interval configuration from interface configuration mode has higher preference than that from the global configuration mode.
Example	To enable gratuitous ARP in global configuration mode, and set the update interval to be 400 seconds. Switch#config Switch(config)#ip gratuitous-arp 400

10.7.2 show ip gratuitous-arp

Command	**show ip gratuitous-arp [interface vlan <*vlan-id*>]**
parameter	***vlan-id*** VLAN ID
default	-
Mode	All the Configuration Modes.
Usage Guide	Displays gratuitous ARP configuration information.
Example	Displays gratuitous ARP configuration information. Switch#show ip gratuitous-arp Gratuitous ARP send is Global enabled, Interval-Time is 300(s) Gratuitous ARP send enabled interface vlan information: Name Interval-Time(seconds) Vlan1 400 Vlan10 350

10.8 Dynamic ARP Inspection

10.8.1 ip arp inspection

Command	**ip arp inspection vlan <vlan-id>** **no ip arp inspection vlan <vlan-id>**	
parameter	**vlan-id**	is the vlan which is enabled the dynamic ARP inspection function
default	Disable.	
Mode	Global Mode.	
Usage Guide	After configured the dynamic ARP inspection function in global mode, the administrator can intercept, record and drop the ARP data packets which have the invalid MAC address/IP address.	
Example	Enable the dynamic ARP inspection function of vlan10. Switch(config)# Switch(config)#ip arp inspection vlan 10 Switch(config)#exit	

10.8.2 ip arp inspection trust

Command	**ip arp inspection trust** **no ip arp inspection trust**
parameter	-
default	All the ports are the untrusted ports as default.
Mode	Port Mode
Usage Guide	After configured this command under the port mode, the configured port will not inspect the received ARP packet and it will forward it directly. If the ARP data packet is received from the untrusted port, the switch will only forward the lawful data packet. For the illegal data, it will drop the data directly and record this action.
Example	Configure the port 1/0/1 as the trusted port. Switch(config)# Switch(config)#in e 1/0/1 Switch(config-if-ethernet1/0/1)#ip arp inspection trust

10.8.3 ip arp inspection limit-rate

Command	**ip arp inspection limit-rate <rate>** **no ip arp inspection limit-rate**
parameter	**rate** — is the configured limited rate of the ARP packet of the untrusted port, the unit is pps
default	Do not limit the rate for the ARP packets of the trusted or untrusted ports.
Mode	Port Mode
Usage Guide	This command can limit the ARP packet rate of the untrusted port. The rate of the lawful ARP data packets forwarding is in the limited range.
Example	Configure the rate of the ARP packet of the untrusted port 1/0/1 as 100pps.

```
Switch(config)#
Switch(config)#in e 1/0/1
Switch(config-if-ethernet1/0/1)# ip arp inspection limit-rate 100
Switch(config-if-ethernet1/0/1)#exit
```

Chapter 11 DHCP Server Configuration

11.1 DHCP

11.1.1 bootfile

Syntax	**Bootfile <filename>** **no bootfile**	
Parameter	**<filename>**	name of the file to be imported, up to 255 characters are allowed.
Default	None	
Mode	DHCP Address Pool Mode	
Usage	Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on boot up. This command is together with the "next sever".	
Example	The path and filename for the file to be imported is "temp\nos.img" Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#bootfile \temp\nos.img	

11.1.2 clear ip dhcp binding

Syntax	**clear ip dhcp binding (<A.B.C.D> | all)**	
Parameter	**<A.B.C.D>**	IP address that has a binding record in decimal format
	all	all IP addresses that have a binding record
Default	None	
Mode	Admin Mode	
Usage	"**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.	
Example	Removing all IP-hardware address binding records Switch#clear ip dhcp binding all	

11.1.3 clear ip dhcp conflict

Syntax	**clear ip dhcp binding (<A.B.C.D> | all)**	
Parameter	**<A.B.C.D>**	IP address that has a conflict record;
	all	All stands for all addresses that have conflict records.
Default	None	
Mode	Admin Mode	
Usage	show ip dhcp conflict” command can be used to check which IP addresses are conflicting for use. The “clear ip dhcp conflict” command can be used to delete the conflict record for an address. If "all” is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server	
Example	The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log. Switch#clear ip dhcp conflict 10.1.128.160	

11.1.4 clear ip dhcp server statistics

Syntax	**clear ip dhcp server statistics**
Parameter	None
Default	None
Mode	Admin Mode
Usage	DHCP count statistics can be viewed with “**show ip dhcp server statistics**” command, all information is accumulated. You can use the “**clear ip dhcp server statistics**” command to clear the count for easier statistics checking
Example	Clearing the count for DHCP server. Switch#clear ip dhcp server statistics

11.1.5 client-identifier

Syntax	**client-identifier <unique-identifier>** **no client-identifier**
Parameter	**<unique-identifier>** user identifier, in dotted Hex format
Default	None
Mode	DHCP Address Pool Mode
Usage	This command is used with "host" when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns the IP address defined in "host" command to the client.
Example	Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24

11.1.6 default-router

Syntax	**default-router <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]]** **no default-router**
Parameter	**<A.B.C.D>** IP addresses, in decimal format.
Default	No default gateway is configured for DHCP clients by default.
Mode	DHCP Address Pool Mode
Usage	The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.
Example	Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

11.1.7 dns-server

Syntax	**dns-server <A.B.C.D> [<A.B.C.D>[...<A.B.C.D>]]** **no dns-server**	
Parameter	**<A.B.C.D>**	IP addresses, in decimal format.
Default	No DNS server is configured for DHCP clients by default.	
Mode	DHCP Address Pool Mode	
Usage	Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, therefore address 1 has the highest priority, and address 2 has the second, and so on.	
Example	Set 10.1.128.2 as the DNS server address for DHCP clients. Switch#config Switch(config) # ip dhcp pool 1 Switch(dhcp-1-config)#dns-server 10.1.128.2	

11.1.8 domain-name

Syntax	**domain-name <domain>** **no domain-name**	
Parameter	**<domain>**	domain name, up to 255 characters are allowed.
Default	None	
Mode	DHCP Address Pool Mode	
Usage	Specifies a domain name for the client.	
Example	Specifying “switch.com.cn" as the DHCP clients' domain name. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#domain-name switch.com.cn	

11.1.9 hardware-address

Syntax	**hardware-address <hardware-address> [Ethernet | IEEE802 | <*type-number*>]** **no hardware-address**	
Parameter	**<hardware-address>**	hardware address in Hex
	Ethernet | IEEE802	Ethernet protocol type
	<type-number>	RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.
Default	The default protocol type is Ethernet	
Mode	DHCP Address Pool Mode	
Usage	This command is used with the "host" when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in "host" command to the client.	
Example	Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware 00-00-e2-3a-26-04 Switch(dhcp-1-config)#host 10.1.128.160 24	

11.1.10 host

Syntax	**host <*address*> [<*mask*> | <*prefix-length*>]** **no host**	
Parameter	**<address>**	IP address in decimal format
	<mask>	subnet mask in decimal format
	<prefix-length>	mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".
Default	None	
Mode	DHCP Address Pool Mode	
Usage	If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class. This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.	
Example	Specifying IP address 10.1.128.160 to be bound to user with hardware address	

	00-10-5a-60-af-12 in manual address binding. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12 Switch(dhcp-1-config)#host 10.1.128.160 24

11.1.11 ip dhcp conflict logging

Syntax	**ip dhcp conflict logging** **no ip dhcp conflict logging**
Parameter	none
Default	Logging for address conflict is enabled by default.
Mode	Global Mode
Usage	When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.
Example	Disable logging for DHCP server. Switch#config Switch(config)#no ip dhcp conflict logging

11.1.12 ip dhcp disable

Syntax	**ip dhcp disable** **no ip dhcp disable**
Parameter	none
Default	Enable
Mode	Port mode
Usage	After the port disables DHCP services, directly drop all DHCP packets sent by the port.
Example	The port disables DHCP services. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp disable

11.1.13 ip dhcp excluded-address

Syntax	**ip dhcp excluded-address** ***<low-address>*** **[*<high-address>*]** **no ip dhcp excluded-address** ***<low-address>*** **[*<high-address>*]**	
Parameter	***<low-address>***	starting IP address
	<high-address>	ending IP address
Default	Only individual address is excluded by default	
Mode	Global Mode	
Usage	This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.	
Example	Reserving addresses 1.1.1.1 from dynamic assignment. Switch#config Switch(config)#ip dhcp excluded-address 1.1.1.1	

11.1.14 ip dhcp pool

Syntax	**ip dhcp pool <name>** **no ip dhcp pool <name>**	
Parameter	**<name>**	address pool name, up to 32 characters are allowed
Default	None	
Mode	Global Mode	
Usage	This command is used to configure a DHCP address pool under Global	
Example	Defining an address pool named "1". Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#	

11.1.15 ip dhcp conflict ping-detection enable

Syntax	**ip dhcp conflict ping-detection enable** **no ip dhcp conflict ping-detection enable**
Parameter	None
Default	By default, Ping-detection of conflict is disabled.
Mode	Global Mode
Usage	To enable Ping-detection of conflict, one should enable the log of conflict addresses, when which is disabled, so will the ping-detection of conflict. When a client is unable to receive Ping request messages (when blocked by firewall, for example), this function will check local ARP according to allocated IP: if a designated IP has a corresponding ARP, then an address conflict exists; otherwise, allocate it to the client.
Example	Enable Ping-detection of conflict. Switch#config Switch(config)#ip dhcp conflict ping-detection enable

11.1.16 ip dhcp ping packets

Syntax	**ip dhcp ping packets <request-num>** **no ip dhcp ping packets**	
Parameter	<request num>	number of Ping request message to be sent in Ping-detection of conflict.
Default	No more than 2 Ping request messages will be sent by default.	
Mode	Global Mode	
Usage	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server, whose default value is 2; the no operation of this command will restore the default value.	
Example	Set the max number of Ping request (Echo Request) message to be sent in Ping-detection of conflict on DHCP server as 3. Switch#config Switch(config)#ip dhcp ping packets 3	

11.1.17 ip dhcp ping timeout

Syntax	**ip dhcp ping timeout <timeout-value>** **no ip dhcp ping timeout**	
Parameter	**<timeout-value>**	***<timeout-value>*** is the timeout period of waiting for a reply message after each Ping request message in Ping-detection of conflict.
Default	The timeout period is 500ms by default.	
Mode	Global Mode	
Usage	Set the timeout period (in ms) of waiting for a reply message (Echo Request) after each Ping request message (Echo Request) in Ping-detection of conflict on DHCP server, whose default value is 500ms. The no operation of this command will restore the default value.	
Example	Set the timeout period (in ms) of waiting for each reply message (Echo Request) in Ping-detection of conflict on DHCP server as 600ms. Switch#config Switch(config)#ip dhcp ping timeout 600	

11.1.18 lease

Syntax	**lease (<*days*> [<*hours*>][<*minutes*>] | infinite)** **no lease**	
Parameter	***<days>***	number of days from 0 to 365;
	<hours>	number of hours from 0 to 23
	<minutes>	number of minutes from 0 to 59
	infinite	perpetual use
Default	The default lease duration is 1 day.	
Mode	DHCP Address Pool Mode	
Usage	DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of switch is 1 day.	
Example	Setting the lease of DHCP pool "sd" to 3 days 12 hours and 30 minutes. Switch#config Switch(config)#ip dhcp pool sd Switch(dhcp-sd-config)#lease 3 12 30	

11.1.19 max-lease-time

Syntax	**max-lease-time (<*days*> [<*hours*>][<*minutes*>] | infinite)** **no max-lease-time**	
Parameter	***<days>***	number of days from 0 to 365;
	<hours>	number of hours from 0 to 23
	<minutes>	number of minutes from 0 to 59
	infinite	perpetual use
Default	The default lease time is 1 day.	
Mode	DHCP Address Pool Mode	
Usage	This command is used to DHCP request packets with option51. If the lease time (user requests the address) exceeds the maximum lease time configured, the lease that DHCP server assigns the address is the maximum lease time configured. If the lease time requested by the user is less than the maximum lease time configured, the lease that DHCP server assigns the address is the lease time requested by the user. The maximum lease time is able to be set by the administrator according to the actual network condition, and the maximum lease time is 1 day by default.	
Example	Set the maximum lease time of DHCP address pool1 to 3 days 12 hours and 30 minutes. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#max-lease-time 3 12 30	

11.1.20 netbios-name-server

Syntax	**netbios-name-server <address1> [address2[...<address8>]]** **no netbios-name-server**	
Parameter	**<address1>...<address8>**	IP addresses, in decimal format.
Default	No WINS server is configured by default.	
Mode	DHCP Address Pool Mode	
Usage	This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.	
Example	Setting the server address of DHCP pool "1" to 192.168.1.1. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-name-server 192.168.1.1	

11.1.21 netbios-node-type

Syntax	**netbios-node-type {b-node | h-node | m-node | p-node | <type-number>}** **no netbios-node-type**	
Parameter	**b-node**	broadcasting node
	h-node	hybrid node that broadcasts after point-to-point communication
	m-node	hybrid node to communicate in point-to-point after broadcast;
	p-node	point-to-point node
	<type-number>	node type in Hex from 0 to FF
Default	No client node type is specified by default.	
Mode	DHCP Address Pool Mode	
Usage	If client node type is to be specified, it is recommended to set the client node type to h-node that broadcasts after point-to-point communication.	
Example	Setting the node type for client of pool 1 to broadcasting node. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#netbios-node-type-node	

11.1.22 network-address

Syntax	**network-address <network-number> [<mask> | <prefix-length>]** **no network-address**	
Parameter	**<network-number>**	network number;
	<mask>	subnet mask in the decimal format
	<prefix-length>	mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.
Default	If no mask is specified, default mask will be assigned according to the address class.	
Mode	DHCP Address Pool Mode	
Usage	This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command "hardware address" and "host".	
Example	Configuring the assignable address in pool 1 to be 10.1.128.0/24. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#network-address 10.1.128.0 24	

11.1.23 next-server

Syntax	**next-server <address1>[<address2>[…<address8>]]** **no next-server**	
Parameter	**<address1>...<address8>**	IP addresses, in the decimal format
Default	None	
Mode	DHCP Address Pool Mode	
Usage	This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on boot up. This command is used together with "bootfile".	
Example	Setting the hosting server address as 10.1.128.4. Switch#config Switch(config)#ip dhcp pool 1 Switch(dhcp-1-config)#next-server 10.1.128.4	

11.1.24 option

Syntax	**option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}** **no option <code>**	
Parameter	**<code>**	code for network parameters
	<string>	ASCII string up to 255 characters
	<hex>	a value in Hex that is no greater than 510 and must be of even length
	<ipaddress>	IP address in decimal format, up to 63 IP addresses can be configured.
Default	none	
Mode	DHCP Address Pool Mode	
Usage	The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.	
Example	Setting the WWW server address as 10.1.128.240. Switch#config Switch(config)# ip dhcp pool 1 Switch(dhcp-1-config)#option 72 ip 10.1.128.240	

11.1.25 service dhcp

Syntax

service dhcp

no service dhcp

Parameter

None

Default

DHCP service is disabled by default.

Mode

Global Mode

Usage

Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. Switch can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example

Enabling DHCP server.

```
Switch#config
Switch(config)#service dhcp
```

11.1.26 show ip dhcp binding

Syntax

show ip dhcp binding [[<ip-addr>] [type {all | manual | dynamic}] [count]]

Parameter

<ip-addr>	a specified IP address in decimal format
all	all binding types (manual binding and dynamic assignment)
manual	manual binding
dynamic	dynamic assignment
count	displays statistics for DHCP address binding entries.

Default

None

Mode

Admin and Configuration Mode

Usage

Displays IP-MAC binding information.

Example

```
Switch# show ip dhcp binding
IP address Hardware address Lease expiration Type
10.1.1.233 00-00-E2-3A-26-04 Infinite Manual
10.1.1.254 00-00-E2-3A-5C-D3 60 Automatic
```

Displayed information	Explanation
IP address	IP address IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address
Type	Type of assignment: manual binding or dynamic assignment

11.1.27 show ip dhcp conflict

Syntax **show ip dhcp conflict**

Parameter none

Default none

Mode Admin and Configuration Mode

Usage Displays log information for addresses that have a conflict record.

Example

```
Switch# show ip dhcp conflict
IP Address Detection method Detection Time
10.1.1.1 Ping FRI JAN 02 00:07:01 2002
```

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected
Detection Time	Time when the conflict is detected.

11.1.28 show ip dhcp relay information option

Syntax **show ip dhcp relay information option**

Parameter **none**

Default none

Mode Admin and Configuration Mode

Usage Show the relative configuration for DHCP relay option82

Example

```
Switch#show ip dhcp relay information option
ip dhcp server relay information option(i.e. option 82) is enabled
ip dhcp relay information option(i.e. option 82) is enabled
```

11.1.29 show ip dhcp server statistics

Syntax	**show ip dhcp server statistics**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	Displays statistics of all DHCP packets for a DHCP server

Example

```
Switch# show ip dhcp server statistics
Address pools               1
Database agents              0
Automatic bindings         0
Manual bindings              0
Conflict bindings          0
Expiried bindings           0
Malformed message             0

Message                      Received
BOOTREQUEST                     0
DHCPDISCOVER                    0
DHCPREQUEST                     0
DHCPDECLINE                    0
DHCPRELEASE                     0
DHCPINFORM                     0

Message                      Send
BOOTREPLY                      0
DHCPOFFER                       0
DHCPACK                       0
DHCPNAK                       0
DHCPRELAY                      0
DHCPFORWARD                       0
Switch#
```

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses

Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

11.1.30 ip dhcp broadcast suppress

Syntax	**ip dhcp broadcast suppress** **no ip dhcp broadcast suppress**
Parameter	**none**
Default	Disable
Mode	Global Mode
Usage	Enable DHCP broadcast suppress function, the no command disables the function Suppress the forwarding about DHCP broadcast packets, namely, drop or copy DHCP broadcast packets to CPU.
Example	Enable DHCP broadcast suppress function. Switch# config Switch(config)#ip dhcp broadcast suppress

11.1.31 ip dhcp relay share-vlan

Syntax	**ip dhcp relay share-vlan <vlanid> sub-vlan <vlanlist>** **no ip dhcp relay share-vlan**	
Parameter	**<vlanid>**	VLAN ID of share-vlan
	<vlanlist>	sub-vlan list
Default	None	
Mode	Global Mode	
Usage	Specify sub-vlan of a share-vlan, the no command cancels sub-vlan. share-vlan may include many sub-vlan, but a sub-vlan only corresponds to a share-vlan. When layer 2 device of DHCP Relay receive DHCP Request, firstly judge whether VLAN with layer 3 interface for receiving package. If there is layer 3 interface in package, use the interface to process DHCP Relay, or else use layer 3 interface of share-vlan to process DHCP Relay when the vlan is sub-vlan of share-vlan.	
Example	Switch#config Switch(config)#ip dhcp relay share-vlan 2 sub-vlan 2-4	

11.1.32 ip forward-protocol udp bootps

Syntax	**ip forward-protocol udp bootps** **no ip forward-protocol udp bootps**
Parameter	none
Default	Not forward UPD broadcast packets by default.
Mode	Global Mode
Usage	Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp bootps**"command cancels the service. The forwarding destination address is set in the "**ip helper-address**" command and described later
Example	Setting DHCP packets to be forwarded to 192.168.1.5. Switch#config Switch(config)#ip forward-protocol udp boots Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.1.5

11.1.33 ip helper-address

Syntax	**ip helper-address <ip-address>** **no ip helper-address <ip-address>**
Parameter	**ip-address** IP addresses, in the decimal format
Default	none
Mode	Port mode
Usage	Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address *<ip-address>***" command cancels the setting. The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e. DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. When this command is run after "ip forward-protocol udp <port>" command, the forwarding address configured by this command receives the UDP packets from <port>. The combination of "ip forward-protocol udp <port>" command and this command should be used for configuration.
Example	Switch#config Switch(config)#ip forward-protocol udp bootps Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip helper-address 192.168.2.5

11.1.34 show ip forward-protocol

Syntax	**show ip forward-protocol**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	Show the configured port ID of the protocol which support the forwarding of broadcast packets, it means the port ID for forwarding DHCP packets.
Example	Switch#show ip forward-protocol Forward protocol(UDP port): 67(active)

11.1.35 show ip helper-address

Syntax	**show ip helper-address**
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Show the configuration relation for the port ID of the protocol (It can forward broadcast packets), the interface (It supports forwarding function) and the forwarded destination IP.
Example	Switch#show ip helper-address Forward protocol Interface Forward server 67(active) Vlan1 192.168.2.5

11.1.36 clear ipv6 dhcp binding

Syntax	**clear ipv6 dhcp binding [<ipv6-address>] [pd <ipv6-prefix | prefix-length>]**	
Parameter	<ipv6-address>	specified IPv6 address with binding record
	<ipv6-prefix | prefix-length>	specified IPv6 prefix with binding record; To clear all IPv6 address binding record if there is no specified record.
Default	none	
Mode	Admin Configuration Mode	
Usage	To clear one specified DHCPv6 assigned address binding record or all the IPv6 address binding records. DHCPv6 IPv6 address binding information can be displayed through the command **show ipv6 dhcp binding**. If DHCPv6 client does not use the DHCPv6 allocated IPv6 address but when the life time of the IPv6 address does not end, the DHCPv6 server will not remove its bind for this address. In this situation, the address binding information can be removed manually through this command; and if no parameter is appended, this command will remove all the address binding information, then all addresses and prefix will be assigned again in the DHCPv6 address pool.	
Example	To delete all binding record of IPv6 address and prefix Switch#clear ipv6 dhcp binding	

11.1.37 clear ipv6 dhcp conflict

Syntax	**clear ipv6 dhcp conflict [address]**	
Parameter	address	specified address with the conflict record, no specified address will clear all conflict records.
Default	none	
Mode	Admin Mode	
Usage	Clear the address with the conflict record in address conflict log. With **show ipv6 dhcp conflict** command, the user can check the conflict in which IP addresses. With this command, the user can clears the conflict record of an address. If no specified address will clear the conflict record of all addresses in log. After the conflict records are cleared in log, these addresses can be used by DHCPv6 server again.	
Example	When administrator checks the conflict logs, administrator discovers that address 2001::1 with the conflict record is not used, so its record will be cleared from address conflict files. Switch#clear ipv6 dhcp conflict 2001::1	

11.1.38 clear ipv6 dhcp statistics

Syntax	**clear ipv6 dhcp statistics**
Parameter	none
Default	none
Mode	Admin Mode
Usage	Clear the statistic records of DHCPv6 packets, the statistic counter of DHCPv6 packets is cleared. With **show ipv6 dhcp statistics** command, the user can check the statistic information of the counter for DHCPv6 packets, all statistic information is an accumulative value. With this command will clear the counter to check the debugging conveniently.
Example	Clear the counter of DHCPv6 packets. Switch#clear ipv6 dhcp statistics

11.1.39 dns-server

Syntax	**dns-server <ipv6-address>** **no dns-server <ipv6-address>**
Parameter	**<ipv6-address>** IPv6 address of DNS Server
Default	none
Mode	DHCPv6 Address Pool Configuration Mode.
Usage	To configure the IPv6 address of the DNS server for DHCPv6 client; the no form of this command will remove the DNS configuration. For each address pool, at most three DNS server can be configured, and the addresses of the DNS server must be valid IPv6 addresses.
Example	To configure the DNS Server address of DHCPv6 client as 2001:da8::1. Switch(dhcp-1-config)#dns-server 2001:da8::1

11.1.40 domain-name

Syntax	**domain-name <domain-name>** **no domain-name <domain-name>**
Parameter	**<domain-name>** domain name, less than 32 characters
Default	The domain name parameter of address pool is not configured by default
Mode	DHCPv6 Address Pool Configuration Mode.
Usage	To configure domain name of DHCPv6 client; the no form of this command will delete the domain name. At most 3 domain names can be configured for each address pool.
Example	To set the domain name of DHCPv6 client as test.com.cn Switch(dhcp-1-config)#domain-name test.com.cn

11.1.41 excluded-address

Syntax	**excluded-address <ipv6-address>** **no excluded-address <ipv6-address>**	
Parameter	**<ipv6-address>**	IPv6 address to be excluded from being allocated to hosts in the address pool
Default	Disabled	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure the specified IPv6 address to be excluded from the address pool, the excluded address will not be allocated to any hosts; the no form of this command will remove the configuration. This command is used to preserve the specified address from DHCPv6 address allocation.	
Example	To configure to exclude 2001:da8:123::1 from DHCPv6 address allocation. Switch(config)#excluded-address 2001:da8:123::1	

11.1.42 ipv6 address

Syntax	**ipv6 address <prefix-name> <ipv6-prefix/prefix-length>** **no ipv6 address <prefix-name> <ipv6-prefix/prefix-length>**	
Parameter	**<prefix-name>**	a string with its length no more than 32, designating or manual configuring the name of the address prefix defined in the prefix pool
	<ipv6-prefix/prefix-length>	latter part of the IPv6 address excluding the address prefix, as well as its length.
Default	No global address is configured for interfaces by default.	
Mode	Port mode	
Usage	To configure the specified interface to use prefix delegation for address allocation. The no form of this command will disable the using of prefix delegation for address allocation. The IPv6 address of an interface falls into two parts: ***<prefix-name>*** and ***<ipv6-prefix>/<prefix-length>***. If routing advertisement has been enabled, the first 64 bits of the addresses will be advertised. The address generated by ***<prefix-name>*** and ***<ipv6-prefix/prefix-length>*** combination will be removed, and the advertising of the prefix will be disabled. Only one ***<ipv6-prefix/prefix-length>*** can be configured for one prefix name.	
Example	If the prefix name my-prefix designates 2001:da8:221::/48, then the following command will add the address 2001:da8:221:2008::2008 to interface VLAN1. Switch(Config-if-Vlan1)# ipv6 address my-prefix 0:0:0:2008::2008/64	

11.1.43 ipv6 dhcp client pd

Syntax	**ipv6 dhcp client pd <prefix-name> [rapid-commit]** **no ipv6 dhcp client pd**	
Parameter	**<prefix-name>**	<prefix-name> is the string with its length no more than 32, which designates the name of the address prefix.
	rapid-commit	If **rapid-commit** optional is specified and the prefix delegation server enables the rapid-commit function, then the prefix delegation server will reply the prefix delegation client with the REPLY message directly. And the prefix delegation request will be accomplished by exchanging messages once.
Default	DHCPv6 prefix delegation client is not enabled by default.	
Mode	Port mode	
Usage	To configure DHCPv6 prefix delegation client for the specified interface. The no form of this command will disable the DHCPv6 prefix delegation client and remove the allocated address prefix. This command is used to configure the prefix delegation client on the specified interface, an interface with prefix delegation client enabled will send SOLICIT packets to try to get address prefix from the server. If the prefix is retrieved correctly, the address prefix in the global address pool can be used by the **ipv6 address** command to generate a valid IPv6 address. This command is exclusive with **ipv6 dhcp server** and **ipv6 dhcp relay destination**. If the prefix delegation client is disabled for an interface, then the address prefix which is get from this interface through prefix delegation client, will be removed from the global address pool. Also the interface address which is generated by the prefix delegation client will be removed, and routing advertisement with the prefix will be disabled. If any general prefix has been configured by the **ipv6 general-prefix** command, the same prefix learnt from prefix delegation will be disagreed.	
Example	Switch(Config-if-Vlan1)#ipv6 dhcp client pd ClientA rapid-commit	

11.1.44 ipv6 dhcp client pd hint

Syntax	**ipv6 dhcp client pd hint <prefix|prefix-length>** **no ipv6 dhcp client pd hint <prefix|prefix-length>**
Parameter	**<prefix|prefix-length>** prefix demanded by the client and its length.
Default	There is no such configuration in the system by default.
Mode	Port mode
Usage	Designate the prefix demanded by the client and its length. The no operation of this command will delete that prefix and its length from the specified interface. The system designates a prefix and its length on the interface for a client. If client prefix-proxy demanding function is enabled on the interface and hint function is enabled on the switch, the user will have prior claim to the prefix it demands and the prefix length when the server allocates them. Only one hint prefix is allowed in the system.
Example	Switch(vlan-1-config)#ipv6 dhcp client pd hint 2001::/48

11.1.45 ipv6 dhcp pool

Syntax	**ipv6 dhcp pool <poolname>** **no ipv6 dhcp pool <poolname>**
Parameter	**<poolname>** address pool name of DHCPv6 with its length no more than 32.
Default	Any DHCPv6 address pool are not configured by default.
Mode	Global Mode
Usage	To configure the address pool for DHCPv6, and enter the DHCPv6 address pool configuration mode. In this mode, information such as the address prefix to be allocated, the DNS server addresses, and domain names, can be configured for the DHCPv6 client. The no form of this command will remove the configuration of the address pool. This command should be launched in global configuration mode, and falls in DHCPv6 address pool configuration mode if launched successfully. To remove a configured address pool, interface bindings related to the address pool, as well as the related address bindings will be removed.
Example	To define an address pool, named 1. Switch#config Switch(config)#ipv6 dhcp pool 1

11.1.46 ipv6 dhcp relay destination

Syntax	**ipv6 dhcp relay destination {[<*ipv6-address*>] [interface { <*interface-name*> | vlan <*1-4096*> }] }**
	no ipv6 dhcp relay destination { [<*ipv6-address*>] [interface { <*interface-name*> | vlan <*1-4096*> }] }	

Parameter	***<ipv6-address>***	address of the destination to which the DHCPv6 relay forwards;
	<*interface-name*>	interface name which is used for forwarding of DHCPv6 requests
	<*1-4096*>	VLAN ID
	If **<*ipv6-addess*>** is a global unicast address, the **interface** parameter should not be configured; If **<*ipv6-address*>** is an local address, the **interface** parameter is required be configured; The destination address for the DHCPv6 server will be the multicast address of **ALL_DHCP_Servers (FF05::1:3)**, if the interface parameter is configured only.	
Default	By default, destination address for DHCPv6 relay is not configured.	
Mode	Port mode	
Usage	To configure the destination to which the DHCPv6 relay forwards the DHCPv6 requests from the clients, the destination should be the address of an external DHCPv6 relay or the DHCPv6 server. The no form of this command will remove the configuration. This command is used to configure the DHCPv6 relay for the specified interface, the address should be the address of another DHCPv6 relay or the address DHCPv6 server. At most three relay addresses can be configured for an interface. To be mentioned, the DHCPv6 relay stops working only if all the relay destination address configurations have been removed. This command is mutually exclusive to "ipv6 dhcp server" and "ipv6 dhcp client pd" commands.	
Example	Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp relay destination 2001:da8::1	

11.1.47 ipv6 dhcp server

Syntax	**ipv6 dhcp server <poolname> [preference <value>] [rapid-commit] [allow-hint]** **no ipv6 dhcp server <poolname>**	
Parameter	**<poolname>**	Name of the created DHCPv6 address pool
	<value>	The priority of the DHCPv6 server, the larger the value, the higher the priority, the range: 0-255, the default is 0.
	rapid-commit	The DHCPv6 server sends the REPLY packet to the client immediately after receiving the SOLICIT packet
	allow-hint	Append the client's expected parameter value to its request packet
Default	DHCPv6 address pool based on port is not configured by default.	
Mode	Port mode	
Usage	This command configures the address pool which will be allocated by the DHCPv6 server through the specified interface. The no form of this command will remove the address pool configuration. This command configure the DHCPv6 address pool which is applied by the DHCPv6 server for the specified interface, as well as optional parameters. One VLAN can bind many DHCPv6 address pools and assign the address for DHCPv6 request packet from direct-link and relay delegation.	
Example	Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ipv6 dhcp server PoolA preference 80 rapid-commit allow-hint	

11.1.48 ipv6 general-prefix

Syntax	**ipv6 general-prefix <prefix-name> <ipv6-prefix/prefix-length>** **no ipv6 general-prefix <prefix-name>**	
Parameter	**<prefix-name>**	***<prefix-name>*** is a character string less than 32 characters, to use as IPv6 general prefix name.
	<ipv6-prefix/prefix-length>	***<ipv6-prefix/prefix-length>*** is defined as IPv6 general prefix.
Default	IPv6 general prefix is not configured by default.	
Mode	Global Mode	
Usage	To define an IPv6 general prefix. The no form of this command will delete the configuration. If IPv6 general prefix is configured, the interface will use the configured prefix for IPv6	

	address generating. Commonly, the general prefix is used for enterprise IPv6 prefix, and when entering an IPv6 address, users can simply add the address suffix of to the name of the general prefix. The configured address prefix will be reserved in the general address prefix pool. At most 8 general prefix can be configured at the same time. When trying to remove a configured general prefix name, the operation will fail if any interfaces used the configured prefix. Only one general prefix for a prefix name. The general prefix cannot use the same prefix definition with prefixes learnt from prefix delegation.	
Example	To set the prefix of 2001:da8:221::/48 to general prefix my-prefix. Switch#config Switch(config)# ipv6 general-prefix my-prefix 2001:da8:221::/48	

11.1.49 ipv6 local pool

Syntax	**ipv6 local pool <poolname> <prefix/prefix-length> <assigned-length>** **no ipv6 local pool <poolname>**	
Parameter	**<poolname>**	***<poolname>*** is the name for the IPv6 address pool of the prefix delegation, the length name string should be less than 32.
	<prefix/prefix-length>	***<prefix/prefix-length>*** is the address prefix and its length of the prefix delegation.
	<assigned-length>	***<assigned-length>*** is the length of the prefix in the address pool which can be retrieved by the client, the assigned prefix length should be no less than the value of ***<prefix-length>***
Default	No IPv6 prefix delegation address pool is configured by default.	
Mode	Global Mode	
Usage	To configure the address pool for prefix delegation. The no form of this command will remove the IPv6 prefix delegation configuration. This command should be used with the "**prefix delegation pool**" command to allocate address prefixes to the clients. If IPv6 prefix delegation is removed, the associated "**prefix delegation**" command will be in-effective either.	
Example	Switch#config Switch(config)#ipv6 local pool 1 1100::1/24 24	

11.1.50 lifetime

Syntax	**lifetime {<valid-time> | infinity} {<preferred-time> | infinity}** **no lifetime**	
Parameter	**<valid-time>**	**The valid lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be greater than <preferred-time>**
	<preferred-time>	The preferred lifetime of the IPv6 address allocated in the local address pool, 1-31536000 seconds, must be less than <valid-time>
	infinity	Longest service life
Default	The default valid life time and preferred life time are 2592000 seconds (30 days) and 604800 seconds (7 days) respectively	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure the life time for the addresses or the address prefixes allocated by DHCPv6. The no form of this command will restore the default setting.	
Example	To configure the valid life time as 1000 seconds, and the preferred life time as 600 seconds. Switch#config Switch(config)#lifetime 1000 600	

11.1.51 network-address

Syntax	**network-address <ipv6-pool-start-address> <ipv6-pool-end-address> | <prefix-length> [eui-64])** **no network-address**	
Parameter	**<ipv6-pool-start-address>**	start of the address pool;
	<ipv6-pool-end-address>	end of the address pool
	<prefix-length>	The length of the address prefix, ranging from 3 to 128, the default is 64
	eui-64	According to the eui-64 standard, IPv6 addresses are allocated, not designated as being allocated in order
Default	No address pool is configured by default.。	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure the DHCPv6 address pool; the no form of this command will remove the	

	address pool configuration. This command configures the address pool for the DHCPv6 server to allocate addresses, only one address range can be configured for each address pool. To be noticed, if the DHCPv6 server has been enabled, and the length of the IPv6 address prefix has been configured, the length of the prefix in the address pool should be no less than the length of the prefix of the IPv6 address of the respective layer three interfaces in the switch. If ***<ipv6-pool-end-address>*** is bigger than ***<ipv6-pool-start-address>***, this command returns at once.
Example	To configure the address range for address pool as 2001:da8:123::100-2001:da8:123::200. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#network-address 2001:da8:123::100 2001:da8:123::200

11.1.52 prefix-delegation

Syntax	**prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>] [lifetime <valid-time> <preferred-time>]** **no prefix-delegation <ipv6-prefix/prefix-length> <client-DUID> [iaid <iaid>]**	
Parameter	**<ipv6-prefix/prefix-length>**	***<ipv6-prefix/prefix-length>*** is the length of the prefix to be allocated to the client.
	<client-DUID>	<client-DUID> is the DUID of the client. DUID with the type of DUID-LLT and DUID-LL are supported, the DUID of DUID-LLT type should be of 14 characters.
	<iaid>	***<iaid>*** is the value to be appended in the IA_PD field of the clients' requests.
	<valid-time>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time
	<preferred-time>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time
Default	Disabled	
Mode	Port mode	
Usage	To configure dedicated prefix delegation for the specified user. The no form of this command will remove the dedicated prefix delegation. This command configures the specified IPv6 address prefix to bind with the specified client. If no IAID is configured, any IA of any clients will be able get this address prefix. At	

	most eight static binding address prefix can be configured for each address pool. For prefix delegation, static binding is of higher priority than the prefix address pool.
Example	The following command will allocate 2001:da8::/48 to the client with DUID as 00010006000000005000BBFAA2408, and IAID as 12. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation 2001:da8::/48 00010006000000005000BBFAA240812

11.1.53 prefix-delegation pool

Syntax	**prefix-delegation pool <poolname> [lifetime <valid-time> <preferred-time>]** **no prefix-delegation pool <poolname>**	
Parameter	**<poolname>**	***<poolname>*** is the name of the address prefix pool, the length name string should be less than 32.
	<valid-time>	The valid life cycle (in seconds) of the IPv6 address assigned to the client, the range is 1-31536000, the default is 2592000, and it must be greater than the preferred-time
	<preferred-time>	The preferred lifetime of the IPv6 address assigned to the client (in seconds), the range is 1-31536000, the default is 604800, and it must be less than valid-time
Default	The prefix delegation name used by DHCPv6 address pool is not configured.	
Mode	DHCPv6 Address Pool Configuration Mode.	
Usage	To configure prefix delegation name used by DHCPv6 address pool. The no form of this command deletes the configuration. This command configures the name of the address prefix pool for address allocation. If configured, the addresses in the prefix address pool will be allocated to the clients. This command can be used in association with the **ipv6 local pool** command. For one address pool, only one prefix delegation pool can be bound. When trying to remove the prefix name configuration, the prefix delegation service of the server will be unavailable, if both the address pool is not associated with the prefix delegation pool and no static prefix delegation binding is enabled.	
Example	Switch#show subnet-vlan Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#prefix-delegation pool abc	

11.1.54 service dhcpv6

Syntax	**service dhcpv6** **no service dhcpv6**
Parameter	none
Default	Disabled
Mode	Global Mode
Usage	To enable DHCPv6 server function; the no form of this command disables the configuration. The DHCPv6 services include DHCPv6 server function, DHCPv6 relay function, DHCPv6 prefix delegation function. All of the above services are configured on ports. Only when DHCPv6 server function is enabled, the IP address assignment of DHCPv6 client, DHCPv6 relay and DHCPv6 prefix delegation functions enabled can be configured on ports.
Example	To enable DHCPv6 server. Switch#config Switch(config)# service dhcpv6

11.1.55 show ipv6 dhcp

Syntax	**show ipv6 dhcp**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	To show the enable switch and DUID of DHCPv6 service To show the enable switch and DUID of DHCPv6 service, server identifier options only use DUID of DUID-LLT type.
Example	Switch#show ipv6 dhcp DHCPv6 is enabled LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d> LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>

11.1.56 show ipv6 dhcp binding

Syntax	**show ipv6 dhcp binding [<ipv6-address>| pd <ipv6-prefix|prefix-length>|count]**	
Parameter	**ipv6-address**	specified IPv6 address;
	count	show the number of DHCPv6 address bindings
Default	none	
Mode	Admin and Configuration Mode	
Usage	To show all the address and prefix binding information of DHCPv6, include type, DUID, IAID, prefix, valid time and so on.	

Example

```
Switch#show ipv6 dhcp binding
Client: iatype IANA, iaid 0x0e001d92
DUID: 00:01:00:01:0f:55:82:4f:00:19:e0:3f:d1:83
IANA leased address: 2001:da8::10
Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
Lease obtained at %Jan 01 01:34:44 1970
Lease expires at %Jan 31 01:34:44 1970 (2592000 seconds left)

The number of DHCPv6 bindings is 1
```

11.1.57 show ipv6 dhcp conflict

Syntax	**show ipv6 dhcp conflict**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	Show the log for the address that have a conflict record.

Example

```
Switch#show ipv6 dhcp
DHCPv6 is enabled
LLT DUID is <00:01:00:01:43:b7:1b:81:00:03:0f:01:5f:9d>
LL DUID is <00:03:00:01:00:03:0f:01:5f:9d>
```

11.1.58 show ipv6 dhcp interface

Syntax	**show ipv6 dhcp interface [<interface-name>]**	
Parameter	**<interface-name>**	***<interface-name>*** is the name and number of interface, if the ***<interface-name>*** parameter is not provided, then all the DHCPv6 interface information will be shown.
Default	none	
Mode	Admin and Configuration Mode	
Usage	To show the information for DHCPv6 interface, include Port Mode (Prefix delegation client. DHCPv6 server. DHCPv6 relay) , and the relative conformation information under all kinds of mode.	
Example	Switch#show ipv6 dhcp interface vlan10 Vlan10 is in server mode Using pool: poolv6 Preference value: 20 Rapid-Commit is disabled	

11.1.59 show ipv6 dhcp pool

Syntax	**show ipv6 dhcp pool [poolname]**	
Parameter	**[poolname]**	***<poolname>*** is the DHCPv6 address pool name which configured already, and the length less than 32 characters. If the ***<poolname>*** parameter is not provided, then all the DHCPv6 address pool information will be shown.
Default	none	
Mode	Admin and Configuration Mode	
Usage	To display the configuration and dynamic assignment information for DHCPv6 address pool, include the name of DHCPv6 address pool, the prefix of DHCPv6 address pool, excluded address, DNS server configuration, relative prefix information and so on. To display assigned address binding number of address pool that is used as address assignment server. To display assigned prefix number of address pool that is used as prefix delegation server	
Example	Switch#show ipv6 dhcp pool poolv6	

11.1.60 show ipv6 dhcp statistics

Syntax **show ipv6 dhcp statistics**

Parameter none

Default none

Mode Admin and Configuration Mode

Usage To show the statistic of all kinds of DHCPv6 packets by DHCPv6 server.

Example

```
Switch#show ipv6 dhcp statistics
Address pools                   1
Active bindings               0
Expiried bindings             0
Malformed message               0

Message                         Received                        Send
DHCP6SOLICIT                      0                               0
DHCP6ADVERTISE                      0                               0
DHCP6REQUEST                        0                               0
DHCP6REPLY                        0                               0
DHCP6RENEW                          0                               0
DHCP6REBIND                       0                               0
DHCP6RELEASE                        0                               0
DHCP6DECLINE                      0                               0
DHCP6CONFIRM                        0                               0
DHCP6RECONFIGURE                      0                               0
DHCP6INFORMREQ                       0                               0
DHCP6RELAYFORW                        0                               0
DHCP6RELAYREPLY                     0                               0
```

Show information	Explanation
Address pools	To configure the number of DHCPv6 address pools;
Active bindings	The number of auto assign addresses;
Expiried bindings	The number of expiried bindings;
Malformed message	The number of malformed messages;
Message Recieved	The statistic of received DHCPv6 packets.
DHCP6SOLICIT	The number of DHCPv6 SOLICIT packets.

DHCP6ADVERTISE	The number of DHCPv6 ADVERTISE packets
DHCPv6REQUEST	The number of DHCPv6 REQUEST packets
DHCP6REPLY	The number of DHCPv6 REPLY packets
DHCP6RENEW	The number of DHCPv6 RENEW packets
DHCP6REBIND	The number of DHCPv6 REBIND packets
DHCP6RELEASE	The number of DHCPv6 RELEASE packets
DHCP6DECLINE	The number of DHCPv6 DECLINE packets
DHCP6CONFIRM	The number of DHCPv6 CONFIRM packets
DHCP6RECONFIGURE	The number of DHCPv6 RECONFIGURE packets
DHCP6INFORMREQ	The number of DHCPv6 INFORMREQ packets
DHCP6RELAYFORW	The number of DHCPv6 RELAYFORW packets
DHCP6RELAYREPLY	The number of DHCPv6 RELAYREPLY packets

11.1.61 show ipv6 general-prefix

Syntax **show ipv6 general-prefix**

Parameter **none**

Default none

Mode Admin and Configuration Mode

Usage To show the IPv6 general prefix pool information, include the prefix number in general prefix pool, the name of every prefix, the interface of prefix obtained, and the prefix value.

Example

```
Switch#show ipv6 general-prefix
IPv6 Prefix my, acquired via Manual configuration
   2001:da8:221::/48
```

11.1.62 show ipv6 local pool

Syntax	**show ipv6 local pool**
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	To show the statistic information of DHCPv6 prefix pool, include the name of prefix pool, the prefix and prefix length as well as assigned prefix length, the number of assigned prefix and information in DHCPv6 address pool.
Example	Switch#show ipv6 local pool Pool Prefix Free In use a 2010::1/0/48 65536 0

11.1.63 ip dhcp relay information option

Syntax	**ip dhcp relay information option** **no ip dhcp relay information option**
Parameter	**none**
Default	The system disables the option82 function by default
Mode	Global Mode
Usage	Set this command to enable the option82 function of the switch Relay Agent. The "**no ip dhcp relay information option**" command is used to disable the option82 function of the switch Relay Agent. Only the DHCP Relay Agents configuring with this command can add option82 to the DHCP request message, and let the server to process it. Before enabling this function, users should make sure that the DHCP service is enabled and the Relay Agent will transmit the udp broadcast messages whose destination port is 67.
Example	Enable the option82 function of the Relay Agent. Switch#config Switch(config)#service dhcp Switch(config)# ip forward-protocol udp bootps Switch(config)# ip dhcp relay information option

11.1.64 ip dhcp relay information option delimiter

Syntax	**ip dhcp relay information option delimiter [colon | dot | slash | space]** **no ip dhcp relay information option delimiter**
Parameter	none
Default	Slash("/")
Mode	Global Mode
Usage	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash. Divide the parameters with the configured delimiters after users have defined them which are used to create suboption (remot-de, circuit-id) of option82 in global mode.
Example	Set the parameter delimiters as dot (".") for suboption of option82. Switch#config Switch(config)#ip dhcp relay information option delimiter dot

11.1.65 ip dhcp relay information option remote-id

Syntax	**ip dhcp relay information option remote-id {standard | <remote-id>}** **no ip dhcp relay information option remote-id**	
Parameter	**standard**	**standard** means the default VLAN MAC format.
	<remote-id>	<remote-id> means the remote-id content of option 82 specified by users, its length cannot exceed 64 characters.
Default	Use standard format to set remote-id of option 82	
Mode	Global Mode	
Usage	Set the suboption2 (remote ID option) content of option 82 added by DHCP request packets (They are received by the interface). The no command sets the additive suboption2 (remote ID option) format of option 82 as standard. The additive option 82 information needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format cannot satisfy server's request.	
Example	Set the suboption remote-id of DHCP option82 as street-1-1. Switch#config Switch(config)#ip dhcp relay information option remote-id street-1-1	

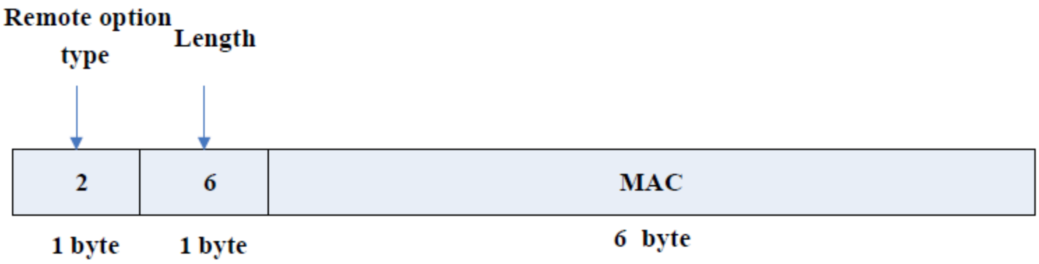
11.1.66 ip dhcp relay information option remote-id format

Syntax	**ip dhcp relay information option remote-id format {default | vs-hp}**	
Parameter	**default**	default means that remote-id is the VLAN MAC address with hexadecimal format.
	vs-up	vs-hp means that remote-id is compatible with the remote-id format of HP manufacturer.
Default	default	
Mode	Global Mode	

Usage

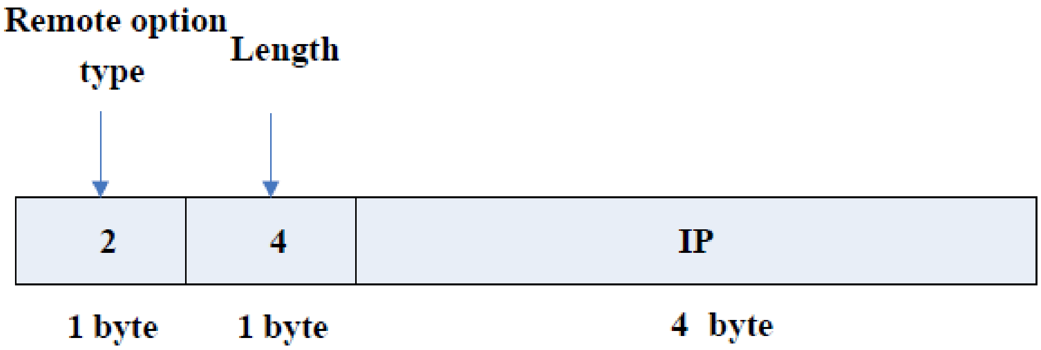
Set remote-id format of Relay Agent option82.

The default remote-id format defined as below:



MAC means VLAN MAC address.

The compatible remote-id format with HP manufacturer defined as below:



IP means the primary IP address of layer 3 interface where DHCP packets from.

Example

Set remote-id of Relay Agent option82 as the compatible format with HP manufacturer.

```
Switch#config
Switch(config)#ip dhcp relay information option remote-id format vs-hp
```

11.1.67 ip dhcp relay information option self-defined remote-id

Syntax	**ip dhcp relay information option self-defined remote-id {hostname | mac | string WORD}** **no ip dhcp relay information option self-defined remote-id**	
Parameter	**WORD**	WORD the defined character string of remote-id by themselves, the maximum length is 64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of remote-id suboption by themselves. After configure this command, if users do not configure remote-id on interface, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occupies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).	
Example	Set self-defined method and character string of remote-id suboption are hostname and abc respectively for option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id hostname string abc	

11.1.68 ip dhcp relay information option self-defined remote-id format

Syntax	**ip dhcp relay information option self-defined remote-id format [ascii | hex]**
Parameter	none
Default	ascii
Mode	Global Mode
Usage	Set self-defined format of remote-id for relay option82. self-defined format use ip dhcp relay information option type self-defined remote-id to create remote-id format.
Example	Set self-defined method of remote-id as hex for relay option82. Switch#config Switch(config)# ip dhcp relay information option self-defined remote-id format hex

11.1.69 ip dhcp relay information option self-defined subscriber-id

Syntax	**ip dhcp relay information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac)| string WORD }** **no ip dhcp relay information option self-defined subscriber-id**
Parameter	**WORD** WORD the defined character string of circuit-id by themselves, the maximum length is 64.
Default	Using standard method.
Mode	Global Mode
Usage	Set creation method for option82, users can define the parameters of circute-id suboption by themselves. After configure this command, if users do not configure circuit-id on interface, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp relay information option delimiter** configuration).
Example	Set self-defined method of circuit-id suboption as port, mac for option82. Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id port id switch-id mac

11.1.70 ip dhcp relay information option self-defined subscriber-id format

Syntax	**ip dhcp relay information option self-defined subscriber-id format [ascii | hex]**
Parameter	none
Default	ascii
Mode	Global Mode
Usage	Set self-defined format of circuit-id for relay option82. self-defined format use ip dhcp relay information option type self-defined subscriber-id to create circuit-id format.
Example	Set self-defined format of circuit-id as hex for relay option82. Switch#config Switch(config)#ip dhcp relay information option self-defined subscriber-id format hex

11.1.71 ip dhcp relay information option subscriber-id

Syntax	**ip dhcp relay information option subscriber-id {standard | <circuit-id>}** **no ip dhcp relay information option subscriber-id**	
Parameter	**<circuit-id>**	***<circuit-id>*** is the circuit-id contents of option82 specified by users, which is a string no longer than 64 characters.
	standard	**standard** means the standard vlan name and physical port name format
Default	The system uses the standard format to set the circuit-id of option 82 by default.	
Mode	Port mode	
Usage	Because the option 82 information added for the switch should cooperate with the third party DHCP server, if the standard circuit-id format of the switch cannot satisfy the server's request, this method will be provided for users to specify the contents of circuit-id according to the situation of the server.	
Example	Set the sub-option circuit-id of DHCP option82 as foobar. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip dhcp relay information option subscriber-id foobar	

11.1.72 ip dhcp relay information option subscriber-id format

Syntax

ip dhcp relay information option subscriber-id format {hex | ascii | vs-hp}

Parameter

hex	hex means that subscriber-id is VLAN and port information with hexadecimal format
ascii	acsii means that subscriber-id is VLAN and port information with ACSII format.
vs-hp	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Default

ascii

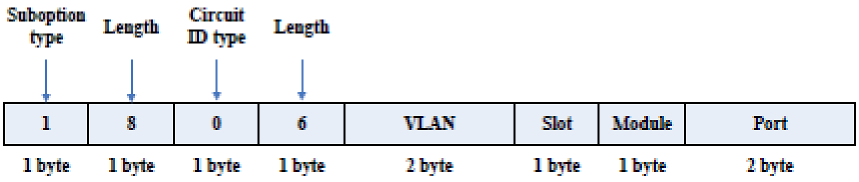
Mode

Global Mode

Usage

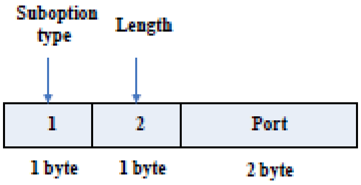
Set subscriber-id format of Relay Agent option82.

VLAN and port information with ASCII format, such as "Vlan1+Ethernet1/0/11", VLAN and port information with hexadecimal format defined as below:



VLAN field fills in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example

Set subscriber-id format of Relay Agent option82 as hexadecimal format.

```
Switch#config
Switch(config)#ip dhcp relay information option subscriber-id format hex
```

11.1.73 ip dhcp relay information policy

Syntax	**ip dhcp relay information policy {drop | keep | replace}** **no ip dhcp relay information policy**	
Parameter	**drop**	drop mode means that if the message has option82, then the system will drop it without processing;
	keep	keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process
	replace	replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process
Default	The system uses replace mode to replace the option 82 segment in the existing message with its own option 82.	
Mode	Port mode	
Usage	This command is used to set the retransmitting policy of the system for the received DHCP request message which contains option82. The "no ip dhcp relay information policy" will set the retransmitting policy of the option 82 DCHP message as "replace". Since the DHCP client messages might go through several DHCP Relay Agents when passed to the DHCP server, the latter Relay Agents on the path should set policies to decide how to process the option82 added by Relay Agents before them. The selection of option 82 retransmitting policies should take the configuration policy of the DHCP server into account.	
Example	Set the retransmitting policy of DHCP messages option 82 as keep. Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp relay information policy keep	

11.1.74 ip dhcp server relay information enable

Syntax	**ip dhcp server relay information enable** **no ip dhcp server relay information enable**
Parameter	none
Default	The system disable the option82 identifying function by default.
Mode	Global Mode
Usage	This command is used to enable the switch DHCP server to identify option82. The "no ip dhcp server relay information enable" command will make the server ignore the option 82. If the users want the switch DHCP server to identify option82 and return option 82 information in the reply message, this command needs to be set, or, the switch DHCP server will ignore the option82.
Example	Set the DHCP server to support option82 Switch#config Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp server relay information enable

11.1.75 show ip dhcp relay information option

Syntax	**show ip dhcp relay information option**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	This command will display the state information of the DHCP option 82 in the system, including option82 enabling switch, the interface retransmitting policy, the circuit ID mode and the switch DHCP server option82 enabling switch. Use this command to check the state information of Relay Agent option82 during operation.
Example	Switch#show ip dhcp relay information option ip dhcp server relay information option(i.e. option 82) is disabled ip dhcp relay information option(i.e. option 82) is enabled Vlan2: ip dhcp relay information policy keep ip dhcp relay information option subscriber-id standard Vlan3: ip dhcp relay information policy replace ip dhcp relay information option subscriber-id foobar

11.1.76 option 43 ascii LINE

Syntax	**option 43 ascii LINE** **no option 43**	
Parameter	**LINE**	The configured option 43 character string with ascii format, its length range between 1 and 255.
Default	No option 43 character string is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 43 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 43.	
Example	Configure option 43 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ascii AP 1000	

11.1.77 option 43 hex WORD

Syntax	**option 43 hex WORD** **no option 43**	
Parameter	**WORD**	The configured option 43 character string with hex format, such as a1241b.
Default	No option 43 is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 43 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 43. When using hex method to configure option 43, the string needs to be written according to TLV (Type-Length-Value) format. For example, issue ip address of 10.1.1.1 through option 43, then the hex string here should be 01040A010101; Type=0x01, it means IP address; Length=0x04, it means the length of IP address is 4 Bytes; Value=0x0A010101, it means the hexadecimal format of 10.1.1.1.	
Example	Configure option 43 with hex format to be "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 hex 01040a010101	

11.1.78 option 43 ip A.B.C.D

Syntax	**option 43 ip A.B.C.D** **no option 43**	
Parameter	**A.B.C.D**	The configured option 43 with IP format, such as 192.168.1.1.
Default	No option 43 is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 43 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 43. Using this command to configure option 43, such as "192.168.1.1", then option 43 filled in packets is "C0A80101".	
Example	Configure option 43 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 43 ip 192.168.1.1	

11.1.79 option 60 ascii LINE

Syntax	**option 60 ascii LINE** **no option 60**	
Parameter	**LINE**	The configured option 60 character string with ascii format, its length range between 1 and 255.
Default	No option 60 character string is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 60 character string with ascii format in ip dhcp pool mode. The no command deletes the configured option 60.	
Example	Configure option 60 with ascii format to be "AP 1000". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ascii AP 1000	

11.1.80 option 60 hex WORD

Syntax	**option 60 hex WORD** **no option 60**	
Parameter	**WORD**	The configured option 60 character string with hex format, such as a1241b
Default	No option 60 is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 60 character string with hex format in ip dhcp pool mode. The no command deletes the configured option 60.	
Example	Configure option 60 with hex format to be "01040a010101". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 hex 01040a010101	

11.1.81 option 60 ip A.B.C.D

Syntax	**option 60 ip A.B.C.D** **no option 60**	
Parameter	**A.B.C.D**	The configured option 60 with IP format, such as 192.168.1.1.
Default	No option 60 is configured.	
Mode	DHCP Address Pool Mode	
Usage	Configure option 60 character string with IP format in ip dhcp pool mode. The no command deletes the configured option 60. Using this command to configure option 60, such as "192.168.1.1", option 60 of packets matched with the configured option 60 is "C0A80101".	
Example	Configure option 60 with IP format to be "192.168.1.1". Switch#config Switch(config)#ip dhcp pool a switch (dhcp-a-config)#option 60 ip 192.168.1.1	

11.1.82 address range

Syntax	**address range <start-ip> <end-ip>** **no address range <start-ip> <end-ip>**	
Parameter	**<start-ip>**	defines the start address of the address pool
	<end-ip>	defines the end address of the address pool
Default	None	
Mode	DHCPv6 address pool class configuration mode	
Usage	This command is used to set address range for a DHCPv6 class in DHCPv6 address pool configuration mode, the no command is used to remove the address range. The prefix/plen form is not supported. It is necessary to check the address range assigned to class in order to make sure that it doesn't exceed the address range of relevant address pool. A class is assigned a single address range and the address range assigned to different class in the same address pool can overlap. If you do not use this command to assign address range for a DHCPv6 cass, then the range for it will be the whole subnet of the address pool by default.	
Example	Associate a DHCPv6 class named CLASS1 to dhcpv6 pool 1 and assign the address range from 2001:da8:100:1::2 to 2001:da8:100:1::30 for CLASS1. Switch#config Switch(config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1 Switch(dhcp-1-class-CLASS1-config)#address range 2001:da8:100:1::2 2001:da8:100:1::30	

11.1.83 class

Syntax	**class <class-name>** **no class <class-name>**	
Parameter	**<class-name>**	name of DHCPv6 class.
Default	none	
Mode	DHCPv6 address pool class configuration mode	
Usage	This command associates class to address pool in DHCPv6 address pool configuration mode and enters class configuration mode in address pool. Use the no command to remove the link. It is recommended to define this class first using global command of IPv6 DHCP class. No class will be created if you input a class name which doesn't exist.	
Example	Associate the DHCPv6 class named CLASS1 to dhcpv6 pool 1. Switch(Config)#ipv6 dhcp pool 1 Switch(dhcp-1-config)#class CLASS1	

11.1.84 ipv6 dhcp class

Syntax	**ipv6 dhcp class <class-name>** **no ipv6 dhcp class <class-name>**	
Parameter	**<class-name>**	the name of DHCPv6 class which is a string with a length of less than 32
Default	none	
Mode	Global Mode	
Usage	This command defines a DHCPv6 class and enters DHCPv6 class configuration mode, the no operation of this command removes this DHCPv6 class. Configure a group of option 37 or option 38, or configure option 37 and option 38 simultaneously in a DHCPv6 class. This command can be used when the server supports DHCPv6 class only.	
Example	Define a DHCPv6 class named CLASS1. Switch(config)#ipv6 dhcp class CLASS1	

11.1.85 ipv6 dhcp relay remote-id

Syntax	**ipv6 dhcp relay remote-id <remote-id>** **no ipv6 dhcp relay remote-id**	
Parameter	**<remote-id>**	user-defined content of option 37.
Default	Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.	
Mode	Port mode	
Usage	This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the remote-id in user-defined option 37 and it is a string with a length of less than 128. The no operation of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address. Because the option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify the remote-id content based on server condition when default remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.	
Example	Enable abc as the remote-id of DHCPv6 option 37. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay remote-id abc	

11.1.86 ipv6 dhcp relay remote-id option

Syntax	**ipv6 dhcp relay remote-id option** **no ipv6 dhcp relay remote-id option**
Parameter	**none**
Default	Disable the relay option 37.
Mode	Global Mode
Usage	This command enables switch relay to support the option 37, the no form of this command disables it. Only after this command is configured, DHCPv6 relay agent can add option 37 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command.
Example	Enable the switch relay to support option 37. Switch#config Switch(config)#service dhcpv6 Switch(config)#ipv6 dhcp relay remote-id option

11.1.87 ipv6 dhcp relay subscriber-id

Syntax	**ipv6 dhcp relay subscriber-id <subscriber-id>** **no ipv6 dhcp relay subscriber-id**
Parameter	**<subscriber-id>** user-defined content of option 38
Default	Set subscriber-id in option 38 to vlan name together with port name.
Mode	Port mode
Usage	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the subscriber-id in user-defined option 38 and it is a string with a length of less than 128. Because the option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify the subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as the subscriber-id in option 38 by default.
Example	Enable abc as the subscriber-id of DHCPv6 option 38. Switch#config Switch(config) # interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp relay subscriber-id abc

11.1.88 ipv6 dhcp relay subscriber-id option

Syntax	**ipv6 dhcp relay subscriber-id option** **no ipv6 dhcp relay subscriber-id option**
Parameter	**none**
Default	Disable the relay option 38.
Mode	Global Mode
Usage	Only after this command is configured, DHCPv6 relay agent can add option 38 in DHCPv6 request packets before sending it to server or next relay agent. Make sure that DHCPv6 service has been enabled before execute this command. The option 38 of switch relay is disabled by default.
Example	Enable the switch relay to support option 38. Switch#config Switch(config) # service dhcpv6 Switch(Config)#ipv6 dhcp relay subscriber-id option

11.1.89 ipv6 dhcp relay subscriber-id select delimiter

Syntax	**ipv6 dhcp relay subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)** **no ipv6 dhcp relay subscriber-id select delimiter**	
Parameter	**(sp | sv | pv | spv)**	a selection in combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.
	WORD	the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two **delimiter WORDs** here, of which the former is the delimiter between slot and port and the latter is the one between port and vlan.
Default	Null	
Mode	Global Mode	
Usage	Configures user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name. The command has no effect on ports with self-defined subscriber-id. If user redefines the subscriber-id of the port after using the command, the user-defined one prevails. This configuration is null by default.	
Example	Switch#config Switch(config)#ipv6 dhcp relay subscriber-id select sp delimiter #	

11.1.90 ipv6 dhcp server remote-id option

Syntax	**ipv6 dhcp server remote-id option** **no ipv6 dhcp server remote-id option**
Parameter	None
Default	Do not support option 37.
Mode	Global Mode
Usage	This command enables DHCPv6 server to support the identification of option 37, the no form of this command disables it. Configure this command if option 37 options is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. Option 37 is not supported by default.
Example	Enable the DHCPv6 server to support option 37. Switch#config Switch(config)#ipv6 dhcp server remote-id option

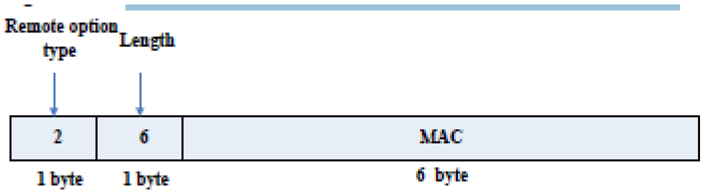
11.1.91 ip dhcp server select relay-forw

Syntax	**ipv6 dhcp server select relay-forw** **no ipv6 dhcp server select relay-forw**
Parameter	none
Default	Selecting option 37 and option 38 of the original packets.
Mode	Global Mode
Usage	This command enables the DHCPv6 server to support selections when multiple option 37 or option 38 options exist and the option 37 and option 38 of relay-forw in the innermost layer are selected. The no operation of it restores the default configuration, i.e. selecting option 37 and option 38 of the original packets. Make sure that the server has been enabled to support option 37 and option 38 before use this command. The system selects option 37 and option 38 of the original packets by default.
Example	Configure that the vlan1 interface of DHCPv6 server selects option 37 and option 38 of relay-forw in the innermost layer. Switch#config Switch(config)#interface vlan 1 Switch(config-if-vlan1)# ipv6 dhcp server select relay-forw

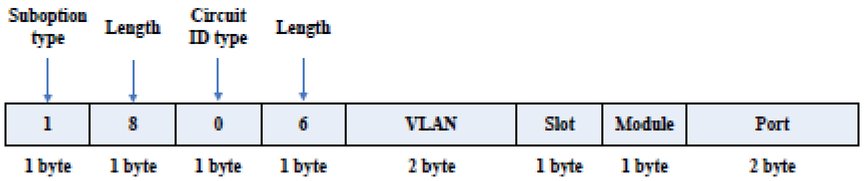
11.1.92 ipv6 dhcp server subscriber-id option

Syntax	**ipv6 dhcp server subscriber-id option** **no ipv6 dhcp server subscriber-id option**
Parameter	none
Default	Do not support option 38.
Mode	Global Mode
Usage	This command enables DHCPv6 server to support the identification of option 38, the no operation of this command disables it. Configure this command if option 38 is expected to be identified and processed by DHCPv6 server, otherwise they will be ignored. option 38 is not supported by default.
Example	Enable DHCPv6 server to support option 38. Switch#config Switch(config)#ipv6 dhcp server subscriber-id option

11.1.93 ipv6 dhcp snooping information option remote-id format

Syntax	**ipv6 dhcp snooping information option remote-id format {hex | ascii }**	
Parameter	**hex**	Hex means that the remote-id is the VLAN MAC address of the hexadecimal switch.
	ascii	acsii means that the remote-id is the VLAN MAC address of the acsii format switch.
Default	ascii	
Mode	Global Mode	
Usage	This command can configure the remote-id format of the switch relay agent's DHCPv6 option37. The hexadecimal remote-id format's definition is as below:  The MAC is the VLAN MAC address of the switch.	
Example	Configure the default remote-id format of the switch relay agent's DHCPv6 option37. Switch#config Switch(config)#ipv6 dhcp snooping information option remote-id format ascii	

11.1.94 ipv6 dhcp snooping information option subscriber-id format

Syntax	**ipv6 dhcp snooping information option subscriber-id format {hex | ascii }**	
Parameter	**hex**	hex means that the subscriber-id is the hexadecimal VLAN and port information
	ascii	acsii means that the subscriber-id is the ACSII VLAN and port information.
Default	ascii	
Mode	Global Mode	
Usage	Configure the default subscribe-id format of the switch DHCPv6 snooping option38. The ACSII VLAN and port information is as Vlan1+Ethernet1/0/11. The hexadecimal VLAN and port information is defined as below:  The VLAN field is written with the switch VLAN ID. For the rackmount switch, Slot means the slot number; for the cassette switch, it is 1. The default module is 0. Port means the port number and starts from 1.	
Example	Configure the subscribe-id format of the switch DHCPv6 snooping option38 as the hexadecimal format. Switch#config Switch(config)#ipv6 dhcp snooping information option subscriber-id format hex	

11.1.95 ipv6 dhcp snooping remote-id

Syntax	**ipv6 dhcp snooping remote-id <remote-id>** **no ipv6 dhcp snooping remote-id**
Parameter	**<remote-id>** user-defined content of option 37.
Default	Using vlan MAC address as remote-id content by default such as "00-01-ac-12-23" with '-' hyphen.
Mode	Port mode
Usage	This command is used to set the form of adding option 37 in received DHCPv6 request packets, of which <remote-id> is the content of remote-id in user-defined option 37 and it is a string with a length of less than 128. The no form of this command restores remote-id in option 37 to enterprise-number together with vlan MAC address. Because option 37 information added by switch may associate with third-party DHCPv6 servers, users can specify remote-id content based on server condition when standard remote-id of the switch cannot satisfy the demand of server. The enterprise-number together with vlan MAC address is used as the remote-id by default.
Example	Enable abc as remote-id of DHCPv6 option 37. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-Ethernet1/0/1)#ipv6 dhcp snooping remote-id abc

11.1.96 ipv6 dhcp snooping remote-id option

Syntax	**ipv6 dhcp snooping remote-id option** **no ipv6 dhcp snooping remote-id option**
Parameter	none
Default	Disable.
Mode	Global Mode
Usage	This command enables DHCPv6 SNOOPING to support option 37, the no form of this command disables it. Only after this command is configured, DHCPv6 SNOOPING can add option 37 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before execute this command. The system disables option 37 of DHCPv6 SNOOPING by default.
Example	Enable option 37 in DHCPv6 SNOOPING. Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping remote-id option

11.1.97 ipv6 dhcp snooping remote-id policy

Syntax	**ipv6 dhcp snooping remote-id policy {drop | keep | replace}** **no ipv6 dhcp snooping remote-id policy**	
Parameter	**drop**	The system only discards it via option 37
	keep	The system keeps option 37 unchanged and forwards the packet
	replace	The system will replace the option 37 field in the existing message with its own option 37 before forwarding the message to the server.
Default	Using replace mode to replace option 37 of current packets with system's own.	
Mode	Global Mode	
Usage	Since DHCPv6 client packets may already include option 37 information, corresponding processing policy of DHCPv6 SNOOPING is required to develop. If the forwarding policy is set as **replace**, option 37 has to be enabled in advance. Use replace mode to replace option 37 of current packets with system's own by default.	
Example	Configure the reforward policy of DHCPv6 packets with option 37 as keep for DHCPv6 SNOOPING Switch#config Switch(config)#ipv6 dhcp snooping remote-id policy keep	

11.1.98 ipv6 dhcp snooping subscriber-id

Syntax	**ipv6 dhcp snooping subscriber-id <subscriber-id>** **no ipv6 dhcp snooping subscriber-id**	
Parameter	<subscriber-id>	user-defined content of option 38
Default	Set subscriber-id in option 38 to vlan name together with port name.	
Mode	Port mode	
Usage	This command is used to set the form of adding option 38 in received DHCPv6 request packets, of which <subscriber-id> is the content of subscriber-id in user-defined option 38 and it is a string with a length of less than 128. The no operation of this command restores subscriber-id in option 38 to vlan name together with port name such as "Vlan2+Ethernet1/0/2". Because option 38 information added by switch may associate with third-party DHCPv6 servers, users can specify subscriber-id content based on server condition when standard subscriber-id of the switch cannot satisfy the demand of server. The vlan name together with physical port name is used as subscriber-id in option 38 by default.	
Example	Enable abc as subscriber-id of DHCPv6 option 38. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping subscriber-id abc	

11.1.99 ipv6 dhcp snooping subscriber-id option

Syntax	**ipv6 dhcp snooping subscriber-id option** **no ipv6 dhcp snooping subscriber-id option**
Parameter	none
Default	Disable option 38 of DHCPv6 SNOOPING.
Mode	DHCP Address Pool Mode
Usage	This command enables DHCPv6 SNOOPING to support option 38, the no form of this command disables it. Only after this command is configured, DHCPv6 SNOOPING can add option 38 in DHCPv6 packets before sending it to server or relay agent. Make sure that DHCPv6 SNOOPING has been enabled before executing this command.The system disables option 38 of DHCPv6 SNOOPING by default.
Example	Enable option 38 in DHCPv6 SNOOPING. Switch#config Switch(config)#ipv6 dhcp snooping enable Switch(config)#ipv6 dhcp snooping subscriber-id option

11.1.100 ipv6 dhcp snooping subscriber-id policy

Syntax	**ipv6 dhcp snooping subscriber-id policy {drop | keep | replace}** **no ipv6 dhcp snooping subscriber-id policy**	
Parameter	**drop**	The system only discards it via option 38
	keep	The system keeps option 38 unchanged and forwards the packet
	replace	The system will replace the option 38 field in the existing message with its own option 38 before forwarding the message to the server.
Default	Using replace mode to replace option 38 of current packets with system's own.	
Mode	Global Mode	
Usage	Since DHCPv6 client packets may already include option 38 information, corresponding processing policy of DHCPv6 SNOOPING is requested to develop. If the reforward policy is set as **replace**, option 38 has to be enabled in advance. The system disables option 38 of DHCPv6 SNOOPING by default.	
Example	Set the reforward policy of DHCPv6 packets with option 38 as keep for DHCPv6 SNOOPING. Switch#config Switch(config)#ipv6 dhcp snooping subscriber-id policy keep	

11.1.101 ipv6 dhcp snooping subscriber-id select delimiter

Syntax

ipv6 dhcp snooping subscriber-id select (sp | sv | pv | spv) delimiter WORD (delimiter WORD |)

no ipv6 dhcp snooping subscriber-id select delimiter

Parameter

(sp | sv | pv | spv) a selection from combinations of slot, port and vlan, among which **sp** represents slot and port, **sv** represents slot and vlan, **pv** represents port and vlan, and **spv** represents slot, port and vlan.

WORD the delimiter between slot, port and vlan which ranges among (#|.|,|;|:|/|space). Note that there're two delimiter WORDs here, of which the former is the delimiter between slot and port while the latter is that between port and vlan.

Default

null

Mode

Global Mode

Usage

Configure user configuration options to generate subscriber-id. The no form of this command restores to its original default configuration, i.e. vlan name together with port name.

This command has no effect on ports with self-defined subscriber-id. If a user redefines subscriber-id of the port after configuring the command, the user-defined one prevails. This configuration is null by default.

Example

```
Switch#config
Switch(config)#ipv6 dhcp snooping subscriber-id select sv delimiter #
```

11.1.102 ipv6 dhcp use class

Syntax

ipv6 dhcp use class

no ipv6 dhcp use class

Parameter

none

Default

DHCPv6 server supports DHCPv6 class during address assignment.

Mode

Global Mode

Usage

This command enables DHCPv6 server to support DHCPv6 class during address assignment, the no operation of this command disables it without removing the relative DHCPv6 class information that has been configured.

By default, DHCPv6 servers support DHCPv6 class during address assignment and the no form of this command doesn't remove DHCPv6 class information that has been configured. Make sure that DHCPv6 service has been enabled before using this

	command. DHCPv6 server supports DHCPv6 class during address assignment by default.
Example	Configure DHCPv6 server to support DHCPv6 class during address assignment. Switch#config Switch(config)# ipv6 dhcp use class

11.1.103 remote-id subscriber-id

Syntax	**{remote-id [*] <remote-id> [*] | subscriber-id [*] <subscriber-id> [*]}**
	no {remote-id [*] <remote-id> [*] | subscriber-id [*] < subscriber-id> [*]}	

Parameter	**<remote-id>**	a string with a length ranging from 1 to 128 bytes is used to match remote-id in option 37.
	<subscriber-id>	a string with a length ranging from 1 to 128 bytes is used to match subscriber-id in option 38.
	[*]	match zero or more characters.
Default	None	
Mode	IPv6 DHCP Class configuration mode	
Usage	This command configures option 37 and option 38 that match the class in IPv6 DHCP class configuration mode. This command configures a mode which matches with the already-defined DHCPv6 class, and a DHCPv6 class may configure multiple commands. If this command is ignored and no mode configured in IPv6 DHCP Class mode, any remote-id or subscriber-id is considered to match with the DHCPv6 class, however, remote-id or subscriber-id must exist in DHCPv6 packet.	
Example	Configure some remote-id or subscriber-id belonging to DHCPv6 class named CLASS1. Switch#config Switch(config)#ipv6 dhcp class CLASS1 Switch(dhcpv6-class-class1-config)#remote-id abc* subscriber-id bcd* Switch(dhcpv6-class-class1-config)#remote-id edf* Switch(dhcpv6-class-class1-config)#subscriber-id *mmn	

11.1.104 show ipv6 dhcp relay option

Syntax	**show ipv6 dhcp relay option**
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Use this command to check relay agents' configuration status for option 37 and option 38.
Example	Switch#show ipv6 dhcp relay option remote-id option enable subscriber-id option enable Interface Vlan 1: remote-id option configure "abc"

11.1.105 show ipv6 dhcp snooping option

Syntax	**show ipv6 dhcp snooping option**
Parameter	none
Default	none
Mode	Admin and Configuration Mode
Usage	Use this command to check snooping configuration status for option 37 and option 38.
Example	Switch#show ipv6 dhcp snooping option remote-id option enable subscriber-id option enable The slot port vlan select option is : port and vlan The delimiter is : #

11.1.106 enable trustview key

Syntax	**enable trustview key {0 | 7} <password>** **no enable trustview key**	
Parameter	**<password>**	***<password>*** is character string length less than 16, which use as encrypted key.
	{0 | 7}	0 for un-encrypted text for the password, while 7 for encrypted.
Default	Disabled	
Mode	Global Mode	
Usage	To configure DES encrypted key for private packets, this command is also the switch for the private packets encrypt and hash function enabled or not. The switch communicates with the TrustView management system through private protocols. By default these packets are not encrypted. In order to prevent spoofing, it can be configured to encrypt these packets. And at the same time, the same password should be configured on TrustView server.	
Example	Enable encrypt or hash function of private message Switch#config Switch(config)# enable trustview key 0 switch	

11.1.107 ip dhcp snooping

Syntax	**ip dhcp snooping enable** **no ip dhcp snooping enable**
Parameter	none
Default	DHCP Snooping is disabled by default
Mode	Global Mode
Usage	Enable the DHCP Snooping function. When this function is enabled, it will monitor all the DHCP Server packets of non-trusted ports.
Example	Enable the DHCP Snooping function. Switch#config Switch(config)#ip dhcp snooping enable

11.1.108 ip dhcp snooping action

Syntax	**ip dhcp snooping action {shutdown | blackhole} [recovery <second>]** **no ip dhcp snooping action**	
Parameter	**shutdown**	When the port detects a fake DHCP Server, it will be shutdown.
	blackhole	When the port detects a fake DHCP Server, the vid and source MAC of the fake packet will be used to block the traffic from this MAC.
	recovery	Users can set to recover after the automatic defense action being executed.(no shut ports or delete correponding blackhole）.
	<second>	Users can set how long after the execution of defense action to recover. The unit is second, and valid range is 10-3600.
Default	No default defense action.	
Mode	Port mode	
Usage	Set or delete the automatic defense action of a port. Only when DHCP Snooping is globally enabled, can this command be set. Trusted port will not detect fake DHCP Server, so, will never trigger the corresponding defense action. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted.	
Example	Set the DHCP Snooping defense action of port ethernet1/0/1 as setting blackhole, and the recovery time is 30 seconds. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#ip dhcp snooping action blackhole recovery 30	

11.1.109 ip dhcp snooping action MaxNum

Syntax	**ip dhcp snooping action {<maxNum>|default}**	
Parameter	**<maxNum>**	the number of defense action on each port, the range of which is 1-200, and the value of which is 10 by default.
	default	recover to the default value.
Default	The default value is 10.	
Mode	Global Mode	
Usage	Set the number of defense action that can be simultaneously took effect. Set the max number of defense actions to avoid the resource exhaustion of the switch caused by attacks. If the number of alarm information is larger than the set value, then the earliest defense action will be recovered forcibly in order to send new defense actions.	
Example	Set the number of port defense actions as 100. Switch#config Switch(config)#ip dhcp snooping action 100	

11.1.110 ip dhcp snooping binding

Syntax	**ip dhcp snooping binding enable** **no ip dhcp snooping binding enable**
Parameter	**none**
Default	DHCP Snooping binding is disabled by default.
Mode	Global Mode
Usage	Enable the DHCP Snooping binding funciton When the function is enabled, it will record the binding information allocated by DHCP Server of all trusted ports. Only after the DHCP SNOOPING function is enabled, the binding function can be enabled.
Example	Enable the DHCP Snooping binding funciton. Switch#config Switch(config)#ip dhcp snooping binding enable

11.1.111 ip dhcp snooping binding dot1x

Syntax	**ip dhcp snooping binding dot1x** **no ip dhcp snooping binding dot1x**
Parameter	**none**
Default	By default, the binding DOT1X funciton is disabled on all ports.
Mode	Port mode
Usage	When this function is enabled, DHCP SNOOPING will notify the DOT1X module about the captured bindng information as a DOT1X controlled user. This command is mutually exclusive to"ip dhcp snooping binding user-contro"command. Only after the DHCP SNOOPING binding function is enabled, the binding dot1x function can be set.
Example	Enable the binding DOT1X funciton on port ethernet1/0/1. Switch#config Switch(config) #interface ethernet 1/0/1 switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding dot1x

11.1.112 ip dhcp snooping binding user

Syntax	**ip dhcp snooping binding user <mac> address <ipaddress> vlan <vlan-id> interface [Ethernet] <ifname>** **no ip dhcp snooping binding user <mac> interface [Ethernet] <ifname>**	
Parameter	**<mac>**	The MAC address of the static binding user, whic is the only index of the binding user.
	<ipaddress>	The IP address of the static binding user
	<vlan-id>	The VLAN ID of static binding user
	<ifname>	The access interface of static binding user
Default	DHCP Snooping has no static binding list entry by default.	
Mode	Global Mode	
Usage	The static binding users is deal in the same way as the dynamic binding users captured by DHCP SNOOPING; the follwoing actions are all allowed: notifying DOT1X to be a controlled user of DOT1X, adding a trusted user list entry directly, adding a bingding ARP list entry. The static binding uses will never be aged, and have a priority higher than dynamic binding users. Only after the DHCP SNOOPING binding function is enabled, the static binding users can be enabled.	
Example	Configure static binding users. Switch#config Switch(config)#ip dhcp snooping binding user 00-11-22-33-44-55 address 1.1.1.1 vlan 1 interface ethernet 1/0/14	

11.1.113 ip dhcp snooping binding user-control

Syntax	**ip dhcp snooping binding user-control** **no ip dhcp snooping binding user-control**
Parameter	None
Default	By default, the binding user funciton is disabled on all ports.
Mode	Port mode
Usage	When this function is enabled, DHCP SNOOPING will treat the captured binding information as trusted users allowed to access all resources. This command is mutually exclusive to “ip dhcp snooping binding dot1x“ command. Only after DHCP SNOOPING binding function is enabled, the binding user function can be set. This command is not limited by “ip dhcp snooping“ based on VLAN, but it is only limited by the global “ip dhcp snooping enable“ command.
Example	Enable the binding USER funciton on port ethernet1/0/1. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(Config-Ethernet 1/0/1)# ip dhcp snooping binding user-control

11.1.114 ip dhcp snooping binding user-control max-user

Syntax	**ipv6 dhcp snooping binding user-control max-user <number>** **no ip dhcp snooping binding user-control max-user**	
Parameter	**<number>**	***<number>*** the max number of users allowed to access the port, from 0 to 1024.
Default	The max number of users allowed by each port to access is 1024.	
Mode	Port mode	

Usage

Set the max number of users allowed to access the port when enabling DHCP Snooping binding user funciton; the no operation of this command will restore default value.

This command defines the max number of trust users distributed according to binding information, with **ip dhcp snooping binding user-contrl** enabled on the port. By default, the number is 1024. Considering the limited hardware resources of the switch, the actual number of trust users distributed depends on the resource amount. If a bigger max number of users is set using this command, DHCP Snooping will distribute the binding informaiton of untrust users to hardware to be trust users as long as there is enough available resources. Otherwise, DHCP Snooping will change the distributed binging informaiton accordint to the new smaller max user number. When the number of distributed bingding informaiton entries reaches the max limit, no new DHCP will be able to become trust user or to access other network resouces via the switch.

Example

Enable DHCP Snooping binding user funtion on Port ethernet1/0/1, setting the max number of user allowed to access by Port Ethernet1/0/1 as 5. ◦

```
Switch#config
Switch(config)#interface ethernet 1/0/1
Switch(config-ethernet 1/0/1)#ip dhcp snooping binding user-control max-user 5
```

11.1.115 ip dhcp snooping information enable

Syntax	**ip dhcp snooping information enable** **no ip dhcp snooping information enable**
Parameter	none
Default	Option 82 function is disabled in DHCP Snooping by default.
Mode	Global Mode
Usage	This command will enable option 82 function of DHCP Snooping on the switch, the no operation of this command will disable that function. Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like vlan1+ethernet1/0/12. That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like 00030f023301. If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.
Example	Enable option 82 function of DHCP Snooping on the switch. Switch#config Switch(config)#ip dhcp snooping enable Switch(config)# ip dhcp snooping binding enable Switch(config)# ip dhcp snooping information enable

11.1.116 ip dhcp snooping information option allow-untrusted (replace|)

Syntax	**ip dhcp snooping information option allow-untrusted (replace)** **no ip dhcp snooping information option allow-untrusted (replace)**	
Parameter	**(replace)**	When the "replace" is setting, the potion82 option is allowed to replace.
Default	Drop DHCP packets with option82 option received by untrusted ports.	
Mode	Global Mode	
Usage	This command is used to set that allow untrusted ports of DHCP snooping to receive DHCP packets with option82 option. When disabling this command, all untrusted ports will drop DHCP packets with option82 option. Usually the switch with DHCP snooping function connects the terminal user directly, so close allow-untrusted by default to avoid option82 option added by user privately. Please set uplink port as trust port when enabling the uplink of DHCP snooping function.	
Example	Enable the function that receives DHCP packets with option82 Switch#config Switch(config)#ip dhcp snooping information option allow-untrusted	

11.1.117 ip dhcp snooping information option delimiter

Syntax	**ip dhcp snooping information option delimiter [colon | dot | slash | space]** **no ip dhcp snooping information option delimiter**
Parameter	none
Default	slash（“/”）
Mode	Global Mode
Usage	Set the delimiter of each parameter for suboption of option82 in global mode, no command restores the delimiter as slash. Divide parameters with the configured delimiters after users have defined them which are used to create suboption (remote-id, circuit-id) of option82 in global mode.
Example	Set the parameter delimiters as dot (“.”) for suboption of option82. Switch#config Switch(config)#ip dhcp snooping information option delimiter dot

11.1.118 ip dhcp snooping information option remote-id

Syntax	**ip dhcp snooping information option remote-id {standard | <remote-id>}** **no ip dhcp snooping information option remote-id**	
Parameter	**standard**	standard means the default VLAN MAC format
	<remote-id>	***<remote-id>*** means the remote-id content of option 82 specified by users, its length can not exceed 64 characters.
Default	Use standard format to set remote-id.	
Mode	Global Mode	
Usage	The additive option 82 needs to associate with third-party DHCP server, it is used to specify the remote-id content by users when the standard remote-id format can not satisfy server's request 。	
Example	Set the suboption remote-id of DHCP option82 as street-1-1. Switch#config Switch(config)#ip dhcp snooping information option remote-id street-1-1	

11.1.119 ip dhcp snooping information option self-defined remote-id

Syntax	**ip dhcp snooping information option self-defined remote-id {hostname | mac | string WORD}** **no ip dhcp snooping information option self-defined remote-id**	
Parameter	**WORD**	**WORD** the defined character string of remote-id by themselves, the maximum length is 64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of remote-id suboption by themselves. After configure this command, if users do not configure ip dhcp snooping information option remote-id globally, it will create remote-id suboption for option82 according to self-defined method. For mac, use the format such as 00-02-d1-2e-3a-0d if it is filled to packets with ascii format, but hex format occpies 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).	
Example	Set self-defined method and character string of remote-id suboption are mac and abc respectively for option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id mac string abc	

11.1.120 ip dhcp snooping information option self-defined remote-id format

Syntax	**ip dhcp snooping information option self-defined remote-id format [ascii | hex]**	
Parameter	**hex**	hex means that the remote-id is the hexadecimal VLAN and port information
	ascii	acsii means that the remote-id is the ACSII VLAN and port information.
Default	ascii	
Mode	Global Mode	
Usage	Set self-defined format of remote-id for snooping option82. self-defined format use ip dhcp snooping information option type self-defined remote-id to create remote-id format.	
Example	Set self-defined format of remote-id as hex for snooping option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined remote-id format hex	

11.1.121 ip dhcp snooping information option self-defined subscriber-id

Syntax	**ip dhcp snooping information option self-defined subscriber-id {vlan | port | id (switch-id (mac | hostname)| remote-mac) | string WORD}** **no ip dhcp snooping information option type self-defined subscriber-id**	
Parameter	**WORD**	**WORD** the defined character string of circuit-id by themselves, the maximum length is 64.
Default	Using standard method.	
Mode	Global Mode	
Usage	Set creation method for option82, users can define the parameters of circute-id suboption by themselves. After configure this command, if users do not configure circuit-id on port, it will create circuit-id suboption for option82 according to self-defined method. Self-defined format of circuit-id: if self-defined subscriber-id format is ascii, the filled format of vlan such as "Vlan2", the format of port such as "Ethernet1/0/1", the format of mac and remote-mac such as "00-02-d1-2e-3a-0d". If self-defined format is hex, the filled format of vlan occupies 2 bytes, port occupies 4 bytes, a byte means slot (for chassis switch, it means slot ID, for box switch, it is 1), a byte means Module (the default is 0), two bytes means port ID beginning from 1, mac and remote-mac occupy 6 bytes. Each option will be filled to packets according to the configured order of the commands and divide them with delimiter (delimiter is **ip dhcp snooping information option delimiter** configuration).	
Example	Set self-defined method of circuit-id suboption as vlan, port, mac and remote-mac for option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id vlan port id remote-mac	

11.1.122 ip dhcp snooping information option self-defined subscriber-id format

Syntax	**ip dhcp snooping information option self-defined subscriber-id format [ascii | hex]**	
Parameter	**hex**	hex means that the subscriber-id is the hexadecimal VLAN and port information
	ascii	acsii means that the subscriber-id is the ACSII VLAN and port information.
Default	ascii	
Mode	Global Mode	
Usage	Set self-defined format of circuit-id for snooping option82. self-defined format uses ip dhcp snooping information option type self-defined subscriber-id to create circuit-id format.	
Example	Set self-defined format of circuit-id as hex for snooping option82. Switch#config Switch(config)#ip dhcp snooping information option self-defined subscriber-id format hex	

11.1.123 ip dhcp snooping information option subscriber-id

Syntax	**ip dhcp snooping information option subscriber-id {standard | <circuit-id>}** **no ip dhcp snooping information option subscriber-id**	
Parameter	**standard**	standard means the standard format of VLAN name and physical port name, such as Vlan2+Ethernet1/0/12.
	<circuit-id>	***<circuit-id>*** means the circuit-id content of option 82 specified by users, its length can not exceed 64 characters.
Default	Use standard format to set circuit-id.	
Mode	Port mode	
Usage	Set the suboption1 (circuit ID option) content of option 82 added by DHCP request packets (they are received by the port). The no command sets the additive suboption1 (circuit ID option) format of option 82 as standard. The additive option 82 needs to associate with third-party DHCP server, it is used to specify the circuit-id content by user when the standard circuit-id format can not satisfy server's request.	
Example	Set the suboption circuit-id of DHCP option82 as P2. Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#ip dhcp snooping information option subscriber-id P2	

11.1.124 ipv6 dhcp snooping information option subscriber-id format

Syntax

ip dhcp snooping information option subscriber-id format {hex | ascii | vs-hp}

Parameter

hex	hex means that subscriber-id is VLAN and port information with hexadecimal format
ascii	acsii means that subscriber-id is VLAN and port information with ACSII format.
vs-hp	vs-hp means that subscriber-id is compatible with the format of HP manufacturer.

Default

ascii

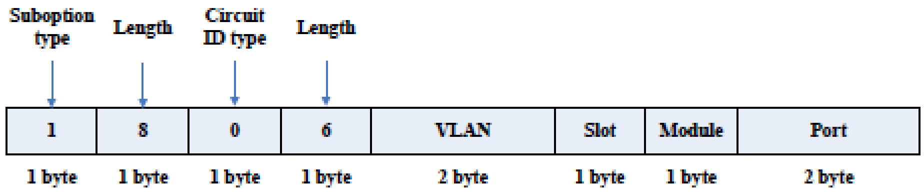
Mode

Global Mode

Usage

This command is used to set subscriber-id format of DHCP snooping option82.

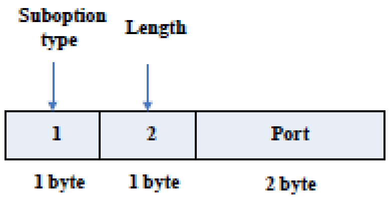
VLAN and port information with ASCII format, such as Vlan1+Ethernet1/0/11, VLAN and



port information with hexadecimal format defined as below:

VLAN field fill in VLAN ID. For chassis switch, Slot means slot number, for box switch, Slot is 1; default Module is 0; Port means port number which begins from 1.

The compatible subscriber-id format with HP manufacturer defined as below:



Port means port number which begins from 1.

Example

Set subscriber-id format of DHCP snooping option82 as hexadecimal format.

```
Switch#config
Switch(config)#ip dhcp snooping information option subscriber-id format hex
```

11.1.125 ip dhcp snooping limit-rate

Syntax	**ip dhcp snooping limit-rate <pps>** **no ip dhcp snooping limit-rate**	
Parameter	**<pps>**	The number of DHCP messages transmitted in every minute, ranging from 0 to 100. Its default value is 100. 0 means that no DHCP message will be transmitted.
Default	The default value is 100.	
Mode	Global Mode	
Usage	Set the DHCP message rate limit After enabling DHCP snooping, the switch will monitor all the DHCP messages and implement software transmission. The software performance of the switch is relative to the type of the switch, its current load and so on.	
Example	Set the message transmission rate as 50pps. Switch#config Switch(config)# ip dhcp snooping limit-rate 50	

11.1.126 ip dhcp snooping trust

Syntax	**ip dhcp snooping trust** **no ip dhcp snooping trust**
Parameter	**none**
Default	By default, all ports are non-trusted ports
Mode	Port mode
Usage	Set or delete the DHCP Snooping trust attributes of a port. Only when DHCP Snooping is globally enabled, can this command be set. When a port turns into a trusted port from a non-trusted port, the original defense action of the port will be automatically deleted; all the security history records will be cleared (except the information in system log)
Example	Set port ethernet1/0/1 as a DHCP Snooping trusted port Switch#config Switch(config)#interface ethernet 1/0/1 switch(config- ethernet 1/0/1)#ip dhcp snooping trust

11.1.127 ip dhcp snooping vlan

Syntax	**ip dhcp snooping vlan (WORD)** **no ip dhcp snooping vlan (WORD)**	
Parameter	**WORD**	VLAN ID
Default	Disable	
Mode	Global Mode	
Usage	Enable the dhcp snooping in vlan. **no ip dhcp snooping vlan <vlan-id>** means to disable the dhcp snooping function on the appointed vlan.	
Example	Enable DHCP snooping function. Switch#config Switch(config)#ip dhcp snooping vlan 10 Switch(config)#no ip dhcp snooping vlan 10	

11.1.128 ip user helper-address

Syntax	**ip user helper-address <svr_addr> [port <udp_port>] source <src_addr> [secondary]** **no ip user helper-address [secondary]**	
Parameter	**<svr_addr>**	The IP address of HELPER SERVER IP in dotted-decimal notation
	<udp_port>	The UDP port of HELPER SERVER, the range of which is1－65535, and its default value is 9119.
	<src_addr>	The local management IP address of the switch, in dotted-decimal notation.
	[secondary]	Whether it is a secondary SERVER address.
Default	There is no HELPER SERVER address by default.	
Mode	Global Mode	
Usage	Set the address and port of HELPER SERVER. DHCP SNOOPING will send the monitored binding information to HELPER SERVER to save it. If the switch starts abnormally, it can recover the binding data from HELPER SERVER. The HELPER SERVER function usually is integrated into DCBI packet. The DHCP SNOOPING and HELPER SERVER use the UDP protocol to communicate, and guarantee the arrival of retransmitted data. HELPER SERVER configuration can also be	

	used to sent DOT1X user data from the server, the detail of usage is described in the chapter of dot1x configuration. Two HELPER SERVER addresses are allowed, DHCP SNOOPING will try to connect to PRIMARY SERVER in the first place. Only when the PRIMARY SERVER is unreachable, will the switch c HELPER SERVER connects to SECONDARY SERVER. **Please pay attention:** source address is the effective management IP address of the switch, if the management IP address of the switch changes, this configuration should be updated in time.
Example	Set the local management IP address as 100.1.1.1, primary HELPER SERVER address as 100.1.1.100 and the port as default value. Switch#config switch(config)#interface vlan 1 Switch(config-if-vlan1)#ip address 100.1.1.1 255.255.255.0 switch(config-if-vlan1)exit switch(config)#ip user helper-address 100.1.1.100 source 100.1.1.1

11.1.129 ip user private packet version two

Syntax	**ip user private packet version two** **no ip user private packet version two**
Parameter	**none**
Default	The switch choose private packet version one to communicate with DCBI.
Mode	Global Mode
Usage	The switch choose private packet version two to communicate with trustview. If the DCBI access control system is applied, the switch should be configured to use private protocol of version one to communicate with the DCBI server. However, if TrustView is applied, version two should be applied.
Example	To configure the switch choose private packet version two to communicate with inter security management background system. Switch#config Switch(config)#ip user private packet version two

11.1.130 show ip dhcp snooping

Syntax **show ip dhcp snooping [interface [ethernet] <interfaceName>]**

Parameter **<interfaceName>** The name of the specific port.

Default none

Mode Admin and Configuration Mode

Usage If there is no specific port, then display the current cofiguration information of dhcp snooping, otherwise, display the records of defense actions of the specific port

Example

```
Switch#show ip dhcp snooping
User primary helper server 1.1.1.1:9119, source 100.1.1.1, socket 0
    seq no 0, connection 0, retry 0, renew 0, binding count 0
    00:00:00 retry, 01:16:57 keep alive, 00:00:00 dead
    Get PrivateDESMD5 Ack 0, Get FreeResource Ack 0, Get HttpRedirPage Ack 0, Get
Binding Ack 0

DHCP Snooping is enabled
DHCP Snooping maxnum of action info:100
DHCP Snooping limit rate is 100 pps, switch ID 10-f0-13-f1-72-3a
DHCP Snooping droped packets 0, discarded packets 0
DHCP Snooping alarm count 0, binding count 1,
  static binding count 1, from shell 1, from server 0
  expired binding 0, request binding 0

interface        trust      action     recovery   alarm num  bind num
--------------- ---------- ---------- ---------- ---------- ----------
Ethernet1/0/1    trust      none       0          0          0
Ethernet1/0/2    untrust    none       0          0          0
Ethernet1/0/3    untrust    none       0          0          0
Ethernet1/0/4    untrust    none       0          0          0
Ethernet1/0/5    untrust    none       0          0          0
Ethernet1/0/6    untrust    none       0          0          0
Ethernet1/0/7    untrust    none       0          0          0
Ethernet1/0/8    untrust    none       0          0          0
Ethernet1/0/9    untrust    none       0          0          0
Ethernet1/0/10   untrust    none       0          0          0
Ethernet1/0/11   untrust    none       0          0          0
Ethernet1/0/12   untrust    none       0          0          0
Ethernet1/0/13   untrust    none       0          0          0
```

```
Ethernet1/0/14    untrust      none          0             0             1
Ethernet1/0/15    untrust      none          0             0             0
Ethernet1/0/16    untrust      none          0             0             0
Ethernet1/0/17    untrust      none          0             0             0
Ethernet1/0/18    untrust      none          0             0             0
Ethernet1/0/19    untrust      none          0             0             0
Ethernet1/0/20    untrust      none          0             0             0
Ethernet1/0/21    untrust      none          0             0             0
Ethernet1/0/22    untrust      none          0             0             0
Ethernet1/0/23    untrust      blackhole    30            0             0
Ethernet1/0/24    untrust      none          0             0             0
Ethernet1/0/25    untrust      none          0             0             0
Ethernet1/0/26    untrust      none          0             0             0
Ethernet1/0/27    untrust      none          0             0             0
Ethernet1/0/28    untrust      none          0             0             0
```

Displayed Information	Explanation
DHCP Snooping is enable	Whether the DHCP Snooping is globally enabled or disabled.
DHCP Snooping binding arp	Whether the ARP binding function is enabled.
DHCP Snooping maxnum of action info	The number limitation of port defense actions
DHCP Snooping limit rate	The rate limitation of receiving packets
switch ID	The switch ID is used to identify the switch, usually using the CPU MAC address
DHCP Snooping droped packets	The number of dropped messages when the received DHCP messages exceeds the rate limit.
discarded packets	The number of discarded packets caused by the communication failure within the system. If the CPU of the switch is too busy to schedule the DHCP SNOOPING task and thus can not handle the received DHCP messages, such situation might happen.
DHCP Snooping alarm count:	The number of alarm information.
binding count	The number of binding information.
expired binding	The number of binding information which is already expired but has not been deleted. The reason why the expired

	information is not deleted immediately might be that the switch needs to notify the helper server about the information, but the helper server has not acknowledged it.
request binding	The number of REQUEST information
interface	The name of port
trust	The truest attributes of the port
action	The automatic defense action of the port
recovery	The automatic recovery time of the port
alarm num	The number of history records of the port automatic defense actions
bind num	The number of port-relative binding information.

11.1.131 show ip dhcp snooping binding all

Syntax	**show ip dhcp snooping binding all**
Parameter	**none**
Default	none
Mode	Admin and Configuration Mode
Usage	This command can check the global binding information of DHCP snooping, each table entry includes the corresponding MAC address, IP address, port name, VLAN ID and the flag of the binding state. Besides, DHCP Snooping must be enabled globally, this command can be configured.

Example

```
Switch#show ip dhcp snooping binding all
ip dhcp snooping static binding count:1, dynamic binding count:0

MAC                      IP address           Interface           Vlan ID    Flag
--------------------------------------------------------------------------
00-11-22-33-44-55    1.1.1.1              Ethernet1/0/14         1            SE
--------------------------------------------------------------------------
```

11.1.132 show trustview status

Syntax
show trust status

Parameter
none

Default
none

Mode
Admin and Configuration Mode

Usage
This command can be used for debugging the communication messages between the switch and the TrustView server, messages such as protocol version notification, encryption negotiation, free resource and web URL redirection, and the number of forced log-off messages, as well as the number of forced accounting update messages, can be displayed.

Example

```
Switch#show trustview status
Primary trustview Server 1.1.1.1:9119
    trustview version2 message inform failed
    trustview inform free resource failed
    trustview inform web redirect address failed
    trustview inform user binding data failed
trustview version 2 message encrypt/digest not enabled
Rcvd 0 force log-off packets
Rcvd 0 force accounting update packets
using version two private packet
```

11.1.133 ip dhcp snooping information enable

Syntax
ip dhcp snooping information enable
no ip dhcp snooping information enable

Parameter
none

Default
Option 82 function is disabled in DHCP Snooping by default.

Mode
Global Mode

Usage
Only by implementing this command, can DHCP Snooping add standard option 82 to DHCP request messages and forward the message. The format of option1 in option 82 (Circuit ID option) is standard vlan name plus physical port name, like "vlan1+ethernet1/0/12". That of option2 in option 82 (remote ID option) is CPU MAC of the switch, like "00030f023301". If a DHCP request message with option 82 options is received, DHCP Snooping will replace those options in the message with its own. If a DHCP reply message with option 82 options is received, DHCP Snooping will dump those options in the message and forward it.

Example
Enable option 82 function of DHCP Snooping on the switch. Switch#config

```
Switch(config)#ip dhcp snooping enable
Switch(config)#ip dhcp snooping binding enable
Switch(config)#ip dhcp snooping information enable
```

Chapter 12 Multicast Protocol

12.1 IPv4 Multicast

12.1.1 access-list (Multicast Destination Control)

Syntax	access-list <6000-7999> (((add | delete) profile-id WORD) | ((deny | permit) ip ((<source> <wildcard-bit>) | (host-source <source-host-ip> [range <2-65535>]) | any-source) ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip> [range <2-255>]) | any-destination)) no access-list <6000-7999> {deny|permit} ip ((<source> <source-wildcard>) | (host-source <source-host-ip> [range <2-65535>]) | any-source) ((<destination> <destination-wildcard>) | (host-destination <destination-host-ip> [range <2-255>]) | any-destination)	
Parameter	<6000-7999>	destination control access-list number.
	add | delete	add or delete the profile
	WORD	File id
	deny | permit	deny or permit
	<source>	multicast source address
	<wildcard-bit>	Address wildcard
	<source-host-ip>	multicast source host address.
	<2-65535>	the range of multicast source host.
	<destination>	multicast destination address
	<destination-host-ip>	multicast destination host address
	<2-255>	the range of multicast destination host.
Default	none	
Mode	Global Mode	
Usage	ACL of Multicast destination control list item is controlled by specifical ACL number from 6000 to 7999, the command applies to configure this ACL. ACL of ip Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list. And adding or deleting the profile-id can be used to change the multicast destination control ACL.	
Example	Switch#config	

```
Switch(config)#access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255
Switch(config)#access-list 6000 add profile-id 1
profile id 1 is not exsit
% Operation failed

Switch(config)#
```

12.1.2 access-list (Multicast Source Control)

Syntax	access-list <5000-5099> (deny | permit) ip ((<source> <wildcard-bit>) | (host <source-host-ip>) | any-source) ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip>) | any-destination} no access-list <5000-5099> (deny | permit) ip ((<source> <wildcard-bit>) | (host <source-host-ip>) | any-source) ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip>) | any-destination)	
Parameter	<5000-5099>	source control access-list number
	deny | permit	deny or permit.
	<source>	multicast source address..
	<wildcard-bit>	address wildcard character.
	<source-host-ip>	multicast source host address.
	<destination>	multicast destination address.
	<destination-host-ip>	multicast destination host address.
Default	None	
Mode	Global Mode	
Usage	ACL of Multicast source control list item is controlled by specifical ACL number from 5000 to 5099, the command applies to configure this ACL. ACL of Multicast source control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to other ACLs, and use wildcard character to configure address range, and also specify a host address or all address. Remarkable, "all address" is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.	
Example	Switch(config)#access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255	

12.1.3 ip multicast destination-control access-group

Syntax	ip multicast destination-control access-group <6000-7999> no ip multicast destination-control access-group <6000-7999>	
Parameter	<6000-7999>	destination-control access-list number.
Default	None	
Mode	Interface Configuration Mode	
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the interface to multicast group, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.	
Example	Switch#config Switch(config)#interface ethernet 1/0/4 Switch(config-if-ethernet1/0/4)#ip multicast destination-control access-group 6000 Switch(config-if-ethernet1/0/4)#	

12.1.4 ip multicast destination-control access-group (sip)

Syntax	ip multicast destination-control <IPADDRESS/M> access-group <6000-7999> no ip multicast destination-control <IPADDRESS/M> access-group <6000-7999>	
Parameter	<IPADDRESS/M>	IP address and mask length
	<6000-7999>	Destination control access-list number
Default	None	
Mode	Global Mode	
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING or IGMP is enabled, for adding the members to multicast group. If configuring multicast destination-control on specified net segment of transmitted igmp-report, and match configured access-list, such as matching permit, the interface can be added, otherwise do not be added. If relevant group or source in show ip igmp groups detail has been established before executing the command, it needs to execute clear ip igmp groups command to clear relevant groups in Admin mode.	
Example	Switch#config Switch(config)#ip multicast destination-control 10.1.1.0/24 access-group 6000	

12.1.5 ip multicast destination-control access-group (vmac)

Syntax	ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999> no ip multicast destination-control <1-4094> <macaddr > access-group <6000-7999>	
Parameter	<1-4094>	VLAN ID
	<macaddr >	Transmitting source MAC address of IGMP-REPORT, the format is "xx-xx-xx-xx-xx-xx";
	<6000-7999>	Destination-control access-list number.
Default	None	
Mode	Global Mode	
Usage	The command is only working under global multicast destination-control enabled, after configuring the command, if IGMP-SPOOPING is enabled, for adding the members to multicast group. If configuring multicast destination-control to source MAC address of transmitted igmp-report, and match configured access-list, such as matching: permit, the interface can be added, otherwise do not be added.	
Example	Switch#config Switch(config)#ip multicast destination-control 1 00-01-03-05-07-09 access-group 6000	

12.1.6 ip multicast policy

Syntax	ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos <priority> no ip multicast policy <IPADDRESS/M> <IPADDRESS/M> cos	
Parameter	<IPADDRESS/M>	are multicast source address, mask length, destination address, and mask length separately.
	<priority>	specified priority, range from 0 to 7
Default	None	
Mode	Global Mode	
Usage	The command configuration modifies to a specified value through the switch matching priority of specified range multicast data packet, and the TOS is specified to the same value simultaneously.Carefully, the packet transmitted in UNTAG mode does not modify its priority.	
Example	Switch(config)#ip multicast policy 10.1.1.0/24 225.1.1.0/24 cos 7	

12.1.7 ip multicast source-control

Syntax	ip multicast source-control no ip multicast source-control
Parameter	None
Default	Disabled
Mode	Global Mode
Usage	The source control access-list applies to interface with only enabling global multicast source control, and configure to disabled global multicast source control without configuring source control access-list on every interface. After configuring the command, multicast data received from every interface does not have matching multicast source control list item, and then they will be thrown away by switches, namely only multicast data matching to PERMIT can be received and forwarded. ◦
Example	Switch(config)#ip multicast source-control

12.1.8 ip multicast source-control access-group

Syntax	ip multicast source-control access-group <5000-5099> no ip multicast source-control access-group <5000-5099>
Parameter	<5000-5099> Source control access-list number.
Default	None
Mode	Interface Configuration Mode
Usage	The command configures with only enabling global multicast source control. After that, it will match multicast data message imported from the interface according to configured access-list, such as matching: permit, the message will be received and forwarded; otherwise the message will be thrown away.
Example	Switch (config)#interface ethernet1/0/4 Switch (config-if-ethernet1/0/4)#ip multicast source-control access-group 5000 Switch (config-if-ethernet1/0/4)#

12.1.9 ip multicast destination-control

<table>
<tr><td>Syntax</td><td>ip multicast destination-control</td></tr>
<tr><td>Parameter</td><td>None</td></tr>
<tr><td>Default</td><td>Disabled</td></tr>
<tr><td>Mode</td><td>Global Mode</td></tr>
<tr><td>Usage</td><td>Only after globally enabling the multicast destination control, the other destination control configuration can take effect; the destination access list can be applied to ports, VLAN-MAC and SIP. After configuring this command, IGMP-SNOOPING and IGMP will match according to the rules mentioned above when they try to add ports after receiving IGMP-REPORT.</td></tr>
<tr><td>Example</td><td>Switch(config)#ip multicast destination-control</td></tr>
</table>

12.1.10 profile-id (Multicast Destination Control Rule List)

<table>
<tr><td>Syntax</td><td colspan="2">profile-id <1-50> (deny | permit) ip ((<source> <wildcard-bit>) | (host-source <source-host-ip> [range <2-65535>]) | any-source} ((<destination> <wildcard-bit>) | (host-destination <destination-host-ip> [range <2-255>]) | any-destination)
no profile-id <1-50&gt;</td></tr>
<tr><td>Parameter</td><td>&lt;1-50&gt;</td><td>profile-id</td></tr>
<tr><td></td><td>deny | permit</td><td>deny or permit.</td></tr>
<tr><td></td><td>&lt;source&gt;</td><td>multicast source address</td></tr>
<tr><td></td><td>&lt;wildcard-bit&gt;</td><td>address wildcard character.</td></tr>
<tr><td></td><td>&lt;source-host-ip&gt;</td><td>multicast source host address.</td></tr>
<tr><td></td><td>&lt;2-65535&gt;</td><td>range of multicast source host</td></tr>
<tr><td></td><td>&lt;destination&gt;</td><td>multicast destination address</td></tr>
<tr><td></td><td>&lt;destination-host-ip&gt;</td><td>multicast destination host address</td></tr>
<tr><td></td><td>&lt;2-255&gt;</td><td>range of multicast destination host.</td></tr>
<tr><td>Default</td><td colspan="2">none</td></tr>
<tr><td>Mode</td><td colspan="2">Global Mode</td></tr>
<tr><td>Usage</td><td colspan="2">Profile-list of Multicast destination control list item is controlled by specifical profile-id number from 1 to 50, the command applies to configure this profile to add it into the ACL for using. Multicast destination control only needs to configure source IP address and destination IP address controlled (group IP address), the configuration mode is basically the same to ACLs, and use mask length to configure address range, and also specify a host address or all address. Remarkable, “all address” is 224.0.0.0/4 according to group IP address, not 0.0.0.0/0 in other access-list.</td></tr>
<tr><td>Example</td><td colspan="2">switch(config)# profile-id 1 deny ip any-source host-destination 224.1.1.2</td></tr>
</table>

12.1.11 show ip multicast destination-control

Syntax	show ip multicast destination-control [detail] show ip multicast destination-control interface <Interfacename> [detail] show ip multicast destination-control host-address <ipaddress> [detail] show ip multicast destination-control <vlan-id> <mac-address> [detail]	
Parameter	detail	expresses if it display information in detail or not
	<Interfacename>	interface name or interface aggregation name, such as Ethernet1/0/1, port-channel 1 or ethernet1/0/1.
	<ipaddress>	IP address
	<vlan-id>	VLAN ID
	<mac-address>	Mac address
Default	None	
Mode	Admin Mode and Global Mode	
Usage	The command displays multicast destination control rules of configuration including detail option, and access-list information applied in detail.	
Example	Switch#show ip multicast destination-control ip multicast destination-control is enabled multicast destination-control access-group 6000 used on interface Ethernet1/0/4	

12.1.12 show ip multicast destination-control access-list

Syntax	show ip multicast destination-control access-list show ip multicast destination-control access-list <6000-7999>	
Parameter	<6000-7999>	access-list number.
Default	None	
Mode	Admin Mode and Global Mode	
Usage	The command displays destination control multicast access-list of configuration.	
Example	Switch#show ip multicast destination-control access-list access-list 6000 permit ip 10.1.1.1 0.0.0.255 232.0.0.0 0.0.0.255	

12.1.13 show ip multicast destination-control filter-profile-list

Syntax	show ip multicast destination-control filter-profile-list show ip multicast destination-control filter-profile-list <1-50>	
Parameter	<1-50>	profile-id
Default	None	
Mode	Admin Mode and Global Mode	
Usage	This command can show the configured destination control profile rule list.	
Example	Switch#show l2-address-table multicast vlan 1 Vlan Address Insert Type Creator Ports ---- -------------------------- ---------- -------------------------------------	

12.1.14 show ip multicast policy

Syntax	show ip multicast policy
Parameter	None
Default	None
Mode	Admin Mode and Global Mode
Usage	The command displays multicast policy of configuration
Example	Switch#show ip multicast policy ip multicast-policy 10.1.1.0/24 225.0.0.0/8 cos 5

12.1.15 show ip multicast source-control

Syntax	show ip multicast source-control [detail] show ip multicast source-control interface <Interfacename> [detail]	
Parameter	detail	expresses if it displays information in detail.
	<Interfacename>	interface name, such as ethernet 1/0/1 or ethernet1/0/1.
Default	None	
Mode	Admin Mode and Global Mode	
Usage	The command displays multicast source control rules of configuration, including detail option, and access-list information applied in detail.	
Example	Switch#show ip multicast source-control detail ip multicast source-control is enabled Interface Ethernet1/0/13 use multicast source control access-list 5000 access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255	

12.1.16 show ip multicast source-control access-list

Syntax	show ip multicast source-control access-list show ip multicast source-control access-list <5000-5099>	
Parameter	<5000-5099>	access-list number
Default	None	
Mode	Admin Mode and Global Mode	
Usage	The command displays source control multicast access-list of configuration	
Example	Switch#show ip multicast source-control access-list access-list 5000 permit ip 10.1.1.0 0.0.0.255 232.0.0.0 0.0.0.255 access-list 5000 deny ip 10.1.1.0 0.0.0.255 233.0.0.0 0.255.255.255	

12.1.17 clear ip igmp snooping vlan

Syntax	clear ip igmp snooping vlan <1-4094> groups [A.B.C.D]	
Parameter	<1-4094>	VLAN ID
	[A.B.C.D]	group address.
Default	None	
Mode	Admin Configuration Mode	
Usage	Use show command to check the deleted group record.	
Example	Switch#clear ip igmp snooping vlan 1 groups	

12.1.18 clear ip igmp snooping vlan

Syntax	clear ip igmp snooping vlan <1-4094> mrouter-port [ethernet] IFNAME	
Parameter	<1-4094>	VLAN ID
	IFNAME	port name
Default	None	
Mode	Admin Configuration Mode	
Usage	use show command to check the deleted mrouter port of the specific VLAN. 。	
Example	Delete mrouter port in vlan 1. Switch#clear ip igmp snooping vlan 1 mrouter-port	

12.1.19 ip igmp snooping

Syntax	ip igmp snooping no ip igmp snooping
Parameter	none
Default	IGMP Snooping is disabled by default.
Mode	Global Mode
Usage	Use this command to enable IGMP Snooping, that is permission every VLAN config the function of IGMP snooping. The "no ip igmp snooping" command disables this function.
Example	Enable IGMP Snooping Switch#config Switch(config)#ip igmp snooping Switch(config)#

12.1.20 ip igmp snooping proxy

Syntax	ip igmp snooping proxy no ip igmp snooping proxy
Parameter	none
Default	Enable
Mode	Global Mode
Usage	Enable IGMP Snooping proxy function, the no command disables the function.
Example	Switch#config Switch(config)#no ip igmp snooping proxy Switch(config)#

12.1.21 ip igmp snooping vlan

Syntax	ip igmp snooping vlan <vlan-id> no ip igmp snooping vlan <vlan-id>	
Parameter	<vlan-id>	VLAN ID
Default	IGMP Snooping is disabled by default.	
Mode	Global Mode	
Usage	To configure IGMP Snooping on specified VLAN, the global IGMP Snooping should be first enabled. Disable IGMP Snooping on specified VLAN with the "no ip igmp snooping vlan <vlan-id>" command.	
Example	Enable IGMP Snooping for VLAN 100 in Global Mode. Switch#config Switch(config)#ip igmp snooping vlan 100	

12.1.22 ip igmp snooping vlan immediate-leave

Syntax	ip igmp snooping vlan <vlan-id> immediate-leave no ip igmp snooping vlan <vlan-id> immediate-leave	
Parameter	<vlan-id>	VLAN ID
Default	This function is disabled by default.	
Mode	Global Mode	
Usage	Enable immediate-leave function of the IGMP Snooping in specified VLAN; the"no" form of this command disables the immediate-leave function of the IGMP Snooping	
Example	Enable the IGMP Snooping fast leave function for VLAN 100. Switch#config Switch(config)#ip igmp snooping vlan 100 immediate-leave	

12.1.23 ip igmp snooping vlan

Syntax	ip igmp snooping vlan <vlan-id> immediately-leave mac-based no ip igmp snooping vlan <vlan-id> immediately-leave mac-based
Parameter	<vlan-id> VLAN ID
Default	This function is disabled by default.
Mode	Global Mode
Usage	Configure this command to delete the existed igmp snooping table entries according to the source mac in leave packet when the switch which is enabled the igmp snooping function receives the leave packet. Only when the received the port, source mac and multicast group of the leave packet are the same as the port, host mac and multicast group of the existed igmp snooping table entry, the snooping table entry can be deleted. If this command is not configured, delete the existed igmp snooping table entry according to the port and multicast group of the leave packet. Configure the immediately-leave under the same vlan at the same time to make this command effective. In this time, deal with it according to the host mac of the port.
Example	Use the following configuration when delete the table entry according to the host mac of the port. Switch#config Switch(config)#ip igmp snooping vlan 12 immediately-leave Switch(config)#ip igmp snooping vlan 12 immediately-leave mac-based

12.1.24 ip igmp snooping vlan l2-general-querier

Syntax	ip igmp snooping vlan < vlan-id > l2-general-querier no ip igmp snooping vlan < vlan-id > l2-general-querier
Parameter	<vlan-id> is ID number of the VLAN, ranging is <1-4094>
Default	VLAN is not as the IGMP Snooping layer 2 general querier.
Mode	Global Mode
Usage	It is recommended to configure a layer 2 general querier on a segment. IGMP Snooping function will be enabled by this command if not enabled on this VLAN before configuring this command, IGMP Snooping function will not be disabled when disabling the layer 2 general querier function. This command is mainly for sending general queries regularly to help switches within this segment learn mrouter ports. Comment: There are three paths IGMP snooping learn mrouter 1 Port receives the IGMP query messages 2 Port receives multicast protocol packets, and supports DVMRP, PIM 3 Static configured port
Example	Switch(config)#ip igmp snooping vlan 1 l2-general-querier

12.1.25 ip igmp snooping vlan l2-general-querier-source

Syntax	ip igmp snooping vlan < vlan-id > l2-general-querier-source <A.B.C.D> no ip igmp snooping vlan <vlanid> l2-general-querier-source	
Parameter	<vlan-id>	VLAN ID
	<A.B.C.D>	<A.B.C.D> is the source address of the query operation
Default	0.0.0.0	
Mode	Global Mode	
Usage	It is not supported on Windows 2000/XP to query with the source address as 0.0.0.0. So the layer 2 query source address configuration does not function. The client will stop sending requesting datagrams after one is sent. And after a while, it can not receive multicast datagrams.	
Example	Switch(config)#ip igmp snooping vlan 2 L2-general-query-source 192.168.1.2	

12.1.26 ip igmp snooping vlan l2-general-querier-version

Syntax	ip igmp snooping vlan <vlanid> l2-general-querier-version <version>	
Parameter	<vlan-id>	VLAN ID
	<version>	version number, limited to <1-3>.
Default	version 3	
Mode	Global Mode	
Usage	When the switch is connected to V1 and V2 capable environment, and for VLAN which has source of layer 2 query configuration, the VLAN can be queried only if the version number has been specified. This command is used to query the layer 2 version number.	
Example	Switch(config)#ip igmp snooping vlan 2 l2-general-querier-version 2	

12.1.27 ip igmp snooping vlan limit

Syntax	ip igmp snooping vlan <vlanid> limit {group <g_limit> | source <s_limit>} no ip igmp snooping vlan <vlan-id> limit	
Parameter	<vlan-id>	VLAN ID
	<g_limit>	<1-65535>, max number of groups joined
	<s_limit>	<1-65535>, max number of source entries in each group, consisting of include source and exclude source.
Default	Maximum 50 groups by default, with each group capable with 40 source entries.	
Mode	Global Mode	
Usage	When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, IGMP snooping must be enabled on VLAN. The "no" form of this command restores the default other than set to "no limit". For the safety considerations, this command will not be configured to "no limit". It is recommended to use default value and if layer 3 IGMP is in operation, please make this configuration in accordance with the IGMP configuration as possible.	
Example	Switch(config)#ip igmp snooping vlan 2 limit group 300	

12.1.28 ip igmp snooping vlan interface

Syntax	ip igmp snooping vlan <vlanid> interface (ethernet | port-channel) IFNAME limit {group <g_limit> | source <s_limit>} strategy (replace | drop) no ip igmp snooping vlan <1-4094> interface (ethernet | port-channel) IFNAME limit group source strategy	
Parameter	<vlan-id>	VLAN ID
	IFNAME	Interface name
	<g_limit>	<1-65535>, The maximum number of groups allowed joining
	<s_limit>	<1-65535>, The maximum number of source table entries in each group, including include source and exclude source.
	replace	Replace the group and source information
	drop	Drop the new group and source information
Default	There is no limitation as default.	
Mode	Global Mode	
Usage	When the number of the groups joined under the port or the number of sources in this group exceeds the limit, it will be dealt according to the configured strategy. If it is drop, drop the new group and source information; if it is replace, find a dynamic group and source from the port to conduct deleting and replacing, and then add the new group and source information. The premise of using this command is that this VLAN is enabled	

	IGMP Snooping function. No command configures as "no limitation".
Example	Switch(config)#ip igmp snooping vlan 2 interface ethernet 1/0/11 limit group 300 source 200 strategy replace

12.1.29 ip igmp snooping vlan mrouter-port interface

Syntax	ip igmp snooping vlan <vlanid> mrouter-port interface [ehternet | port-channel] <ifname> no ip igmp snooping vlan <vlan-id> mrouter-port interface[<ehternet> | <port-channel>] <ifname>	
Parameter	<vlan-id>	VLAN ID
	IFNAME	Name of interface
Default	No static mrouter port on VLAN by default.	
Mode	Global Mode	
Usage	When a port is a static mrouter port while also a dynamic mrouter port, it should be taken as a static mrouter port. Deleting static mrouter port can only be realized by the no command.	
Example	Switch(config)#ip igmp snooping vlan 2 mrouter-port interface ethernet1/0/13	

12.1.30 ip igmp snooping vlan mrouter-port learnpim

Syntax	ip igmp snooping vlan <vlanid> mrouter-port learnpim no ip igmp snooping vlan <vlan-id> mrouter-port learnpim	
Parameter	<vlan-id>	VLAN ID
Default	Enable	
Mode	Global Mode	
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pim packets). After a port received pim packets, it will be set to mrouter port for implementing the automatic learning.	
Example	Disable the function that vlan 100 learns mrouter-port (according to pim packets). Switch(config)#no ip igmp snooping vlan 100 mrouter-port learnpim	

12.1.31 ip igmp snooping vlan mrpt

Syntax	ip igmp snooping vlan <vlanid> mrpt <value> no ip igmp snooping vlan <vlan-id> mrpt	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	mrouter port survive period, ranging between <1-65535>seconds
Default	255s	
Mode	Global Mode	
Usage	This command validates on dynamic mrouter ports but not on mrouter port. To use this command, IGMP Snooping of this VLAN should be enabled previously.	
Example	Switch(config)#ip igmp snooping vlan 2 mrpt 100	

12.1.32 ip igmp snooping vlan query-interval

Syntax	ip igmp snooping vlan <vlanid> query-interval <value> no ip igmp snooping vlan <vlan-id> query-interval	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	query interval, ranging between <1-65535>seconds
Default	125s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query-interval 130	

12.1.33 ip igmp snooping vlan query-mrsp

Syntax	ip igmp snooping vlan <vlanid> query-mrsp <value> no ip igmp snooping vlan <vlan-id> query-mrspt	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	ranging between <1-25> seconds
Default	10s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query-mrsp 18	

12.1.34 ip igmp snooping vlan query-robustness

Syntax	ip igmp snooping vlan <vlanid> query-robustness <value> no ip igmp snooping vlan <vlan-id> query-robustness	
Parameter	<vlan-id>	VLAN ID
	<value>	ranging between <2-10>
Default	2s	
Mode	Global Mode	
Usage	It is recommended to use the default settings. Please keep this configure in accordance with IGMP configuration as possible if layer 3 IGMP is running.	
Example	Switch(config)#ip igmp snooping vlan 2 query- robustness 3	

12.1.35 ip igmp snooping vlan report source-address

Syntax	ip igmp snooping vlan <vlanid> report source-address <A.B.C.D> no ip igmp snooping vlan <vlan-id> report source-address	
Parameter	<vlan-id>	VLAN ID
	<A.B.C.D>	IP address, can be 0.0.0.0
Default	Disabled	
Mode	Global Mode	
Usage	Default configuration is recommended here. If IGMP snooping needs to be configured, the source address for forwarded IGMP messages can be 0.0.0.0. If it is required by the upstream that IGMP messages should use the same network address, the source address of IGMP messages should be configured to be the same with upstream. ◦	
Example	Switch(config)#ip igmp snooping vlan 2 report source-address 10.1.1.1	

12.1.36 ip igmp snooping vlan specific-query-mrsp

Syntax	ip igmp snooping vlan <vlanid> specific-query-mrsp <value> no ip igmp snooping vlan <vlan-id> specific-query-mrspt	
Parameter	<vlan-id>	specific VLAN ID, the range from 1 to 4094
	<value>	the maximum query response time, unit is second, the range from 1 to 25, default value is 1
Default	Enable	
Mode	Global Mode	
Usage	After enable vlan snooping in global mode, input this command to configure the maximum query response time of the specific group.	
Example	Configure/cancel the specific-query-mrsp of vlan3 as 2s. Switch(config)#ip igmp snooping vlan 3 specific-query-mrsp 2 Switch(config)#no ip igmp snooping vlan 3 specific-query-mrspt	

12.1.37 ip igmp snooping vlan static-group

Syntax	ip igmp snooping vlan <vlanid> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME> no ip igmp snooping vlan <vlan-id> static-group <A.B.C.D> [source <A.B.C.D>] interface [ethernet | port-channel] <IFNAME>	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<A.B.C.D>	address of group or source
	<IFNAME>	Name of interface
Default	None	
Mode	Global Mode	
Usage	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.	
Example	Switch(config)#ip igmp snooping vlan 1 static-group 224.1.1.1 source 192.168.1.1 interface ethernet 1/0/1	

12.1.38 ip igmp snooping vlan suppression-query-time

Syntax	ip igmp snooping vlan <vlanid> suppression-query-time <value> no ip igmp snooping vlan <vlan-id> suppression-query-time	
Parameter	<vlan-id>	VLAN ID, ranging between <1-4094>
	<value>	ranging between<1-65535> seconds
Default	255s	
Mode	Global Mode	
Usage	Configure the suppression query time. The "no ip igmp snooping vlan <vlan-id> suppression-query-time" command restores to the default value. This command can only be configured on L2 general querier. The Suppression-query-time refers to the period of suppression state in which the querier enters when receives query from the layer 3 IGMP in the segments.	
Example	Switch(config)#ip igmp snooping vlan 2 suppression-query-time 270	

12.1.39 show ip igmp snooping

Syntax	show ip igmp snooping [vlan <vlan-id>]	
Parameter	<vlan-id>	VLAN ID
Default	none	
Mode	Admin Configuration Mode	
Usage	If no VLAN number is specified, it will show whether global IGMP Snooping switch is on, which VLAN is configured with l2-general-querier function, and if a VLAN number is specified, detailed IGMP messages for this VLAN will be shown.	

Example

Show IGMP Snooping summary messages of the switch

```
Switch(config)#show ip igmp snooping
Global igmp snooping status: Enabled
L3 multicasting: running
Igmp snooping is turned on for vlan 1(querier)
Igmp snooping is turned on for vlan 2
```

Displayed Information	Explanation
Global igmp snooping status	Whether the global igmp snooping switch on the switch is on
L3 multicasting	whether the layer 3 multicast protocol of the switch is running
Igmp snooping is turned on for vlan 1(querier)	which VLANs on the switch is enabled with igmp snooping function, whether they are l2-general-querier

2.Display the IGMP Snooping summary messages of vlan1.

```
Switch#show ip igmp snooping vlan 1
Igmp snooping information for vlan 1
Igmp snooping L2 general querier :Yes(COULD_QUERY)
Igmp snooping query-interval :125(s)
Igmp snooping max reponse time :10(s)
Igmp snooping robustness :2
Igmp snooping mrouter port keep-alive time :255(s)
Igmp snooping query-suppression time :255(s)
IGMP Snooping Connect Group Membership
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups     Sources          Ports             Exptime System Level
238.1.1.1 (192.168.0.1) Ethernet1/0/8 00:04:14 V2
(192.168.0.2) Ethernet1/0/8 00:04:14 V2

Igmp snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2
```

Displayed Information	Explanation
Igmp snooping L2 general querier	Whether the VLAN enables l2-general-querier function and show whether the querier state is could-query or suppressed
Igmp snooping query-interval	Query interval of the VLAN
Igmp snooping max reponse time	Max response time of the VLAN
Igmp snooping robustness	IGMP Snooping robustness configured on the VLAN
Igmp snooping mrouter port keep-alive time	keep-alive time of dynamic mrouter of the VLAN
Igmp snooping query-suppression time	Suppression timeout of VLAN when as l2-general-querier
IGMP Snooping Connect Group Membership	Group membership of this VLAN, namely the correspondence between ports and (S,G)
Igmp snooping vlan 1 mrouter port	mrouter port of the VLAN, including both static and dynamic

12.1.40 clear ipv6 mld snooping vlan

Syntax	clear ipv6 mld snooping vlan <1-4094> groups [X:X::X:X]	
Parameter	<1-4094>	VLAN ID
	[X:X::X:X]	specific group address
Default	None	
Mode	Admin Configuration Mode	
Usage	Delete the group record of the specific VLAN. Use show command to check the deleted group record	
Example	Delete all groups. Switch#clear ipv6 mld snooping vlan 1 groups	

12.1.41 clear ipv6 mld snooping vlan <1-4094> mrouter-port

Syntax	clear ipv6 mld snooping vlan <1-4094> mrouter-port [ethernet] IFNAME	
Parameter	<1-4094>	VLAN ID
	IFNAME	port name
Default	None	
Mode	Admin Configuration Mode	
Usage	Delete the mrouter port of the specific VLAN. Use show command to check the deleted group record.	
Example	Delete the mrouter port in vlan 1. Switch#clear ipv6 mld snooping vlan 1 mrouter-port	

12.1.42 ipv6 mld snooping

Syntax	ipv6 mld snooping no ipv6 mld snooping
Parameter	None
Default	MLD Snooping disabled on the switch by default
Mode	Global Mode
Usage	Enable global MLD Snooping on the switch, namely allow every VLAN to be configured with MLD Snooping; the "no" form of this command will disable MLD Snooping on all the VLANs as well as the global MLD snooping
Example	Enable MLD Snooping under global mode. Switch(config)#ipv6 mld snooping

12.1.43 ipv6 mld snooping vlan

Syntax	ipv6 mld snooping vlan <vlan-id> no ipv6 mld snooping vlan <vlan-id>
Parameter	<vlan-id> VLAN ID, with a valid range of <1-4094>.
Default	MLD Snooping disabled on VLAN by default
Mode	Global Mode
Usage	Enable MLD Snooping on specified VLAN; the "no" form of this command disables MLD Snooping on specified VLAN. To configure MLD snooping on certain VLAN, the global MLD snooping should be first enabled. Disable MLD snooping on specified VLAN with the no ipv6 mld snooping vlan vid command
Example	Enable MLD snooping on VLAN 100 under global mode. Switch(config)#ipv6 mld snooping vlan 100

12.1.44 ipv6 mld snooping vlan immediate-leave

Syntax	ipv6 mld snooping vlan <vlan-id> immediate-leave no ipv6 mld snooping vlan <vlan-id> immediate-leave
Parameter	<vlan-id> VLAN ID, with valid range of <1-4094>.
Default	Disabled by default
Mode	Global Mode
Usage	Enable immediate-leave function of the MLD protocol in specified VLAN; the "no" form of this command disables the immediate-leave function of the MLD protocol Enabling the immediate-leave function of the MLD protocol will hasten the process the port leaves one multicast group, in which the specified group query of the group will not be sent and the port will be directly deleted.
Example	Enable the MLD immediate-leave function on VLAN 100. Switch(config)#ipv6 mld snooping vlan 100 immediate-leave

12.1.45 ipv6 mld snooping vlan l2-general-querier

Syntax	ipv6 mld snooping vlan <vlan-id> l2-general-querier no ipv6 mld snooping vlan < vlan-id > l2-general-querier	
Parameter	<vlan-id>	VLAN ID, with a valid range of <1-4094>
Default	VLAN is not a MLD Snooping L2 general querier by default.	
Mode	Global Mode	
Usage	It is recommended to configure an L2 general querier on a segment. If before configure with this command, MLD snooping is not enabled on this VLAN, this command will no be executed. When disabling the L2 general querier function, MLD snooping will not be disabled along with it. Main function of this command is sending general queries periodically to help the switches within this segment learn mrouter port. Comment: There are three ways to learn mrouter port in MLD Snooping: 1. The port which receives MLD query messages 2. The port which receives multicast protocol packets and support PIM 3. The port statically configured.	
Example	Set VLAN 100 to L2 general querier. Switch(config)#ipv6 mld snooping vlan 100 l2-general-querier	

12.1.46 ipv6 mld snooping vlan limit

Syntax	ipv6 mld snooping vlan <vlan-id> limit {group <g_limit> | source <s_limit>} no ipv6 mld snooping vlan < vlan-id > limit	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<g_limit>	max number of groups joined, range: 1-65535
	<s_limit>	max number of source entries in each group, consisting of include source and exclude source, range: 1-65535
Default	Maximum 50 groups by default, with each group capable with 40 source entries.	
Mode	Global Mode	
Usage	When number of joined group reaches the limit, new group requesting for joining in will be rejected for preventing hostile attacks. To use this command, MLD snooping must be enabled on VLAN. The "no" form of this command restores the default other than set to "no limit". For the safety considerations, this command will not be configured to "no limit". It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 limit group 300	

12.1.47 ipv6 mld snooping vlan mrouter-port interface

Syntax	ipv6 mld snooping vlan <vlan-id> mrouter-port interface [ethernet | port-channel] <ifname> no ipv6 mld snooping vlan <vlan-id> mrouter-port interface [ethernet | port-channel] <ifname>	
Parameter	<vlan-id>	VLAN ID,the valid range is<1-4094>
	<ifname>	Name of interface
Default	When a port is made static and dynamic mrouter port at the same time, it's the static mrouter properties is preferred. Deleting the static mrouter port can only be done with the "no" form of this command	
Mode	Global Mode	
Usage	Set the static mrouter port of the VLAN; the "no" form of this command cancels the configuration.	
Example	Switch(config)#ipv6 mld snooping vlan 2 mrouter-port interface ethernet1/0/13	

12.1.48 ipv6 mld snooping vlan mrouter-port learnpim6

Syntax	ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6 no ipv6 mld snooping vlan <vlan-id> mrouter-port learnpim6	
Parameter	<vlan-id>	VLAN ID, ranging from 1 to 4094.
Default	Enable	
Mode	Global Mode	
Usage	Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets). After a port received pimv6 packets, it will be set to mrouter port for implementing the automatic learning.	
Example	Disable the function that vlan 100 learns mrouter-port (according to pimv6 packets). Switch(config)#ipv6 mld snooping vlan 2 mrouter-port learnpim6	

12.1.49 ipv6 mld snooping vlan mrpt

Syntax	ipv6 mld snooping vlan <vlan-id> mrpt <value> no ipv6 mld snooping vlan <vlan-id> mrpt	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<value>	mrouter port keep-alive time with a valid range of <1-65535> secs.
Default	255s	
Mode	Global Mode	
Usage	Configure the keep-alive time of the mrouter port. This configuration is applicable on dynamic mrouter port, but not on static mrouter port. To use this command, MLD snooping must be enabled on the VLAN.	
Example	Switch(config)#ipv6 mld snooping vlan 2 mrpt 100	

12.1.50 ipv6 mld snooping vlan query-interval

Syntax	ipv6 mld snooping vlan <vlan-id> query-interval <value> no ipv6 mld snooping vlan <vlan-id> query-interval	
Parameter	<vlan-id>	VLAN ID, the valid range is <1-4094>
	<value>	query interval, valid range: <1-65535>secs.
Default	125s	
Mode	Global Mode	
Usage	Configure the query interval. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible. ◦	
Example	Switch(config)#ipv6 mld snooping vlan 2 query-interval 130	

12.1.51 ipv6 mld snooping vlan query-mrsp

Syntax	ipv6 mld snooping vlan <vlan-id> query-mrsp <value> no ipv6 mld snooping vlan <vlan-id> query-mrspt	
Parameter	<vlan-id>	VLAN ID,the valid range is<1-4094>
	<value>	the valid range is <1-25> secs .
Default	10s	
Mode	Global Mode	
Usage	Configure the maximum query response period. The "no" form of this command restores the default value. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 query-mrsp 18	

12.1.52 ipv6 mld snooping vlan query-robustness

Syntax	ipv6 mld snooping vlan <vlan-id> query-robustness <value> no ipv6 mld snooping vlan <vlan-id> query-robustness	
Parameter	<vlan-id>	VLAN ID,the valid range is <1-4094>
	<value>	the valid range is <2-10>.
Default	2s	
Mode	Global Mode	
Usage	Configure the query robustness; the "no" form of this command restores to the default value. It is recommended to use default value and if layer 3 MLD is in operation, please make this configuration in accordance with the MLD configuration as possible.	
Example	Switch(config)#ipv6 mld snooping vlan 2 query- robustness 3	

12.1.53 ipv6 mld snooping vlan static-group

Syntax	ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME> no ipv6 mld snooping vlan <vlan-id> static-group <X:X::X:X> [source< X:X::X:X>] interface [ethernet | port-channel] <IFNAME>	
Parameter	<vlan-id>	VLAN ID, range：1-4094
	<X:X::X:X>	The address of group or source.
	<IFNAME>	Name of interface
Default	None	
Mode	Global Mode	
Usage	Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. When a group is a static while also a dynamic group, it should be taken as a static group. Deleting static group can only be realized by the no form of the command.	
Example	Switch(config)#ipv6 mld snooping vlan 2 static-group ff1e::15 source 2000::1 interface ethernet 1/0/1	

12.1.54 ipv6 mld snooping vlan suppression-query-time

Syntax	ipv6 mld snooping vlan <vlan-id> suppression-query-time <value> no ipv6 mld snooping vlan <vlan-id> suppression-query-time	
Parameter	<vlan-id>	VLAN ID, valid range: <1-4094>
	<value>	valid range: <1-65535>secs.
Default	255s	
Mode	Global Mode	
Usage	Configure the suppression query time; the "no" form of this command restores the default value. This command can only be configured on L2 general querier. The Suppression-query-time represents the period the suppression state maintains when general querier receives queries from layer 3 MLD within the segment. To use this command, the query-intervals in different switches within the same segment must be in accordance. It is recommended to use the default value.	
Example	Switch(config)#ipv6 mld snooping vlan 2 suppression-query-time 270	

12.1.55 show ipv6 mld snooping

Syntax

show ipv6 mld snooping [vlan <vlan-id>]

Parameter

<vlan-id> VLAN ID

Default

none

Mode

Admin Configuration Mode

Usage

If no VLAN number is specified, it will show whether the global MLD snooping is enabled and layer 3 multicast protocol is running, as well as on which VLAN the MLD Snooping is enabled and configured l2-general-querier. If a VLAN number is specified, the detailed MLD Snooping messages of this VLAN will be displayed.

Example

1.Summary of the switch MLD snooping

```
Switch(config)#show ipv6 mld snooping
Global mld snooping status: Enabled
L3 multicasting: running
Mld snooping is turned on for vlan 1(querier)
Mld snooping is turned on for vlan 2
```

Displayed Information	Explanation
Global mld snooping status	Whether or not the global MLD Snooping is enabled on the switch
L3 multicasting	Whether or not the layer 3 multicast protocol is running on the switch.
Mld snooping is turned on for vlan 1(querier)	On which VLAN of the switch is enabled MLD Snooping, if the VLAN are l2-general-querier.

2.Display the detailed MLD Snooping information of vlan1

```
Switch#show ipv6 mld snooping vlan 1
Mld snooping information for vlan 1

Mld snooping L2 general querier :Yes(COULD_QUERY)
Mld snooping query-interval :125(s)
Mld snooping max reponse time :10(s)
Mld snooping robustness :2
Mld snooping mrouter port keep-alive time :255(s)
Mld snooping query-suppression time :255(s)

MLD Snooping Connect Group Membership
```

```
Note:*-All Source, (S)- Include Source, [S]-Exclude Source
Groups Sources Ports Exptime System Level
Ff1e::15 (2000::1) Ethernet1/0/8 00:04:14 V2
(2000::2) Ethernet1/0/8 00:04:14 V2

Mld snooping vlan 1 mrouter port
Note:"!"-static mrouter port
!Ethernet1/0/2
```

Displayed Information	Explanation
Mld snooping L2 general querier	whether or not l2-general-querier is enabled on VLAN, the querier display status is set to could-query or suppressed
Mld snooping query-interval	Query interval time of the VLAN
Mld snooping max reponse time	Max response time of this VLAN
Mld snooping robustness	Robustness configured on the VLAN
Mld snooping mrouter port keep-alive time	Keep-alive time of the dynamic mrouter on this VLAN
Mld snooping query-suppression time	timeout of the VLAN as l2-general-querier at suppressed status.
MLD Snooping Connect Group Membership	Group membership of the VLAN, namely the correspondence between the port and （S,G）
Mld snooping vlan 1 mrouter port	Mrouter port of the VLAN, including both static and dynamic.

12.1.56 multicast-vlan

Syntax	multicast-vlan no multicast-vlan
Parameter	none
Default	Multicast VLAN function not enabled by default.
Mode	VLAN Configuration Mode
Usage	Enable multicast VLAN function on a VLAN; the “no” form of this command disables the multicast VLAN function. The multicast VLAN function can not be enabled on Private VLAN. To disabling the multicast VLAN function of the VLAN, configuration of VLANs associated with the multicast VLAN should be deleted. Note that the default VLAN can not be configured with this command and only one multicast VLAN is allowed on a switch.
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan

12.1.57 multicast-vlan association

Syntax	multicast-vlan association <vlan-list> no multicast-vlan association <vlan-list>	
Parameter	<vlan-list>	<vlan-list> the VLAN ID list associated with multicast VLAN. Each VLAN can only be associated with one multicast VLAN and the association will only succeed when every VLAN listed in the VLAN ID table exists.
Default	The multicast VLAN is not associated with any VLAN by default.	
Mode	VLAN Configuration Mode	
Usage	Associate several VLANs with a multicast VLAN; the "no" form of this command cancels the association relations. After a VLAN is associated with the multicast VLAN, when there comes the multicast order in the port of this VLAN, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. The VLAN associated with the multicast VLAN should not be a Private VLAN. A VLAN can only be associated with another VLAN after the multicast VLAN is enabled. Only one multicast VLAN can be enabled on a switch.	
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association 3, 4	

12.1.58 multicast-vlan association interface

Syntax	multicast-vlan association interface (ethernet | port-channel) IFNAME out-tag <tag-id> no multicast-vlan association interface (ethernet | port-channel) IFNAME	
Parameter	IFNAME	The name of the ethernet port or port-channel port
	<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.
Default	None	
Mode	VLAN Configuration Mode	
Usage	Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports	

	and the multicast VLAN. 'associated VLAN' and 'associated port' of the multicast VLAN are absolute, they do not affect each other when happening the cross. The port of the aggregation member cannot be associated, but the associated port is able to be added to port-group and cancelling the association. The configured port type includes port-channel port or ethernet port and the port is only configured as ACCESS mode. The port (it will be associated) cannot belong to the multicast VLAN, in the same way, the associated port cannot be divided in multicast VLAN. 5. When the associated port mode is set as non ACCESS mode, the mode cannot be changed.
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#multicast-vlan association interface port-channel 2 Switch(config-vlan2)#no multicast-vlan association interface ethernet 1/2 Switch(config-vlan2)#no multicast-vlan association interface port-channel 2

12.1.59 multicast-vlan mode

Syntax	multicast-vlan mode {dynamic | compatible}
	no multicast-vlan mode {dynamic | compatible}	

Parameter	dynamic	dynamic mode
	compatible	compatible mode
Default	Neither of the two modes	
Mode	VLAN Configuration Mode	
Usage	This command is used to configure the two modes of the multicast vlan; the no command cancels this configuration. When configured as dynamic mode, the mrouter port will not be added automatically any mort when issuing the multicast entries; when configured as compatible mode, the report packet will be not transmitted to the mrouter port any more. When it is not configured as default, the mrouter port will be added when issuing the multicast entries and the report packet will be transmitted to the mrouter port when it is received.	
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast vlan mode dynamic	

12.1.60 switchport association multicast-vlan

Syntax	switchport association multicast-vlan <vlan-id> out-tag <tag-id> no switchport association multicast-vlan <vlan-id>	
Parameter	<vlan-id>	The multicast VLAN associates with the port. Each port can only be associated with one multicast VLAN, and the association will be successful only when the multicast VLAN is existent.
	<tag-id>	Specify vlan tag of the multicast data forwarded by the associated port, only the tag of the associated port allows the multicast VLAN, the tag-id takes effect. Its range from 1 to 4094.
Default	The port is not associated with any multicast VLAN by default.	
Mode	Interface Configuration Mode	
Usage	Associate a port with the specified multicast VLAN; the no command cancels the association. After a port is associated with the multicast VLAN, when there comes the multicast order in the port, then the multicast data will be sent from the multicast VLAN to this port, so to reduce the data traffic. If the associated port is set as trunk port and allows the multicast VLAN, the multicast traffic with the specified vlan tag will be forwarded. The port can only be associated with the multicast VLAN after the multicast VLAN is enabled.	
Example	Switch(config)#vlan 2 Switch(config-vlan2)# multicast-vlan Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#switchport mode trunk Switch(config-if-ethernet1/0/1)#switchport association multicast-vlan 2 out-tag 5	

Chapter 13 Security Function

13.1 ACL

13.1.1 absolute-periodic/periodic

Command	[no] absolute-periodic {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday |Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday |Sunday}<end_time> [no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday} |daily| weekdays | weekend} <start_time> to <end_time>	
Parameter	Monday	Monday
	Tuesday	Tuesday
	Wednesday	Wednesday
	Thursday	Thursday
	Friday	Friday
	Saturday	Saturday
	Sunday	Sunday
	daily	Every day of the week
	weekdays	Monday thru Friday
	weekend	Saturday thru Sunday
	<start_time>	start time ,HH:MM:SS (hour: minute: second)
	<end_time>	end time,HH:MM:SS (hour: minute: second)
Default	No time-range configuration.	
Mode	time-range mode	
Usage Guide	This command is used for the switch configuration command effective time-range. By creating a time period and referencing it in a command, the user can make the command take effect within the time range defined that time period. When, for example, a ACL rule only needs to take effect within a specific time range, it can be configured first and then referenced when configuring the ACL rule, so that the ACL rule can only take effect within the time range defined for that time period. In a time period, the time range can be defined in two ways: Absolute cycle time a period of time that takes effect within a specified time range, such as Tuesday 8:00 to Saturday 8:00. Periodic period: a period of time in which a cycle (such as 14 to 16:00 a week) takes effect. The no command to delete the configured time-range.	

Example	Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday. Switch(config)#time-range admin_timer Switch(config-time-range-admin_timer)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00 Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday. Switch(config-time-range-admin_timer)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

13.1.2 absolute start

Command	[no] absolute start <start_time> <start_data> [end <end_time> <end_data>]	
Parameter	<start_time>	start time ,HH:MM:SS (hour: minute: second)
	<start_data>	start data ,YYYY.MM.DD（year.month.day）
	<end_time>	end time ,HH:MM:SS (hour: minute: second)
	<end_data>	end data ,YYYY.MM.DD（year.month.day）
Default	No time-range configuration by default.	
Mode	Time-range mode	
Usage Guide	Define an absolute time-range, this time-range operates subject to the clock of this equipment. Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration. The no command delete configuration.	
Example	Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005. Switch(config)#time-range admin_timer Switch(config-time-range-admin_timer)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26	

13.1.3 access-list (ip extended)

Command

access-list <num> {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

access-list <num> {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

access-list <num> {deny | permit} tcp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

access-list <num> {deny | permit} udp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax>] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

access-list <num> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf |<protocol-num> } {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [precedence <prec>] [tos <tos>][time-range <time-range-name>]

no access-list <num>

Parameter

<num>	the No. of access-list, 100-299
deny	deny packets
permit	permit packets
<sIpAddr>	the source IP address, the format is dotted decimal notation
<sMask>	the reverse mask of source IP, the format is dotted decimal notation
<sPort>	source port No., 0-65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
<protocol>	the No. of upper-layer protocol of ip, 0-255
<dIpAddr>	the destination IP address, the format is dotted decimal notation
<dMask>	the reverse mask of destination IP, the format is dotted decimal notation

<dPort>	destination port No. 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	the type of igmp, 0-15
<icmp-type>	the type of icmp, 0-255
<icmp-code>	protocol No. of icmp, 0-255
<prec>	IP priority, 0-7
<tos>	to value, 0-15
<time-range-name>	the name of time-range

Default	By default,no access-lists configured.
Mode	Global mode
Usage Guide	Create a numeric extended IP access rule to match specific IP protocol or all IP protocol;if access-list of this coded numeric extended does not exist,thus to create such a access-list. When the user assign specific <num> for the first time,ACL of the serial number is created,then the lists are added into this ACL;the access list which marked 200-299 can configure not continual reverse mask of IP address. <igmp-type>represent the type of IGMP packet, and usual values please refer to the following description: 17(0x11): IGMP QUERY packet 18(0x12): IGMP V1 REPORT packet 22(0x16): IGMP V2 REPORT packet 23(0x17): IGMP V2 LEAVE packet 34(0x22): IGMP V3 REPORT packet 19(0x13): DVMR packet 20(0x14): PIM V1 packet Particular notice:The packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured. The no command delete configuration.
Example	Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass. Switch(config)#access-list 110 deny icmp any any-destination Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32

13.1.4 access-list (ip standard)

Command

access-list <num> {deny | permit} {{<sIpAddr> <sMask >} | any-source|{host-source <sIpAddr>}}
no access-list <num>

Parameter

<num>	the No. of access-list, 100-199
deny	deny packets
permit	permit packets
<sIpAddr>	the source IP address, the format is dotted decimal notation
<sMask>	the reverse mask of source IP, the format is dotted decimal notation

Default

By default,no access-lists configured.

Mode

Global mode

Usage Guide

Create a numeric standard IP access-list. If this access-list exists, then add a rule list;When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL.

The "no access-list <num>" operation of this command is to delete a numeric standard IP access-list.

Example

Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.

```
Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255
Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255
```

13.1.5 access-list(mac extended)

Command	access-list <num> {deny | permit} {any-source-mac | {host-source-mac <sIpAddr>}} <host_smac>} | {<smac> <smac-mask>}} {any-destination-mac | {host-destination-mac <host_dmac>} | {<dmac> <dmac-mask>}} [untagged-eth2 | tagged-eth2 | untagged-802-3 | tagged-802-3] no access-list <num>	
Parameter	<num>	the access-list No. which is a decimal's No. from 1100-1199
	deny	deny packets
	permit	permit packets
	any-source-mac	any source address
	host-source-mac	source mac address
	<sIpAddr>	the source IP address, the format is dotted decimal notation
	<host_smac>	source mac address
	<smac>	source mac address
	<smac-mask>	mask (reverse mask) of source MAC address
	any-destination-mac	any destination address
	host-destination-mac	destination MAC address
	<host_dmac>	destination MAC address
	<dmac>	destination MAC address
	<dmac-mask>	mask (reverse mask) of destination MAC address
	untagged-eth2	format of untagged ethernet II packet
	tagged-eth2	format of tagged ethernet II packet;
	untagged-802-3	format of untagged ethernet 802.3 packet
	tagged-802-3	format of tagged ethernet 802.3 packet
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Define an extended numeric MAC ACL rule. When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL. "no access-list <num>" command deletes an extended numeric MAC access-list rule.	
Example	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets pass. Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2	

13.1.6 access-list(mac-ip extended)

Command

access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}| {<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}icmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}| any-destination|{host-destination<destination-host-ip>}}[<icmp-type> [<icmp-code>]] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]

access-list<num>{deny|permit}{any-source-mac| {host-source-mac<host_smac>}| {<smac><smac-mask>}} {any-destination-mac|{host-destination-mac <host_dmac>}| {<dmac><dmac-mask>}}igmp {{<source><source-wildcard>}|any-source| {host-source<source-host-ip>}} {{<destination><destination-wildcard>}| any-destination| {host-destination<destination-host-ip>}} [<igmp-type>] [precedence <precedence>] [tos <tos>][time-range<time-range-name>]

access-list <num> {deny|permit}{any-source-mac| {host-source-mac<host_smac> }| { <smac> <smac-mask> }}{any-destination-mac| {host-destination-mac <host_dmac> }| { <dmac> <dmac-mask> }}tcp {{ <source> <source-wildcard> }|any-source| {host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }] {{ <destination> <destination-wildcard> } | any-destination | {host-destination <destination-host-ip> }} [d-port { <port3> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence<precedence>] [tos <tos>] [time-range <time-range-name>]

access-list <num> {deny|permit}{any-source-mac| {host-source-mac<host_smac> }| { <smac> <smac-mask> }}{any-destination-mac| {host-destination-mac <host_dmac> }| { <dmac> <dmac-mask> }}udp {{ <source> <source-wildcard> }|any-source| {host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }] {{ <destination> <destination-wildcard> }|any-destination| {host-destination <destination-host-ip> }}[d-port{ <port3> | range <dPortMin> <dPortMax> }] [precedence <precedence>] [tos <tos>][time-range <time-range-name>]

access-list <num> {deny|permit}{any-source-mac| {host-source-mac <host_smac> }| { <smac> <smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }| { <dmac> <dmac-mask> }} {eigrp|gre|igrp|ip|ipinip|ospf|{ <protocol-num> }} {{ <source><source-wildcard> }|any-source|{host-source <source-host-ip> }} {{ <destination><destination-wildcard> }|any-destination| {host-destination <destination-host-ip> }}[precedence <precedence>] [tos <tos>][time-range <time-range-name>]

no access-list <num>

Parameter	<num>	access-list serial No. this is a decimal's No. from 3100-3299
	deny	deny packets
	permit	permit packets
	any-source-mac	any source mac address
	any-destination-mac	any destination mac address
	host_smac , smac	source mac address
	smac-mask	(reverse mask) of source MAC address
	host_dmac , dmas	destination mac address
	dmac-mask	(reverse mask) of destination MAC address
	protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
	source-host-ip	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
	source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
	destination-host-ip	No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
	destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
	s-port	means the need to match TCP/UDP source port
	port1	value of TCP/UDP source interface No.,Interface No. is an integer from 0-65535
	d-port	means need to match TCP/UDP destination interface
	sPortMin	the down boundary of source port
	sPortMax	the up boundary of source port
	port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
	dPortMin	the down boundary of destination port
	dPortMax	the up boundary of destination port
	[ack] [fin] [psh] [rst] [urg] [syn]	only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of

	corresponding position, then initialization of TCP data report is enabled to form a match when in connection
precedence	packets can be filtered by priority which is a number from 0-7
tos	packets can be filtered by service type which ia number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

Default	By default,no access-lists configured.
Mode	Global mode
Usage Guide	Define an extended numeric MAC-IP ACL rule. When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address. The no command deletes a extended numeric MAC-IP ACL access-list rule.
Example	Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100. Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination

13.1.7 access-list (mac standard)

Command	access-list <num> {deny | permit} {any-source-mac | {host-source-mac <host_smac> } | {<smac> <smac-mask>} } no access-list <num>	
Parameter	<num>	the access-list No. which is a decimal's No. from 700-799
	deny	deny packets
	permit	permit packets
	host_smac，smac	source mac address
	smac-mask	(reverse mask) of source MAC address
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Define a standard numeric MAC ACL rule. When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL. The no command deletes a standard numeric MAC ACL access-list rule.	
Example	Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab. Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-00 Switch(config)# access-list 700 deny 00-00-00-00-00-ab 00-00-00-FF-00-00	

13.1.8 clear access-group statistic

Command	clear access-group statistic [ethernet <interface-name>]	
Parameter	interface-name	interface-name
Default	None.	
Mode	Admin Mode	
Usage Guide	Empty packet statistics information of the specified interface.	
Example	Empty packet statistics information of interface. Switch#clear access-group statistic	

13.1.9 firewall

Command	firewall {enable | disable}	
Parameter	{enable | disable}	enable or disable
Default	None.	
Mode	Global Mode	
Usage Guide	Enable or disable firewall. Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.	
Example	Enable firewall. Switch(config)#firewall enable	

13.1.10 ip access extended

Command	[no] ip access extended <name>	
Parameter	name	the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32.
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Create a named extended IP access list. When this command is issued for the first time, an empty access list will be created. The no prefix will remove the named extended IP access list including all the rules.	
Example	To create a extended IP access list name tcpFlow. Switch(config)#ip access-list extended tcpFlow	

13.1.11 ip access standard

Command	[no] ip access standard<name>	
Parameter	name	the name of the access list. The name can be formed by non-all-digit characters of length of 1 to 32
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Create a named standard access list. When this command is issued for the first time, an empty access list will be created. The no prefix will remove the named standard access list including all the rules in the list.	
Example	To create a standard IP access list name ipFlow. Switch(config)#ip access-list standard ipFlow	

13.1.12 ipv6 access-list

Command	ipv6 access-list <num-std> {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} no ipv6 access-list <num-std>	
Parameter	num-std	the list number, list range is between 500 ~ 599
	deny	deny packets
	permit	permit packets
	sIPv6Prefix	the prefix of the ipv6 source address
	sPrefixlen	the length of prefix of the ipv6 source address, range is between 1 ~ 128
	sIPv6Addr	the ipv6 source address
Default	By default,no access-lists configured.	
Mode	Global mode	

Usage Guide	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list. The no command deletes a numbered standard IP access-list.
Example	Creates a numbered 520 standard IP access-list, allow the source packet from 2003:1:2:3::1/64 pass through the net, and deny all the other packet from the source address 2003:1:2::1/48 pass through. Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64 Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48

13.1.13 ipv6 access standard

Command	ipv6 access-list standard <name> no ipv6 access-list standard <name>	
Parameter	name	the name for access list, the character string length is from 1 to 32
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Create a name-based standard IPv6 access list. When this command is run for the first time, only an empty access list with no entry will be created. The no command deletes the name-based standard IPv6 access list (including all entries).	
Example	Create a standard IPv6 access list named ip6Flow. Switch(config)#ipv6 access-list standard ip6Flow	

13.1.14 ipv6 access extended

Command	ipv6 access-list extended <name> no ipv6 access-list extended <name>	
Parameter	name	the name for access list, the character string length is from 1 to 32
Default	By default,no access-lists configured.	
Mode	Global mode	
Usage Guide	Create a name-based extended IPv6 access list. When this command is run for the first time, only an empty access list with no entry will be created. The no command delete the name-based extended IPv6 access list.	
Example	Create an extensive IPv6 access list named tcpFlow. Switch(config)#ipv6 access-list extended tcpFlow	

13.1.15 access-group

Command	{ip|ipv6|mac|mac-ip} access-group <name> {in} [traffic-statistic] no {ip|ipv6|mac|mac-ip} access-group <name> {in}	
Parameter	name	the name for access list, the character string length is from 1 to 32
	traffic-statistic	flow statistics
Default	By default,the entry of port is not bound ACL.	
Mode	Port Mode	
Usage Guide	Apply an access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options. Note:when a ACL has multiple rules, traffic-statistic can't configure. There are four kinds of packet head field based on concerned:MAC ACL,IP ACL,MAC-IP ACL and IPv6 ACL; to some extent,ACL filter behavior (permit,deny) has a conflict when a data packet matches multi types of four ACLs.The strict priorities are specified for each ACL based on outcome veracity.It can determine final behavior of packet filter through priority when the filter behavior has a conflict. When binding ACL to port, there are some limits as below: 1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL. 2. When binding four ACLs and data packet matching the multi ACLs simultaneity, the priority from high to low are shown as below, Ingress IPv6 ACL Ingress MAC-IP ACL Ingress MAC ACL Ingress IP ACL The no command deletes access-list binding on the port.	
Example	Binding AAA access-list to entry direction of port. Switch(config)#interface ethernet 1/0/5 Switch(config-If-Ethernet1/0/5)#ip access-group aaa in	

13.1.16 mac access extended

Command	mac-access-list extended <name> no mac-access-list extended <name>
Parameter	name — name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32. (remark: sensitivity on capital or small letter.)
Default	By default，no access-lists configured.
Mode	Global mode
Usage Guide	Define a name-manner MAC ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included. The no command deletes this ACL.
Example	Create an MAC ACL named mac_acl. Switch(config)# mac-access-list extended mac_acl Switch(config-mac-ext-nacl-mac_acl)#

13.1.17 mac-ip access extended

Command	mac-ip-access-list extended <name> no mac-ip-access-list extended <name>	
Parameter	name	name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 32 (remark: sensitivity on capital or small letter).
Default	By default，no named MAC-IP access-list.	
Mode	Global mode	
Usage Guide	Define a name-manner MAC-IP ACL or enter access-list configuration mode. After assigning this command for the first time, only an empty name access-list is created and no list item included. The no command deletes this ACL.	
Example	Create an MAC-IP ACL named macip_acl. Switch(config)# mac-ip-access-list extended macip_acl Switch(config-macIp-ext-nacl-macip_acl)#	

13.1.18 permit | deny (ip extended)

Command

[no] {deny | permit} icmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<icmp-type> [<icmp-code>]] [precedence <prec>][tos <tos>] [time-range<time-range-name>]

[no] {deny | permit} igmp {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [<igmp-type>] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

[no] {deny | permit} tcp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [ack+fin+psh+rst+urg+syn] [precedence <prec>] [tos <tos>][time-range <time-range-name>]

[no] {deny | permit} udp {{ <sIpAddr> <sMask> } | any-source | {host-source <sIpAddr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] {{ <dIpAddr> <dMask> } | any-destination | {host-destination <dIpAddr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [precedence <prec>] [tos <tos>] [time-range<time-range-name>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <protocol-num>} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}} {{<dIpAddr> <dMask>} | any-destination | {host-destination <dIpAddr>}} [precedence <prec>] [tos <tos>][time-range<time-range-name>]

Parameter

deny	deny packets
permit	permit packets
<sIpAddr>	the source IP address, the format is dotted decimal notation
<sMask>	the reverse mask of source IP, the format is dotted decimal notation
<sPort>	source port No., 0-65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
<dIpAddr>	the destination IP address, the format is dotted decimal notation
<dMask>	the reverse mask of destination IP, the format is dotted decimal

	notation, attentive position o, ignored position 1
<dPort>	destination port No. 0-65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	the type of igmp, 0-15
<icmp-type>	the type of icmp, 0-255
<icmp-code>	protocol No. of icmp, 0-255
<prec>	IP priority, 0-7
<tos>	to value, 0-15
<time-range-name>	time range name

Default

By default，no access-list configured.

Mode

Name extended IP access-list configuration mode

Usage Guide

Create a name extended IP access rule to match specific IP protocol or all IP protocol.

The no command will delete this access list.

Example

Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)# access-list ip extended udpFlow
Switch(config-ip-ext-nacl-udpFlow)#deny igmp any any-destination
Switch(config-ip-ext-nacl-udpFlow)#permit udp any host-destination 192.168.0.1 d-port
32
```

13.1.19 permit | deny (ip standard)

Command

```
{deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}
no {deny | permit} {{<sIpAddr> <sMask>} | any-source | {host-source <sIpAddr>}}
```

Parameter

deny	deny packets
permit	permit packets
<sIpAddr>	the source IP address, the format is dotted decimal notation
<sMask>	the reverse mask of source IP, the format is dotted decimal notation

Default

By default，no access-list configured.

Mode

Name standard IP access-list configuration mode

Usage Guide

Create a name standard IP access rule

The no command deletes this name standard IP access rule.

Example

Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

```
Switch(config)# access-list ip standard ipFlow
Switch(config-std-nacl-ipFlow)# permit 10.1.1.0 0.0.0.255
Switch(config-std-nacl-ipFlow)# deny 10.1.1.0 0.0.255.255
```

13.1.20 permit | deny (ipv6 extended)

Command

[no] {deny | permit} icmp {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [<icmp-type> [<icmp-code>]] [dscp <dscp>] [flow-label <fl>] [time-range <time-range-name>]

[no] {deny | permit} tcp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [syn | ack | urg | rst | fin | psh] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} udp { <sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr> }} [s-port { <sPort> | range <sPortMin> <sPortMax> }] { <dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr> }} [d-port { <dPort> | range <dPortMin> <dPortMax> }] [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} <next-header> {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>][time-range <time-range-name>]

[no] {deny | permit} {<sIPv6Prefix/sPrefixlen> | any-source | {host-source <sIPv6Addr>}} {<dIPv6Prefix/dPrefixlen> | any-destination | {host-destination <dIPv6Addr>}} [dscp <dscp>] [flow-label <fl>] [time-range<time-range-name>]

Parameter

deny	deny packets
permit	permit packets
<sIPv6Addr>	the source IPv6 address
<sPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128
<sPort>	source port number, the range is 0 ~ 65535
<sPortMin>	the down boundary of source port
<sPortMax>	the up boundary of source port
<dIPv6Addr>	the destination IPv6 address
<dPrefixlen>	the length of the IPv6 address prefix, the range is 1 ~ 128

<dPort>	destination port number, the range is 0 ~ 65535
<dPortMin>	the down boundary of destination port
<dPortMax>	the up boundary of destination port
<igmp-type>	type of the IGMP
<icmp-type>	icmp type
<icmp-code>	icmp protocol number
<dscp>	IPv6 priority ,the range is 0 ~ 63
<flowlabel>	value of the flow label, the range is 0 ~ 1048575
syn,ack,urg,rst,fin, psh,tcp	label position
<next-header>	the IPv6 next-header
<time-range-name>	time range name

Default

By default，No access control list configured.

Mode

IPv6 nomenclature extended access control list mode

Usage Guide

Create an extended nomenclature IPv6 access control rule for specific IPv6 protocol.

The no command will delete this access list.

Example

Create an extended access control list named udpFlow,denying the igmppackets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

```
Switch(config)#ipv6 access-list extended udpFlow
Switch(config-ipv6-ext-nacl-udpFlow)#deny igmp any any-destination
Switch(config-ipv6-ext-nacl-udpFlow)#ppermit udp any-source host-destination 2001:1:2:3::1 dPort 32
```

13.1.21 permit | deny (ipv6 standard)

Command

[no] {deny | permit} {{<sIPv6Prefix/sPrefixlen>} | any-source | {host-source <sIPv6Addr>}}

Parameter

deny	deny packets
permit	permit packets
<sPrefixlen>	the length of the IPv6 address prefix, the valid range is 1~128
<sIPv6Addr>	the source IPv6 address

Default

No access list configured by default.

Mode

Standard IPv6 nomenclature access list mode

Usage Guide

Create a standard nomenclature IPv6 access control rule.

The no form of this command deletes the nomenclature standard IPv6 access control rule.

Example

Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.

```
Switch(config)#ipv6 access-list standard ipv6Flow
Switch(config-ipv6-std-nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(config-ipv6-std-nacl-ipv6Flow)# deny 2001:1:2:3::1/48
```

13.1.22 permit | deny (mac extended)

Command

```
[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} [cos <cos-val> [ <cos-bitmask> ]] [vlanId <vid-value> [ <vid-mask> ]]
[ethertype <protocol> [ <protocol-mask> ]]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} [untagged-eth2 [ethertype <protocol>[protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} [untagged-802-3]

[no]{deny|permit} {any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} [tagged-eth2 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value>
[ <vid-mask> ]] [ethertype <protocol>[ <protocol-mask> ]]]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }} {any-destination-mac|{host-destination-mac <host_dmac> }|{ <dmac>
<dmac-mask> }} [tagged-802-3 [cos <cos-val>[ <cos-bitmask> ]] [vlanId <vid-value>
[ <vid-mask> ]]]
```

Parameter	deny	deny packets
	permit	permit packets
	any-source-mac	any source of MAC address
	any-destination-mac	any destination of MAC address
	host_smac, smac	source MAC address
	smac-mask	mask (reverse mask) of source MAC address
	host_dmac, dmas	destination MAC address
	dmac-mask	(reverse mask) of destination MAC address
	untagged-eth2	format of untagged ethernet II packet
	tagged-eth2	format of tagged ethernet II packet
	untagged-802-3	format of untagged ethernet 802.3 packet
	tagged-802-3	format of tagged ethernet 802.3 packet
	cos-val	cos value, 0-7
	cos-bitmask	cos mask, 0-7reverse mask and mask bit is consecutive

vid-value	VLAN No, 1-4094
vid-bitmask	VLAN mask, 0-4095, reverse mask and mask bit is consecutive
protocol	specific Ethernet protocol No., 1536-65535
protocol-bitmask	protocol mask, 0-65535, reverse mask and mask bit is consecutive

Default

By default，no access-list configured.

Mode

Name extended MAC access-list configuration mode

Usage Guide

Define an extended name MAC ACL rule.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

The no command deletes this extended name IP access rule.

Example

The forward source MAC address is not permitted as 00-12-11-23-XX-XX of 802.3 data packet.

```
Switch(config)# mac-access-list extended macExt
Switch(config-mac-ext-nacl-macExt)#deny 00-12-11-23-00-00 00-00-00-00-ff-ff
any-destination-mac untagged-802-3
Switch(config-mac-ext-nacl-macExt)#deny   00-12-11-23-00-00   00-00-00-00-ff-ff
any tagged-802
```

13.1.23 permit | deny (mac-ip extended)

Command

```
[no]{deny|permit} {any-source-mac|{host-source-mac<host_smac>}|
{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}} icmp{{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}|
any-destination|{host-destination  <destination-host-ip>}}  [<icmp-type>  [<icmp-code>]]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]

[no]{deny|permit} {any-source-mac|{host-source-mac<host_smac>}|
{<smac><smac-mask>}} {any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}} igmp{{<source><source-wildcard>}|any-source|
{host-source<source-host-ip>}} {{<destination><destination-wildcard>}|
any-destination|{host-destination <destination-host-ip>}} [<igmp-type>]
[precedence <precedence>] [tos <tos>][time-range<time-range-name>]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }| { <smac>
<smac-mask> }}{any-destination-mac|{host-destination-mac<host_dmac> }|
{ <dmac> <dmac-mask> }}tcp{{ <source><source-wildcard> }|any-source| {host-source
<source-host-ip> }}[s-port { <port1> |range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> } | any-destination| {host-destination
<destination-host-ip> }} [d-port { <port3> | range<dPortMin> <dPortMax> }]
[ack + fin + psh + rst + urg + syn] [precedence <precedence> ] [tos <tos> ]
[time-range <time-range-name> ]

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac> }|{ <smac>
<smac-mask> }}{any-destination-mac|{host-destination-mac <host_dmac> }|
{ <dmac> <dmac-mask> }}udp{{ <source> <source-wildcard> }|any-source|
{host-source <source-host-ip> }}[s-port{ <port1> | range <sPortMin> <sPortMax> }]
{{ <destination> <destination-wildcard> }|any-destination| {host-destination
<destination-host-ip> }} [d-port { <port3> | range <dPortMin> <dPortMax> }]
[precedence <precedence> ] [tos <tos> ][time-range <time-range-name> ]

[no]{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac>
<smac-mask>}}{any-destination-mac|{host-destination-mac<host_dmac>}|
{<dmac><dmac-mask>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<protocol-num>}}
{{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}
{{<destination><destination-wildcard>}|any-destination|{host-destination
<destination-host-ip>}} [precedence <precedence>] [tos <tos>]
```

	[time-range<time-range-name>]	
Parameter	num	access-list serial No. this is a decimal's No. from 3100-3199
	deny	deny packets
	permit	permit packets
	any-source-mac	any source MAC address
	any-destination-mac	any destination MAC address
	host_smac, smac	source MAC address
	smac-mask	(reverse mask) of source MAC address
	host_dmac, dmas	destination MAC address
	dmac-mask	(reverse mask) of destination MAC address
	protocol	No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list
	source-host-ip, source	No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression
	source-wildcard	reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
	destination-host-ip , destination	destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression
	destination-wildcard	mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask
	s-port	means the need to match TCP/UDP source port
	port1	value of TCP/UDP source interface No., Interface No. is an integer from 0-65535
	<sPortMin>	the down boundary of source port
	<sPortMax>	the up boundary of source port
	d-port	means need to match TCP/UDP destination interface
	port3	value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535
	<dPortMin>	the down boundary of destination port
	<dPortMax>	the up boundary of destination port
	[ack] [fin] [psh] [rst] [urg] [syn]	(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is

	enabled to form a match when in connection
precedence	packets can be filtered by priority which is a number from 0-7
tos	packets can be filtered by service type which ia number from 0-15
icmp-type	ICMP packets can be filtered by packet type which is a number from 0-255
icmp-code	ICMP packets can be filtered by packet code which is a number from 0-255
igmp-type	ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255
time-range-name	name of time range

Default	By default，no access-list configured.
Mode	Name extended MAC-IP access-list configuration mode
Usage Guide	Define an extended name MAC-IP ACL rule. No form deletes one extended numeric MAC-IP ACL access-list rule.
Example	Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100. Switch(config)# mac-ip-access-list extended macIpExt Switch(config-macip-ext-nacl-macIpExt)# deny any-source-mac any-destination-mac udp any-source s-port 100 any-destination

13.1.24 show access-lists

Command

show access-lists [<num>|<acl-name>]

Parameter

<num>|<acl-name>	specific ACL No|specific ACL name character string

Default

None。

Mode

Admin Mode

Usage Guide

Reveal ACL of configuration.

When not assigning names of ACL, all ACL will be revealed, used x time（ s ）indicates the times of ACL to be used.

Example

Reveal ACL of configuration.

```
Switch#show access-lists
access-list 10(used 0 time(s))
  access-list 10 deny any-source
access-list 100(used 1 time(s))
  access-list 100 deny ip any any-destination
  access-list 100 deny tcp any any-destination
access-list 1100(used 0 time(s))
  access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800
```

13.1.25 show access-group

Command	show access-group in (interface {Ethernet | Ethernet IFNAME})	
Parameter	IFNAME	Port name
Default	None.	
Mode	admin/ Global Mode	
Usage Guide	Display the ACL binding status on the port. When not assigning interface names, all ACL tied to port will be revealed.	

Example

Displays all ACL bound to the port.

```
Switch#show access-group
interface name: Ethernet 1/0/1
  IP Ingress access-list used is 100, traffic-statistics Disable.
interface name: Ethernet1/0/2
  IP Ingress access-list used is 1, packet(s) number is 11110.
```

13.1.26 show firewall

Command	show firewall	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Reveal configuration information of packet filtering functions.	

Example

Display firewall status.

```
Switch#show firewall
Firewall status: Enable.
```

13.1.27 show ipv6 access-lists

Command	show ipv6 access-lists [<num>|<acl-name>]	
Parameter	<num>	the number of specific access control list, the valid range is 500 ~ 699, amongst 500 ~ 599 is digit standard IPv6 ACL number, 600 ~ 699 is the digit extended IPv6 ACL number
	<acl-name>	the nomenclature character string of a specific access control list, lengthening within 1 ~ 32
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Show the configured IPv6 access control list. When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted.	

Example

Show the configured IPv6 access control list.

```
Switch#show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
  ipv6 access-list 500 deny any-source
ipv6 access-list 510(used 1 time(s))
  ipv6 access-list 510 deny ip any-source any-destination
  ipv6 access-list 510 deny tcp any-source any-destination
ipv6 access-list 520(used 1 time(s))
  ipv6 access-list 520 permit ip any-source any-destination
```

13.1.28 show time-range

Command	show time-range <word>
Parameter	<word> assign name of time-range needed to be revealed
Default	None.
Mode	Admin/Global Mode
Usage Guide	Reveal configuration information of time range functions. When not assigning time-range names, all time-range will be revealed. in used x time（s） is shown the times the ACL had been quoted.
Example	Reveal configuration information of time range functions. Switch#show time-range time-range timer1 (inactive, used 0 times) absolute-periodic Saturday 0:0:0 to Sunday 23:59:59 time-range timer2 (inactive, used 0 times) absolute-periodic Monday 0:0:0 to Friday

13.1.29 time-range

Command	[no] time-range <time_range_name>
Parameter	<time_range_name> time range name must start with letter or number, and the length cannot exceed 32 characters long
Default	By default，no time-range configuration.
Mode	Global Mode
Usage Guide	Create the name of time-range as time range name, enter the time-range mode at the same time. The no command to delete this time range.
Example	Create a time-range named admin_timer. Switch(config)#Time-range admin_timer

13.2 Self-defined ACL

13.2.1 userdefined-access-list standard offset

Command

userdefined-access-list standard offset [window1 { l3start | l4start} <offset>] [window2 { l3start | l4start } <offset>] [window3 { l3start | l4start } <offset>] [window4 { l3start | l4start } <offset>] [window5 { l3start | l4start } <offset>] [window6 { l3start | l4start } <offset>] [window7 { l3start | l4start } <offset>] [window8 { l3start | l4start } <offset>] [window9 { l3start | l4start } <offset>] [window10 { l3start | l4start } <offset>] [window11 { l3start | l4start } <offset>] [window12 { l3start | l4start } <offset>]

no userdefined-access-list standard offset [window1] [window2] [window3] [window4] [window5] [window6] [window7] [window8] [window9] [window10] [window11] [window12]

Parameter

window1-window12	self-defined window 1 to 12
l3start	The start offset position is start of layer3 (It can be effective only when the start of layer3 exists)
l4start	The start offset position is start of layer4 (It can be effective only when the start of layer4 exists)
offset	The configured offset is from 0 to 178 (unit is 2Bytes)

Default

No Configuration Template.

Mode

Global Mode

Usage Guide

Create a standard self-defined ACL template. If the template exists, the corresponding window of the template can be modified.

{l2endoftag | l3start | l4start}: used to configure the start offset position of a window, <offset>: used to the offset of a window, the range is <0-178>, unit is 2Bytes,namely, 0 means 0Bytes offset and 1 means 2Bytes offset. Standard self-defined ACL template can configure the start offset position and offset for 12 window at most. One standard self-defined ACL template can be shared in global mode. The window cannot be modified if the standard self-defined ACL rule is configured with this window. But if the standard self-defined ACL rule is not configured, the window configuration can be modified with this command.

The no command can delete one or more offset configuration of the window in the template or delete the whole template. The window in the template can be deleted

	successfully when it is not used by the self-defined ACL rule. Ipv6 only supports window1-6, the biggest offset of l3start includes the head of L2, the biggest offset of l4start includes the head of L2 and L3. The no command deletes the window of the standard self-defined ACL template. If the window is not specified, the standard self-defined ACL template will be deleted.
Example	Create a global template with 7 windows (3-9) to configure the start offset position and the offset: Switch(config)#userdefined-access-list standard offset window3 l2 0 window4 l2 2 window5 l3 0 window6 l3 1 window7 l3 2 window8 l4 1 window9 l4 2

13.2.2 userdefined-access-list standard

Command

```
userdefined-access-list standard <1200-1299> {permit|deny} {window1|window2|
window3|window4|window5|window6|window7|window8|window9|window10|
window11|window12}

no userdefined-access-list standard <1200-1299> {permit|deny} {window1|window2|
window3|window4|window5|window6|window7|window8|window9|window10|
window11|window12}
```

Parameter

<1200-1299>	the access-list No. from 1200 to 1299 in decimal notation
permit	permit access
deny	deny access
window1-window12	custom windows 1 to 12

Default

By default, no any access-list configured.

Mode

Global Mode

Usage Guide

Create a numbered standard self-defined ACL. If the standard self-defined ACL exists, then a rule will be added to the ACL.
When users specify the specified <num> for the first time, create the ACL with this serial number, then add the entry into this ACL.

The no command deletes a numbered standard self-defined ACL.

Example

Permit the second bytes of the start of l3 is 0x4501. Permit the packets that the forth byte of the start of l4 is 0xFF.
Configure a rule in the same list to deny the packets that the fifth and the sixth bytes of the start of l3 is 0xFFAA.

```
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1
Switch(config)#userdefined-access-list standard 1200 permit window1 4501 FFFF
window2 00FF 00FF
Switch(config)#userdefined-access-list standard offset window3 l3 2
Switch(config)#userdefined-access-list standard 1200 deny any-source-mac
any-destination-mac untagged-eth2 window3 FFAA FFFF
```

13.2.3 userdefined access-group

Command

```
userdefined access-group <name> {in} [traffic-statistic]

no userdefined access-group <name> {in}
```

Parameter

<name>	the access-list name from 1200-1399 in decimal notation

Default

By default，userdefined-access-list is not bound to the port.

Mode

Physical Port Configuration Mode

Usage Guide

Apply userdefined-access-list to one direction of the port. Decide whether the statistical counter should be added to the ACL according to the options.
A self-defined access-list can be bound to the ingress of a port and can be configured at the ingress of the same port with other access-lists at the same time.The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.

The no command deletes the configuration bound to the port.

Example

The configured self-defined access-list is shown in the following:

```
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
```

Bind the self-defined access-list to Ethernet1/1:

```
Switch(config)#interface ethernet1/1
Switch(config-if-ethernet1/1)#userdefined access-group 1300 in
```

13.2.4 vacl userdefined access-group

Command

vacl userdefined access-group <name> {in} vlan <vlanId> [traffic-statistic]

no vacl userdefined access-group <name> {in} vlan <vlanId>

Parameter

<name>	the access-list name from 1200 to 1399 in decimal notation
vlanId	the bound VLAN，the range is 1-4094

Default

By default，userdefined-access-list is not bound to any VLAN.

Mode

Global Mode

Usage Guide

Apply userdefined-access-list to one direction of the specified VLAN, decide whether the statistical counter should be added to the ACL according to the options or.

A self-defined access-list can be bound to the ingress of a VLAN and can be configured at the ingress of the same VLAN with other access-lists at the same time.The deny rule is precedent when different access-lists are matching, that means if there is a access-lists match the deny rule, the deny rule must be executed, the permit rule will be executed oppositely.

The no command deletes the configuration bound to the specified VLAN.

Example

The configured self-defined access-list is shown in the following:

```
Switch(config)#userdefined-access-list standard offset window1 l3 0 window2 l4 1 window3 l3 1
Switch(config)#userdefined-access-list standard 1300 permit window1 4501 FFFF window2 00FF 00FF
Switch(config)#userdefined-access-list standard 1300 deny window1 FFAA0000 FFFF0000
```

Bind the self-defined access-list to VLAN1:

```
Switch(config)#vacl userdefined access-group 1300 in vlan 1
```

13.3 802.1x

13.3.1 dot1x accept-mac

Command	[no] dot1x accept-mac <mac-address> [interface <interface-name>]
Parameter	mac-address stands for MAC address interface-name for interface name and port number
Default	None.
Mode	Global Mode
Usage Guide	Add a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected. The no command deletes the entry from dot1x address filter table.
Example	Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/0/5. Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/0/5

13.3.2 dot1x eapor enable

Command	[no] dot1x eapor enable
Parameter	none none
Default	EAP relay authentication is used by default.
Mode	Global Mode
Usage Guide	Enables the EAP relay authentication function in the switch. The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server. The no command sets EAP local end authentication.
Example	Setting EAP local end authentication for the switch. Switch(config)#no dot1x eapor enable

13.3.3 dot1x enable

Command	[no] dot1x enable
Parameter	none none
Default	802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.
Mode	Global Mode and Port Mode
Usage Guide	Enables the 802.1x function in the switch and ports. The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed. The no command disables the 802.1x function.
Example	Enabling the 802.1x function of the switch and enable 802.1x for port1/0/12. Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable

13.3.4 dot1x ipv6 passthrough

Command	[no] dot1x ipv6 passthrough
Parameter	none none
Default	IPv6 passthrough function is disabled on the switch by default.
Mode	Port Mode
Usage Guide	Enable IPv6 passthrough function on a switch port, only applicable when access control mode is userbased. The function can only be enabled when 802.1x function is enabled both globally and on the port,with userbased being the control access mode. After it is enabled,users can send IPv6 messages without authentication. The no operation of this command will disable the function.
Example	Enable IPv6 passthrough function on port Ethernet1/0/12. Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/12 Switch(config-if-ethernet1/0/12)#dot1x enable Switch(config-if-ethernet1/0/12)#dot1x ipv6 passthrough

13.3.5 dot1x guest-vlan

Command	dot1x guest-vlan <vlanid> no dot1x guest-vlan
Parameter	vlanid the specified VLAN id, ranging from 1 to 4094
Default	By default，there is no 802.1x guest-vlan function on the port.
Mode	Port Mode
Usage Guide	Set the guest-vlan of the specified port. The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results: The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest VLAN. The authentication server assigns an Auto VLAN, then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again. Attention： There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port. Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect. The no command is used to delete the guest-vlan.
Example	Set Guest-VLAN of port Ethernet1/0/3 as VLAN 10. Switch(config)#dot1x enable Switch(config)#interface ethernet 1/0/3 Switch(config-if-ethernet1/0/3)#dot1x guest-vlan 10

13.3.6 dot1x macfilter enable

Command	[no] dot1x macfilter enable
Parameter	none none
Default	dot1x address filter is disabled by default.
Mode	Global Mode
Usage Guide	Enables the dot1x address filter function in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted. The no command disables the dot1x address filter function.
Example	Enabling dot1x address filter function for the switch. Switch(config)#dot1x macfilter enable

13.3.7 dot1x macbased guest-vlan

Command	dot1x macbased guest-vlan <vlanid> no dot1x macbased guest-vlan
Parameter	vlanid the configured vlan id, the range is from 1 to 4094
Default	Do not configure 802.1x macbased guest-vlan by default.
Mode	Port Mode
Usage Guide	Configure to appoint the port's guest-vlan based on the mac authentication. If there is no dedicated authentication client or the client version was too low, and it makes no clients authenticate successfully on the port in some time, then the access device will make this user join to the guest VLAN. User can get the 802.1x client software in guest VLAN, update the client or do other updating things (such as anti-virus software,

system patches and etc.) When the user under the port in Guest VLAN issues the authentication, this port will be stay in guest VLAN if the authentication failed;
if it was successful, there are two situations as below:
The authentication server issues an auto VLAN, in this time, the user left the guest VLAN and joined to the auto VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.
The authentication server did not issue the VLAN, in this time, the user left the guest VLAN and joined to the configured native VLAN. After the user was downline, this user will be assigned to the configured guest VLAN again.

Notice：

dot1x macbased guest-vlan can be configured only on the port based on mac authentication and in HYBRID mode.
Different macbased guestVLAN can be configured on different ports, but only one macbased guestVLAN can be configured on one port.

The no command deletes this guest-vlan.

Example

Configure the guest-vlan of Ethernet1/0/3 as Vlan 10.

```
Switch(config-if-ethernet1/0/3)#dot1x macbased guest-vlan 10
```

13.3.8 dot1x macbased port-down-flush

Command

[no] dot1x macbased port-down-flush

Parameter

none	none

Default

The command is not enabled by default.

Mode

Global Mode

Usage Guide

Enables this command, when the dot1x certification according to mac is down, delete the user who passed the certification of the port
When users who passed the certification according to mac changed among different ports, delete the user for the new certification. The command should be enable to delete the user.

	The no command does not make the down operation.
Example	When the dot1x certification according to mac is down, delete the user who passed the certification of the port. Switch(config)#dot1x macbased port-down-flush

13.3.9 dot1x max-req

Command	dot1x max-req <count> no dot1x max-req	
Parameter	count	the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10
Default	The default maximum for retransmission is 2.	
Mode	Global Mode	
Usage Guide	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response. The default value is recommended in setting the EAP request/ MD5 retransmission times. The no command restores the default setting.	
Example	Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times. Switch(config)#dot1x max-req 5	

13.3.10 dot1x user allow-movement

Command	[no] dot1x user allow-movement
Parameter	none — none
Default	Disable the authentication function after the user moves the port.
Mode	Global Mode
Usage Guide	Enable the authentication function after the user moves the port, so the switch allows user to process this authentication. In the condition that the switch connects with hub, when the user will be moved to other port, dot1x user allow-movement command should be enabled. The no command disables the function.
Example	Enable the authentication function after the user moves the port. Switch(config)#dot1x user allow-movement

13.3.11 dot1x user free-resource

Command	dot1x user free-resource <prefix> <mask> no dot1x user free-resource
Parameter	prefix — the segment for limited resource, in dotted decimal format mask — the mask for limited resource, in dotted decimal format
Default	There is no free resource by default.
Mode	Global Mode
Usage Guide	To configure 802.1x free resource. This command is available only if user based access control is applied. If user based access control has been applied, this command configures the limited resources which can be accessed by the un-authenticated users. For port based and MAC based access

	control, users could access no network resources before authentication. If TrustView management system is available, the free resource can be configured in TrustView server, and the TrustView server will distribute the configuration to the switches. To be noticed, only one free resource can be configured for the overall network. The no form command closes this function.
Example	To configure the free resource segment as 1.1.1.0, the mask is 255.255.255.0. Switch(config)#dot1x user free-resource 1.1.1.0 255.255.255.0

13.3.12 dot1x max-user macbased

Command	dot1x max-user macbased <number> no dot1x max-user macbased
Parameter	number the maximum users allowed, the valid range is 1 to 256
Default	The default maximum user allowed is 1.
Mode	Port Mode
Usage Guide	Sets the maximum users allowed connect to the port. This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network. The no command restores the default setting.
Example	Setting port 1/0/3 to allow 5 users. Switch(config-if-ethernet1/0/3)#dot1x max-user macbased 5

13.3.13 dot1x max-user userbased

Command	dot1x max-user userbased <number> no dot1x max-user userbased	
Parameter	number	the maximum number of users allowed to access the network, ranging from 1 to 1~256
Default	The maximum number of users allowed to access each port is 10 by default.	
Mode	Port Mode	
Usage Guide	Set the upper limit of the number of users allowed access the specified port when using user-based access control mode. This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed access the network, those extra users can not access the network. the no command is used to reset the default value.	
Example	Setting port 1/0/3 to allow 5 users. Switch(config-if-ethernet1/0/3)#dot1x max-user userbased 5	

13.3.14 dot1x portbased mode single-mode

Command	[no] dot1x portbased mode single-mode	
Parameter	none	none
Default	Disable the single-mode by default.	
Mode	Port Mode	
Usage Guide	Set the single-mode based on portbase authentication mode. This command takes effect when the access mode of the port is set as portbase only. Before configuring the single-mode, if the port has enabled dot1x port-method portbased	

	command and exist online users, the switch will enforce all users of this port are offline. After that, this port only allows a user to pass the authentication, the user can access the specified network resource, but other authentication users of this port will be denied and can not access the network. After disabling the single-mode, the switch also enforce the authenticated user is offline. The no command disables this function.
Example	Set port 1/0/1 based on port authentication mode to single mode. Switch(config-if-ethernet1/0/1)#dot1x portbased mode single-mode

13.3.15 dot1x port-control

Command	dot1x port-control {auto | force-authorized | force-unauthorized} no dot1x port-control	
Parameter	auto	enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant
	force-authorized	sets port to authorized status, unauthenticated data is allowed to pass through the port
	force-unauthorized	will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port
Default	When 802.1x is enabled for the port, auto is set by default.	
Mode	Port Mode	
Usage Guide	Sets the 802.1x authentication status. If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to auto. The no command restores the default setting.	
Example	Setting port1/0/1 to require 802.1x authentication mode. Switch(config-if-ethernet1/0/1)#dot1x port-control auto	

13.3.16 dot1x port-method

Command

dot1x port-method {macbased | portbased | userbased {standard | advanced}}
no dot1x port-method

Parameter

macbased	means the access control method based on MAC address
portbased	means the access control method based on port
userbased	means the access control method based on user, it can be divided into two types, one is standard access control method, and the other is advanced access control method
standard	Standard Access Control Method Based on User
advanced	Advanced User-Based Access Control

Default

Advanced access control method based on user is used by default.

Mode

Port Mode

Usage Guide

This command is used to configure the dot1x authentication method for the specified port.When port based authentication is applied,only one host can authenticate itself through one port.And after authentication,the host will be able to access all the resources.When MAC based authentication is applied,multiple host which are connected to one port can access all the network resources after authentication. When either of the above two kinds of access control is applied,un-authenticated host cannot access any resources in the network.

When user based access control is applied,un-authenticated users can only access limited resources of the network. The user based access control falls into two kinds – the standard access control and the advanced access control.The standard user based access control does not limit the access to the limited resources when the host is not authenticated yet.While the user based advanced access control can control the access to the limited resources before authentication is done.

Notes：

For standard control method based on user,the 802.1x free resource must be configured first, and it needs to be used with dot1x privateclient enable.

The no form command restores the default access control method.

Example

To configure the access control method based on port for Etherent1/0/4.

```
Switch(config-if-ethernet1/0/4)#dot1x port-method portbased
```

13.3.17 dot1x privateclient enable

Command	[no] dot1x privateclient enable
Parameter	none none
Default	Private 802.1x authentication packet format is disabled by default.
Mode	Global Mode
Usage Guide	To configure the switch to force the authentication client to use private 802.1xauthentication protocol. To implement integrated solution, the switch must be enabled to use private 802.1x protocol, or many applications will not be able to function. For detailed information, please refer to DCBI integrated solution. If the switch forces the authentication client to use private 802.1x protocol, the standard client will not be able to work. The no prefix will disable the command and allow the authentication client to use the standard 802.1x authentication protocol.
Example	To force the authentication client to use private 802.1x authentication protocol. Switch(config)#dot1x privateclient enable

13.3.18 dot1x privateclient protect enable

Command	[no] dot1x privateclient protect enable
Parameter	none none
Default	Disable the privateclient protect function by default.
Mode	Global Mode
Usage Guide	Enable the privateclient protect function of the switch. Support the partial encryption of the privateclient protocol to advance the security of the privateclient. The no command disables the protect function.
Example	Enable the privateclient protect function of the switch. Switch(config)#dot1x privateclient protect enable

13.3.19 dot1x re-authenticate

Command	dot1x re-authenticate [interface <interface-name>]
Parameter	interface-name stands for port number, omitting the parameter for all ports
Default	None
Mode	Global Mode
Usage Guide	Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.
Example	Enabling real-time re-authentication on port1/0/8. Switch(config)#dot1x re-authenticate interface ethernet 1/0/8

13.3.20 dot1x re-authentication

Command	[no] dot1x re-authentication
Parameter	none none
Default	Periodical re-authentication is disabled by default.
Mode	Global Mode
Usage Guide	Enables periodical supplicant authentication. When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval.This function is not recommended for common use. The no command disables this function.
Example	Enabling the periodical re-authentication for authenticated users. Switch(config)#dot1x re-authentication

13.3.21 dot1x timeout quiet-period

Command	dot1x timeout quiet-period <seconds> no dot1x timeout quiet-period	
Parameter	seconds	the silent time for the port in seconds, the valid range is 1 to 65535
Default	The default value is 10 seconds.	
Mode	Global Mode	
Usage Guide	Sets time to keep silent on supplicant authentication failure. Default value is recommended. The no command restores the default value.	
Example	Setting the silent time to 120 seconds. Switch(config)#dot1x timeout quiet-period 120	

13.3.22 dot1x timeout re-authperiod

Command	dot1x timeout re-authperiod <seconds> no dot1x timeout re-authperiod	
Parameter	seconds	the interval for re-authentication, in seconds, the valid range is 1 to 65535
Default	The default value is 3600 seconds.	
Mode	Global Mode	
Usage Guide	Sets the supplicant re-authentication interval. dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect. The no command restores the default setting.	
Example	Setting the re-authentication time to 1200 seconds. Switch(config)#dot1x timeout re-authperiod 1200	

13.3.23 dot1x timeout tx-period

Command	dot1x timeout tx-period <seconds> no dot1x timeout tx-period	
Parameter	seconds	the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535
Default	The default value is 30 seconds.	
Mode	Global Mode	
Usage Guide	Sets the interval for the supplicant to re-transmit EAP request/identity frame. Default value is recommended. The no command restores the default setting.	
Example	Setting the EAP request frame re-transmission interval to 1200 seconds. Switch(config)#dot1x timeout tx-period 1200	

13.3.24 dot1x unicast enable

Command	[no] dot1x unicast enable	
Parameter	none	none
Default	The 802.1x unicast passthrough function is not enabled in global mode.	
Mode	Global Mode	
Usage Guide	Enable the 802.1x unicast passthrough function of switch. The 802.1x unicast passthrough authentication for the switch must be enabled first to enable the 802.1x unicast passthrough function, then the 802.1x function is configured. The no operation of this command will disable this function.	
Example	Enabling the 802.1x unicast passthrough function of the switch and enable the 802.1x for port 1/0/1. Switch(config)#dot1x enable Switch(config)# dot1x unicast enable Switch(config)#interface ethernet1/0/1 Switch(Config-If-Ethernet1/0/1)#dot1x enable	

13.3.25 show dot1x

Command	show dot1x [interface <interface-list>]	
Parameter	interface-list	the port list,If no parameter is specified, information for all ports is displayed.
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.	

Example

Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
  reauth-enabled          no
  reauth-period          3600
  quiet-period           10
  tx-period              30
  max-req                 2
  authenticator mode     passive

Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
dot1x-privateclient Disable
dot1x-unicast Disable

802.1x is enabled on ethernet Ethernet1/0/1
Authentication Method:Port based
Max User Number:1
  Status               Authorized
  Port-control         Auto
  Supplicant           00-03-0F-FE-2E-D3

Authenticator State Machine
  State                Authenticated
Backend State Machine
  State                Idle
Reauthentication State Machine
  State                Stop
```

13.4 The Number Limitation Function of MAC and IP in Port, VLAN

13.4.1 ip arp dynamic maximum

Command	ip arp dynamic maximum <value> no ip arp dynamic maximum	
Parameter	value	upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP in the VLAN is disabled.	
Mode	VLAN Configuration Mode	
Usage Guide	Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN. When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted. The no command is used to disable the number limitation function of dynamic ARP in the VLAN.	
Example	Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50. Switch(config)#interface vlan1 Switch(config-if-vlan1)# ip arp dynamic maximum 50	

13.4.2 ipv6 nd dynamic maximum

Command	ipv6 nd dynamic maximum <value> no ipv6 nd dynamic maximum	
Parameter	value	upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096
Default	The number limitation function of dynamic NEIGHBOR in the VLAN is disabled.	
Mode	VLAN Configuration Mode	
Usage Guide	Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN. When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. The no command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.	
Example	Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50. Switch(config)#interface vlan1 Switch(config-if-vlan1)# ipv6 nd dynamic maximum 50	

13.4.3 show arp-dynamic count

Command

show arp-dynamic count {vlan | interface ethernet <portName>}

Parameter

vlan	the specified vlan ID
portName	the name of layer-2 port

Default

None.

Mode

Admin/Global Mode

Usage Guide

Display the number of dynamic ARP of corresponding port and VLAN.

Example

Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP.

```
Switch(config)# show arp-dynamic count interface ethernet 1/0/3
Port                    MaxCount                    CurrentCount
-------------------------------------------------------------------------------------------------
Ethernet1/0/3                 5                              1
-------------------------------------------------------------------------------------------------
Switch(config)# show arp-dynamic count vlan 1
Vlan                   MaxCount                     CurrentCount
-------------------------------------------------------------------------------------------------
1                        55                              15
-------------------------------------------------------------------------------------------------
```

13.4.4 show mac-address dynamic count

Command

show mac-address dynamic count { vlan | interface ethernet <portName>}

Parameter

vlan	display the specified VLAN ID
portName	the name of layer-2 port

Default

None.

Mode

Admin/Global Mode

Usage Guide

Display the number of dynamic MAC of corresponding port and VLAN.

Example

Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC.

```
Switch(config)# show mac-address dynamic count interface ethernet 1/0/3
Port                    MaxCount                   CurrentCount
----------------------------------------------------------------------------------------------------
Ethernet1/0/3                  5                              1
----------------------------------------------------------------------------------------------------
Switch(config)# show mac-address dynamic count vlan 1
Vlan                    MaxCount                   CurrentCount
----------------------------------------------------------------------------------------------------
1                          55                            15
----------------------------------------------------------------------------------------------------
```

13.4.5 show nd-dynamic count

Command

show nd-dynamic count { vlan | interface ethernet <portName>}

Parameter

vlan	display the specified VLAN ID
portName	the name of layer-2 port

Default

None.

Mode

Admin/Global Mode

Usage Guide

Display the number of dynamic ND of corresponding port and VLAN.

Example

Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND.

```
Switch(config)# show nd-dynamic dynamic count interface ethernet 1/0/3
Port                    MaxCount                    CurrentCount
-------------------------------------------------------------------------------------------------------
Ethernet1/0/3                  5                              1
-------------------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic dynamic count vlan 1
Vlan                    MaxCount                    CurrentCount
-------------------------------------------------------------------------------------------------------
1                         55                              15
-------------------------------------------------------------------------------------------------------
```

13.4.6 switchport arp dynamic maximum

Command	switchport arp dynamic maximum <value> no switchport arp dynamic maximum
Parameter	value — upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP on the port is disabled.
Mode	Port Mode
Usage Guide	Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port. When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function. The no command is used to disable the number limitation function of dynamic ARP on the port.
Example	Enable the number limitation function of dynamic ARP in port 1/0/2 mode, the max number to be set is 20. Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport arp dynamic maximum 20

13.4.7 switchport mac-address dynamic maximum

Command	switchport mac-address dynamic maximum <value> no switchport mac-address dynamic maximum
Parameter	value — upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic MAC address on the port is disabled.
Mode	Port Mode
Usage Guide	Set the max number of dynamic MAC address allowed by the port, and at the same time, enable the number limitation function of dynamic MAC address on the port. When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x,MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed. The no command is used to disable the number limitation function of dynamic MAC address on the port.
Example	Enable the number limitation function of dynamic MAC address in port 1/0/2 mode, the max number to be set is 20. Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport mac-address dynamic maximum 20

13.4.8 switchport mac-address violation

Command

```
switchport mac-address violation {protect | shutdown} [recovery <5-3600>]
no switchport mac-address violation
```

Parameter

protect	protect mode
shutdown	shutdown mode
recovery	Configure the border port to automatically restore after execute shutdown violation mode
<5-3600>	Recovery time, do not restore by default

Default

By default, the port is protected mode.

Mode

Port Mode

Usage Guide

Set the violation mode of the port.

The port sets the violation mode after enable the number limit function of MAC only. If the violation mode is protect, the port only disable the dynamic MAC address

learning function when the MAC address number of the port exceeds the upper limit of secure MAC. If the violation mode is shutdown, the port will be disabled when the MAC address number exceeds the upper limit of secure MAC, and the user can enable the port by configuring no shutdown command manually or the automatic recovery timeout.

The no command restores the violation mode to protect.

Example

Set the violation mode as shutdown, the recovery time as 60s for port1.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# switchport mac-address violation shutdown recovery 60
```

13.4.9 switchport nd dynamic maximum

Command	switchport nd dynamic maximum <value> no switchport nd dynamic maximum	
Parameter	value	upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096
Default	The number limitation function of dynamic ARP on the port is disabled.	
Mode	Port Mode	
Usage Guide	Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port. When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function. The no command is used to disable the number limitation function of dynamic NEIGHBOR on the port.	
Example	Enable the number limitation function of dynamic NEIGHBOR in port 1/0/2 mode, the max number to be 20. Switch(config)#interface ethernet 1/0/2 Switch(config-if-ethernet1/0/2)# switchport nd dynamic maximum 20	

13.4.10 vlan mac-address dynamic maximum

Command	vlan mac-address dynamic maximum <value> no vlan mac-address dynamic maximum
Parameter	value — upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096
Default	The number limitation function of dynamic MAC address in the VLAN is disabled.
Mode	VLAN Configuration Mode
Usage Guide	Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN. When configuring the max number of dynamic MAC allowed in the VLAN,if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted. The no command is used to disable the number limitation function of dynamic MAC address in the VLAN.
Example	Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50. Switch(config)#vlan1 Switch(config-if-vlan1)#vlan mac-address dynamic maximum 50

13.5 AM Configuration

13.5.1 am enable

Command	[no] am enable
Parameter	none none
Default	AM function is disabled by default.
Mode	Global Mode
Usage Guide	Globally enable/disable AM function. The no command disables AM function.
Example	Enable AM function on the switch. Switch(config)#am enable

13.5.2 am port

Command	[no] am port
Parameter	none none
Default	AM function is disabled on all port.
Mode	Port Mode
Usage Guide	Enable/disable AM function on port. The no command disables AM function on the port.
Example	Enable AM function on interface 1/0/3 of the switch. Switch(config-if-ethernet 1/0/3)#am port

13.5.3 am ip-pool

Command	[no] am ip-pool <ip-address> <num>	
Parameter	ip-adress	the starting address of an address segment in the IP address pool
	num	the number of consecutive addresses following ip-address, less than or equal with 32
Default	By default，IP address pool is empty.	
Mode	Port Mode	
Usage Guide	Set the AM IP segment of the interface, allow/deny the IP messages or APRmessages from a source IP within that segment to be forwarded via the interface. The no command delete configuration.	
Example	Configure that interface 1/0/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1. Switch(config-if-ethernet 1/0/3)#am ip-pool 10.10.10.1 10	

13.5.4 am mac-ip-pool

Command	[no] am mac-ip-pool <mac-address> <ip-address>	
Parameter	mac-address	the source MAC address
	ip-address	the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers
Default	By default，MAC-IP address pool is empty.	
Mode	Port Mode	
Usage Guide	Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface. The no command delete configuration.	
Example	Configure that the interface 1/0/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded. Switch(config-if-ethernet 1/0/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1	

13.5.5 no am all

Command	no am all [ip-pool | mac-ip-pool]	
Parameter	ip-pool	the IP address pool
	mac-ip-pool	the MAC-IP address pool
Default	By default，both address pools are empty at the beginning.	
Mode	Global Mode	
Usage Guide	Delete MAC-IP address pool or IP address pool or both pools configured by all users.	
Example	Delete all configured IP address pools. Switch(config)#no am all ip-pool	

13.5.6 show am

Command	show am [interface <interface-name>]	
Parameter	interface-name	the name of the interface of which the configuration information will be displayed
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Display the configured AM entries. No parameter means to display the AM configuration information of all interfaces.	
Example	Display all configured AM entries. Switch#show am interface ethernet 1/0/5 AM is enabled Interface Etherne1/0/5 am interface am ip-pool 50.10.10.1 30 am mac-ip-pool 00-02-04-06-08-09 20.10.10.5 am ip-pool 50.20.10.1 20	

13.6 Security Feature

13.6.1 dosattack-check srcip-equal-dstip enable

Command	[no] dosattack-check srcip-equal-dstip enable
Parameter	none none
Default	Disable the function by which the switch checks if the source IP address is equal to the destination IP address.
Mode	Global Mode
Usage Guide	Enable the function by which the switch checks if the source IP address is equal to the destination IP address. By enabling this function, data packet whose source IP address is equal to its destination address will be dropped. The "no" form of this command disables this function.
Example	Drop the data packet whose source IP address is equal to its destination address. Switch(config)# dosattack-check srcip-equal-dstip enable

13.6.2 dosattack-check tcp-flags enable

Command	[no] dosattack-check srcip-equal-dstip enable
Parameter	none none
Default	This function disable on the switch by default.
Mode	Global Mode
Usage Guide	Enable the function by which the switch will check the unauthorized TCP label function. With this function enabled, the switch will be able to drop follow four data packets

	containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command. The “no” form of this command will disable this function.
Example	Drop one or more types of above four packet types. Switch(config)# dosattack-check tcp-flags enable

13.6.3 dosattack-check srcport-equal-dstport enable

Command	[no] dosattack-check srcport-equal-dstport enable
Parameter	none none
Default	Disable the function by which the switch will check if the source port is equal to the destination port.
Mode	Global Mode
Usage Guide	Enable the function by which the switch will check if the source port is equal to the destination port. With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port. The no command disables this function.
Example	Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port. Switch(config)#dosattack-check srcport-equal-dstport enable

13.6.4 dosattack-check icmp-attacking enable

Command	[no] dosattack-check icmp-attacking enable	
Parameter	none	none
Default	By default，disable the ICMP fragment attack checking function on the switch.	
Mode	Global Mode	
Usage Guide	Enable the ICMP fragment attack checking function on the switch. With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value. The "no" form of this command disables this function.	
Example	Enable the ICMP fragment attack checking function. Switch(config)#dosattack-check icmp-attacking enable	

13.6.5 dosattack-check icmpV4-size

Command	dosattack-check icmpV4-size <64-1023>	
Parameter	<64-1023>	the max net length of the ICMPv4 data packet permitted by the switch
Default	The value is 0x200 by default.	
Mode	Global Mode	
Usage Guide	Configure the max net length of the ICMPv4 data packet permitted by the switch. To use this function you have to enable "dosattack-check icmp-attacking enable" first.	
Example	Set the max net length of the ICMPv4 data packet permitted by the switch to 100. Switch(config)#dosattack-check icmp-attacking enable Switch(config)#dosattack-check icmpV4-size 100	

13.7 ACACS+

13.7.1 tacacs-server authentication host

Command	tacacs-server authentication host <ip-address> [port <port-number>][timeout <seconds>] [key {0 | 7} <string>] [primary] no tacacs-server authentication host <ip-address>	
Parameter	ip-address	the IP address of the server
	port-number	the listening port number of the server, the valid range is 0~65535, amongst 0 indicates it will not be an authentication server
	seconds	the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60
	strin	the key string, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	indicates it's a primary server
Default	No TACACS+ authentication configured on the system by default.	
Mode	Global Mode	
Usage Guide	This command is for specifying the IP address, port number, timeout timer value and the key string of the TACACS+ server used on authenticating with the switch. The parameter port is for define an authentication port number which must be in accordance with the authentication port number of specified TACACS+ server which is 49 by default. The parameters key and timeout is used to configure the self-key and self-timeout, if the switch is not configure the timeout<seconds> and key<string>, it will use the global value and key by command tacacs-server timeout<seconds> and tacacs-server key <string>. This command can configure several TACACS+ servers communicate with the switch. The configuration sequence will be used as authentication server sequence. And in case primary is configured on one TACACS+ server, the server will be the primary server. The no form of this command deletes TACACS+ authentication server.	
Example	Configure the TACACS+ authentication server address to 192.168.1.2, and use the global configured key. Switch(config)#tacacs-server authentication host 192.168.1.2	

13.7.2 tacacs-server key

Command	tacacs-server key {0 | 7} <string> no tacacs-server key	
Parameter	string	the key string of the TACACS+ server. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters.
Default	None.	
Mode	Global Mode	
Usage Guide	Configure the key of TACACS+ authentication server. The key is used on encrypted packet communication between the switch and the TACACS+ server. The configured key must be in accordance with the one on the TACACS+ server or else no correct TACACS+ authentication will be performed. It is recommended to configure the authentication server key to ensure the data security. The no command deletes the TACACS+ server key.	
Example	Configure test as the TACACS+ server authentication key. Switch(config)#tacacs-server key 0 test	

13.7.3 tacacs-server nas-ipv4

Command	tacacs-server nas-ipv4 <ip-address> no tacacs-server nas-ipv4	
Parameter	ip-address	the source IP address of TACACS+ packet, in dotted decimal notation, it must be a valid unicast IP address
Default	By default，no specific source IP address for TACACS+ packet is configured, the IP address of the interface from which the TACACS+ packets are sent is used as source IP address of TACACS+ packet.	

Mode	Global Mode
Usage Guide	Configure the source IP address of TACACS+ packet sent by the switch. The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send TACACS+ packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from TACACS+ server are dropped when the interface link-down. The no command deletes the configuration.
Example	Configure the source ip address of TACACS+ packet as 192.168.2.254. Switch(config)#tacacs-server nas-ipv4 192.168.2.254

13.7.4 tacacs-server timeout

Command	tacacs-server timeout <seconds> no tacacs-server timeout	
Parameter	seconds	the value of TACACS+ authentication timeout timer, shown in seconds and the valid range is 1~60
Default	3 seconds by default.	
Mode	Global Mode	
Usage Guide	Configure a TACACS+ server authentication timeout timer. The command specifies the period the switch wait for the authentication through TACACS+ server. When connected to the TACACS+, and after sent the authentication query data packet to the TACACS+ server, the switch waits for the response. If no replay is received during specified period, the authentication is considered failed. The no command restores the default configuration.	
Example	Configure the timeout timer of the tacacs+ server to 30 seconds. Switch(config)#tacacs-server timeout 30	

13.8 RADIUS

13.8.1 aaa enable

Command	[no] aaa enable
Parameter	none none
Default	AAA authentication is not enabled by default.
Mode	Global Mode
Usage Guide	Enables the AAA authentication function in the switch. The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch. The no command disables the AAA authentication function.
Example	Enabling AAA function for the switch. Switch(config)#aaa enable

13.8.2 aaa-accounting enable

Command	[no] aaa-accounting enable
Parameter	none none
Default	AAA accounting is not enabled by default.
Mode	Global Mode
Usage Guide	Enables the AAA accounting function in the switch. When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an "accounting started" message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting

server every five seconds, and an "accounting stopped" message is sent to the RADIUS accounting server on accounting end.
Note: The switch send the "user offline" message to the RADIUS accounting server only when accounting is enabled, the "user offline"message will not be sent to the RADIUS authentication server.

The no command disables the AAA accounting function.

Example

Enabling AAA accounting for the switch.

```
Switch(config)#aaa-accounting enable
```

13.8.3 aaa-accounting update

Command

aaa-accounting update {enable | disable}

Parameter

none	none

Default

By default，Enable the AAA update accounting function.

Mode

Global Mode

Usage Guide

Enable or disable the AAA update accounting function.
After the update accounting function is enabled, the switch will sending accounting message to each online user on time.

Example

Disable the AAA update accounting function for switch.

```
Switch(config)#aaa-accounting update disable
```

13.8.4 radius nas-ipv4

Command	radius nas-ipv4 <ip-address> no radius nas-ipv4
Parameter	ip-address — the source IP address of the RADIUS packet, in dotted decimal notation, it must be a valid unicast IP address
Default	By default，No specific source IP address for RADIUS packet is configured, the IP address of the interface from which the RADIUS packets are sent is used as source IP address of RADIUS packet.
Mode	Global Mode
Usage Guide	Configure the source IP address for RADIUS packet sent by the switch. The source IP address must belongs to one of the IP interface of the switch, otherwise an failure message of binding IP address will be returned when the switch send RADIUS packet. We suggest using the IP address of loopback interface as source IP address, it avoids that the packets from RADIUS server are dropped when the interface link-down. The no command deletes the configuration.
Example	Configure the source ip address of RADIUS packet as 192.168.2.254. Switch(config)#radius nas-ipv4 192.168.2.254

13.8.5 radius nas-ipv6

Command	radius nas-ipv6 <ipv6-address> no radius nas-ipv6
Parameter	ipv6-address — the source IPv6 address of the RADIUS packet, it must be a valid unicast IPv6 address
Default	By default,No specific source IPv6 address for RADIUS packet is configured, the IPv6 address of the interface from which the RADIUS packets are sent is used as source IPv6 address of RADIUS packet.
Mode	Global Mode
Usage Guide	Configure the source IPv6 address for RADIUS packet sent by the switch. The source IPv6 address must belongs to one of the IPv6 interface of the switch, otherwise a failure message of binding IPv6 address will be returned when the switch send RADIUS packet. We suggest using the IPv6 address of loopback interface as source IPv6 address, it avoids that the packets from RADIUS server are dropped when the interface link-down. The no command deletes the configuration.
Example	Configure the source ipv6 address of RADIUS packet as 2001:da8:456::1. Switch(config)#radius nas-ipv6 2001:da8:456::1

13.8.6 radius-server accounting host

Command	radius-server accounting host {<ipv4-address> | <ipv6-address>} [port <port-number>] [key {0 | 7} <string>] [primary] no radius-server accounting host {<ipv4-address> | <ipv6-address>}	
Parameter	ipv4-address	stands for the server IPv4 address
	ipv6-address	stands for the server IPv6 address
	port-number	server listening port number from 0 to 65535
	string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
	primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first
Default	No RADIUS accounting server is configured by default.	
Mode	Global Mode	
Usage Guide	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server. This command is used to specify the IPv4/IPv6 address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The <port-number> parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting servers, and all the accounting servers can be backup servers for each other. If primary is specified, then the specified RADIUS server will be the primary server. It only configures a RADIUS primary server whether the server use IPv4 address or IPv6 address. The no command deletes the RADIUS accounting server.	
Example	Sets the RADIUS accounting server of IPv6 address to 2004:1:2:3::2, as the primary server, with the accounting port number as 3000. Switch(config)#radius-server accounting host 2004:1:2:3::2 port 3000 primary	

13.8.7 radius-server authentication host

Command

radius-server authentication host {<ipv4-address> | <ipv6-address>}[port <port-number>] [key {0 | 7} <string>] [primary] [access-mode {dot1x | telnet}]

no radius-server authentication host {<ipv4-address> | <ipv6-address>}

Parameter

ipv4-address	stands for the server IPv4 address
ipv6-address	stands for the server IPv6 address
port-number	server listening port number from 0 to 65535
string	the key string. If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
primary	for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if primary is not configured, otherwise, the specified RADIUS server will be used first
dot1x | telnet	designates the current RADIUS server only use 802.1x authentication or telnet authentication, all services can use current RADIUS server by default

Default

No RADIUS authentication server is configured by default.

Mode

Global Mode

Usage Guide

Specifies the IPv4 address or IPv6 address and listening port number, cipher key, whether be primary server or not and access mode for the RADIUS server.

This command is used to specify the IPv4 address or IPv6 address and port number, cipher key string and access mode of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. When the first server has responded (whether the authentication is successed or failed), switch does not send the authentication request to the next. If primary is specified, then the specified RADIUS server will be the primary server. It will use the cipher key which be configured by radius-server key <string> global command if the current RADIUS server not configure key<string>. Besides, it can designate the current RADIUS server only use 802.1x authentication or telnet authentication via access-mode option. It is not configure access-mode option and all services can use current RADIUS server by default.

The no command deletes the RADIUS authentication server.

Example	Setting the RADIUS authentication server address as 2004:1:2:3::2. Switch(config)#radius-server authentication host 2004:1:2:3::2

13.8.8 radius-server dead-time

Command	radius-server dead-time <minutes> no radius-server dead-time	
Parameter	minutes	the down -restore time for RADIUS server in minutes, the valid range is 1 to 255
Default	The default value is 5 minutes.	
Mode	Global Mode	
Usage Guide	This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid. The no command restores the default setting.	
Example	Setting the down-restore time for RADIUS server to 3 minutes. Switch(config)#radius-server dead-time 3	

13.8.9 radius-server key

Command	radius-server key {0 | 7} <string> no radius-server key	
Parameter	string	a key string for RADIUS server, If key option is set as 0, the key is not encrypted and its range should not exceed 64 characters, if key option is set as 7, the key is encrypted and its range should not exceed 64 characters
Default	None.	
Mode	Global Mode	
Usage Guide	Specifies the key for the RADIUS server (authentication and accounting). The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly. The no command deletes the key for RADIUS server.	
Example	Setting the RADIUS authentication key to be "test". Switch(config)#radius-server key 0 test	

13.8.10 radius-server retransmit

Command	radius-server retransmit <retries> no radius-server retransmit	
Parameter	retries	a retransmission times for RADIUS server, the valid range is 0 to 100
Default	The default value is 3 times.	
Mode	Global Mode	
Usage Guide	This command specifies the retransmission time for a packet without a RADIUS server	

	response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not work, the switch sets the server as invalid. The no command restores the default setting.
Example	Setting the RADIUS authentication packet retransmission time to five times. Switch(config)#radius-server retransmit 5

13.8.11 radius-server timeout

Command	radius-server timeout <seconds> no radius-server timeout	
Parameter	seconds	the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000
Default	The default value is 3 seconds.	
Mode	Global Mode	
Usage Guide	This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting time, the switch resends the request packet or sets the server as invalid according to the current conditions. The no command restores the default setting.	
Example	Setting the RADIUS authentication timeout timer value to 30 seconds. Switch(config)#radius-server timeout 30	

13.8.12 radius-server accounting-interim-update timeout

Command

radius-server accounting-interim-update timeout <seconds>
no radius-server accounting-interim-update timeout

Parameter

seconds	the interval of sending fee-counting update messages, in seconds, ranging from 60 to 3600

Default

The default interval of sending fee-counting update messages is 300 seconds.

Mode

Global Mode

Usage Guide

This command set the interval at which NAS sends fee-counting update messages. In order to realize the real time fee-counting of users, from the moment the user becomes online, NAS will send a fee-counting update message of this user to the RADIUS server at the configured interval.

The interval of sending fee-counting update messages is relative to the maximum number of users supported by NAS. The smaller the interval, the less the maximum number of the users supported by NAS; the bigger the interval, the more the maximum number of the users supported by NAS. The following is the recommended ratio of interval of sending fee-counting update messages to the maximum number of the users supported by NAS:

The maximum number of users	The interval of sending fee-counting update messages(in seconds)
1-299	300（default）
300-599	600
600-1199	1200
1200-1799	1800
≥1800	3600

The no operation of this command will reset to the default configuration.

Example

The maximum number of users supported by NAS is 700, the interval of sending fee-counting update messages 1200 seconds.

```
Switch(config)#radius-server accounting-interim-update timeout 1200
```

13.8.13 show aaa authenticated-user

Command	show aaa authenticated-user	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Displays the authenticated users online. Usually the administrator concerns only information about the online user, the other information displayed is used for troubleshooting by technical support.	
Example	Displays the authenticated users online. Switch(config)#show aaa authenticated-user -------------------------------------- authenticated users -- UserName Retry RadID Port EapID ChapID OnTime UserIP MAC -- -------------- total: 0 ---------------	

13.8.14 show aaa authenticating-user

Command	show aaa authenticating-user	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Display the authenticating users. Usually the administrator concerns only information about the authenticating user, the other information displays is used for troubleshooting by the technical support.	
Example	Display the authenticating users. Switch(config)#show aaa authenticating-user -------------------------------------- authenticating users --- User-name Retry-time Radius-ID Port Eap-ID Chap-ID Mem-Addr State -- -------------- total: 0 ---------------	

13.8.15 show aaa config

Command	show aaa config	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Displays whether aaa authentication, accounting are enabled and information for key, authentication and accounting server specified.	

Example

Display aaa configuration information.

```
Switch(config)#show aaa config
---------------- AAA config data ------------------
Is Aaa Enabled = 1                    :1 means AAA authentication is enabled, 0 means is
not enabled
Is Account Enabled= 1                 :1 means AAA account is enabled, 0 means is not
enabled
MD5 Server Key = yangshifeng      : Authentication key
authentication server sum = 2          :Configure the number of authentication server
........
```

13.8.16 show radius authenticated-user count

Command	show radius authenticated-user count	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Show the number of on-line users who have already passed the authentication.	

Example

Show the number of on-line users who have already passed the authentication.

```
Switch(config)#show radius authenticated-user count
The authenticated online user num is:   105
```

13.8.17 show radius authenticating-user count

Command	show radius authenticating-user count	
Parameter	none	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Show the number of the authenticating-user.	
Example	Show the number of the authenticating-user. Switch(config)#show radius authenticating-user count The authenticating user num is: 10	

13.8.18 show radius count

Command	show radius count {authenticated-user|authenticating-user} count	
Parameter	authenticated-user	displays the authenticated users online
	authenticating-user	displays the authenticating users
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	Displays the statistics for users of RADIUS authentication.	
Example	Displays the statistics for users of RADIUS authentication. Switch#show radius authenticated-user count The authenticated online user num is: 0	

13.9 IPv6 Security RA

13.9.1 ipv6 security-ra enable

Command	[no] ipv6 security-ra enable
Parameter	none none
Default	The IPv6 security RA function is disabled by default.
Mode	Global Mode
Usage Guide	Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. Only after enabling the global security RA function, the security RA on a port can be enabled. Globally disabling security RA will clear all the configured security RA ports. The global security RA function and the global IPv6 SAVI function are mutually exclusive, so they can not be enabled at the same time. The no operation of this command will globally disable IPv6 security RA function.
Example	Globally enable IPv6 security RA. Switch(config)#ipv6 security-ra enable

13.9.2 ipv6 security-ra enable

Command	[no] ipv6 security-ra enable
Parameter	none none
Default	The IPv6 security RA function is disabled by default.
Mode	Port Configuration Mode
Usage Guide	Enable IPv6 security RA on a port, causing this port not to forward the received RA message. Only after globally enabling the security RA function, can the security RA on a port be

	enabled. Globally disabling security RA will clear all the configured security RA ports. The no ipv6 security-ra enable will disable the IPv6 security RA on a port.
Example	Enable IPv6 security RA on a port. Switch(config-if-ethernet1/0/2)#ipv6 security-ra enable

13.9.3 show ipv6 security-ra

Command	show ipv6 security-ra [interface <interface-list>]
Parameter	interface-list Specifies the port number. No parameter will display all distrust ports, entering a parameter will display the corresponding distrust port.
Default	None.
Mode	Admin/Global Mode
Usage Guide	Display all the interfaces with IPv6 RA function enabled.
Example	Display all the interfaces with IPv6 RA function enabled. Switch# show ipv6 security-ra IPv6 security ra config and state information in the switch Global IPv6 Security RA State: Enable Ethernet1/0/1 IPv6 Security RA State: Yes Ethernet1/0/3 IPv6 Security RA State: Yes

13.10 MAB

13.10.1 authentication mab

Command

```
authentication mab {radius|local} (none)
no authentication mab
```

Parameter

radius	means RADIUS authentication mode
local	means the local authentication
none	means the authentication is needless

Default

By default，using RADIUS authentication mode.

Mode

Global Mode

Usage Guide

Configure the authentication mode and priority of MAC address authentication.
none option is used to the fleeing function of MAC address authentication.
If all configured RADIUS servers don't respond, switch will adopt none authentication mode to allow that MAC address authentication users access the network directly. The option of local is used for the local authentication of MAC address, it authenticates through the local user name and password. If configured as the method of authentication mab radius local none, judge if configured the user name and password used in mab authentication in local when the radius server has no response. If it has been configured, use the local authentication, if not, use the backup none authentication.

The no command restores the default authentication mode.

Example

Configure the local authentication and the fleeing function of MAC address authentication.

```
Switch(config)#authentication mab radius local none
```

13.10.2 clear mac-authentication-bypass binding

Command	clear mac-authentication-bypass binding {mac WORD | interface (ethernet IFNAME | IFNAME) | all}	
Parameter	mac	Delete MAB binding of the specified MAC address
	IFNAME	Delete MAB binding of the specified port
	all	Delete all MAB binding
Default	None.	
Mode	Admin Mode	
Usage Guide	Clear MAB binding information.	
Example	Delete all MAB binding. Switch#clear mac-authentication-bypass binding all	

13.10.3 mac-authentication-bypass binding-limit

Command	mac-authentication-bypass binding-limit <1-100> no mac-authentication-bypass binding-limit	
Parameter	1-100	the max binding number of MAB, ranging from 1 to 100
Default	By default，the max binding number of MAB is 3.	
Mode	Port Configuration Mode	
Usage Guide	Set the max binding number of MAB. Set the max binding number of MAB. When the binding number reaches to the max value, the port will stop binding, if the max binding number is less than the current binding number of the port, the setting will be unsuccessful. The no command will restore the default binding number as 3.	
Example	Configure the max binding number as 10. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass binding-limit 10	

13.10.4 mac-authentication-bypass enable

Command	[no] mac-authentication-bypass enable
Parameter	none none
Default	By default，disable the global and port MAB function.
Mode	Port Configuration Mode
Usage Guide	Enable the global and port MAB function. To process MAB authentication of a port, enable the global MAB function first, and then, enable the MAB function of the corresponding port. The no command disables MAB function.
Example	Enable the global and port Eth1/0/1 MAB function. Switch(config)#mac-authentication-bypass enable Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass enable

13.10.5 mac-authentication-bypass guest-vlan

Command	mac-authentication-bypass guest-vlan <1-4094> no mac-authentication-bypass guest-vlan
Parameter	1-4094 guest vlan ID, ranging from 1 to 4094
Default	None.
Mode	Port Configuration Mode
Usage Guide	Set guest vlan of MAB authentication. Set guest vlan of MAB authentication, only Hybrid port use this command, it is not take effect on access port. After MAB authentication is failing, if the existent guest vlan is configured by the port connecting to the MAB user, the MAB user can join and access guest vlan. The no command deletes guest vlan.
Example	Configure guest vlan of MAB authentication for port 1/0/1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#mac-authentication-bypass guest-vlan 10

13.10.6 mac-authentication-bypass spoofing-garp-check

Command	[no] mac-authentication-bypass spoofing-garp-check	
Parameter	none	none
Default	By default，disable spoofing-garp-check function.	
Mode	Global Mode	
Usage Guide	Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more When the terminal of Windows operating system detects the address conflict, it will sends a gratuitous ARP to correct the error ARP entries generated by gratuitous ARP of the conflict detection. This command is used to detect the spoofing-garp when occuring the address conflict, MAB function is not deal with the packet any more. Notice: when enabling the check function, all ARP will be processed the software check, it will add switch’s load. The no command disables the function.	
Example	Enable spoofing-garp-check function. Switch(config)#mac-authentication-bypass spoofing-garp-check enable	

13.10.7 mac-authentication-bypass timeout linkup-period

Command	mac-authentication-bypass timeout linkup-period <0-30> no mac-authentication-bypass timeout linkup-period	
Parameter	0-30	After the port is shutdown automatically, the interval before it up again, the unit is second, 0 means there is no down/up operation
Default	By default，the interval is 0.	
Mode	Global Mode	

Usage Guide	Set the interval between down and up when VLAN binding in a port is changing to assure the user can obtain IP again. When MAB authentication is successful, belong to vlan according to auto-vlan setting, when MAB authentication is failing, belong to vlan according to guest-vlan setting. After linkup-period is set, when VLAN binding of a port is changing, the port will be shutdown automatically, and will be up again after linkup-period to assure the client obtain IP. The no command to restore default values.
Example	Configure down/up time as 12s. Switch(config)#mac-authentication-bypass timeout linkup-period 12

13.10.8 mac-authentication-bypass timeout offline-detect

Command	mac-authentication-bypass timeout offline-detect (0 | <60-7200>) no mac-authentication-bypass timeout offline-detect	
Parameter	0 | <60-7200>	offline-detect time, the range is 0 or 60 to 7200s
Default	By default，offline-detect time is 180s.	
Mode	Global Mode	
Usage Guide	Configure offline-detect time. When offline-detect time is 0, the switch does not detect MAB binding, when offline-detect time is 60s to 7200s, the switch timely detects the flow corresponding to the MAB binding. If there is no flow in the period of offline-detect time, it will delete this binding and forbid the flow to pass. The no command restores the default value.	
Example	Configure offline-detect time as 200s. Switch(config)#mac-authentication-bypass timeout offline-detect 200	

13.10.9 mac-authentication-bypass timeout quiet-period

Command	mac-authentication-bypass timeout quiet-period <1-60> no mac-authentication-bypass timeout quiet-period	
Parameter	1-60	quiet-period, ranging from 1 to 60s
Default	By default，quiet-period is 30s.	
Mode	Global Mode	
Usage Guide	Set quiet-period of MAB authentication. If MAB authentication is failing, within the quiet-period the switch will not respond the authentication request of this MAC, after quiet-period, it will respond the request again. The no command restores quiet-period as the default value.	
Example	Configure quiet-period of MAB authentication as 60s. Switch(config)#mac-authentication-bypass timeout quiet-period 60	

13.10.10 mac-authentication-bypass timeout reauth-period

Command	mac-authentication-bypass timeout reauth-period <1-3600> no mac-authentication-bypass timeout reauth-period	
Parameter	1-3600	reauthentication interval, ranging from 1 to 3600s
Default	By default，reauthentication interval is 30s.	
Mode	Global Mode	
Usage Guide	Set the reauthentication interval at failing authentication state. At failing authentication state, the user processes the reauthentication timely until the authentication is successful; at the successful state, the user can access the network resources. The no command restores the default value.	

Example	Configure reauthentication time as 20s. Switch(config)#mac-authentication-bypass timeout reauth-period 20

13.10.11 mac-authentication-bypass timeout stale-period

Command	mac-authentication-bypass timeout stale-period <0-60> no mac-authentication-bypass timeout stale-period
Parameter	0-60 The time that delete the binding, ranging from 0 to 60s
Default	By default, it takes 30 s. to delete the binding.
Mode	Global Mode
Usage Guide	Set the time that delete the binding user after MAB port is down. If the time that delete the binding as 0, delete all user binding of this port as soon as the MAB port is down, if the time is bigger than 0, delete the user binding with a delay after the MAB port is down. The no command restores the default value.
Example	Configure the deletion time as 40s. Switch(config)#mac-authentication-bypass timeout stale-period 40

13.10.12 mac-authentication-bypass username-format

Command	[no] mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}	
Parameter	mac-address	Use MAC address of MAB user as username and password to authenticate
	fixed username WORD password WORD	Use the specified username and password to authenticate, the length of username and password ranges between 1 and 32 characters
Default	By default，use MAC address of MAB user as username and password to authenticate.	
Mode	Global Mode	
Usage Guide	Set the authenticate method of MAB authentication. There are two methods for MAB authentication: use MAC address of MAB user as username and password to authenticate or use the specified username and password to authenticate. If there is no specified username and password, the device uses the first method to authenticate by default. The no command to restore default values.	
Example	All MAB users use the same username and password to authenticate, the username is mab-user, the password is mab-pwd. Switch(config)#mac-authentication-bypass username-format fixed username mab-user password mab-pwd	

13.10.13 show mac-authentication-bypass

Command	show mac-authentication-bypass {interface {ethernet IFNAME | IFNAME)|}
Parameter	IFNAME Port name
Default	None.
Mode	Admin/Global Mode
Usage Guide	Show the binding information of MAB authentication.
Example	Show the binding information of MAB authentication.

```
Switch#show mac-authentication-bypass
The Number of all binding is 5
MAC                 Interface      Vlan ID                  State
------------------------------------------------------------------------------------------------------
04-0a-eb-6a-7f-88       Ethernet1/0/1      1                    MAB_QUIET
03-0a-eb-6a-7f-88       Ethernet1/0/1      1                    MAB_QUIET
02-0a-eb-6a-7f-88       Ethernet1/0/1      1               MAB_AUTHENTICATED
00-0a-eb-6a-7f-8e       Ethernet1/0/1      1               MAB_AUTHENTICATED
Switch(config)#show mac-authentication-bypass int e1/0/1
Interface Ethernet1/0/1 user config:
MAB enable: Enable
Binding info: 1
------------------------------------------------------------
MAB Binding built at SUN JAN 01 01:14:48 2006
      VID 1, Port: Ethernet1/1
      Client MAC: 00-0a-eb-6a-7f-8e
      Binding State: MAB_AUTHENTICATED
      Binding State Lease: 164 seconds left
```

13.11 MAB PPPoE Intermediate Agent

13.11.1 pppoe intermediate-agent

Command	[no] pppoe intermediate-agent
Parameter	none none
Default	By default, disable global PPPoE intermediate agent function.
Mode	Global Mode
Usage Guide	Enable global PPPoE intermediate agent function. After enable global PPPoE IA function, process the packet of PPPoE discovery stage according to the related configuration. The no command disables global PPPoE intermediate agent function.
Example	Enable global PPPoE intermediate agent function. Switch(config)#pppoe intermediate agent

13.11.2 pppoe intermediate-agent (Port)

Command	[no] pppoe intermediate-agent
Parameter	none none
Default	By default，disable PPPoE intermediate agent function of the port.
Mode	Port Configuration Mode
Usage Guide	Enable PPPoE intermediate agent function of the port. After enable PPPoE IA function of the port, add vendor tag for PPPoE packet of the port. Note: 1. It must enable global pppoe intermediate-agent function. 2. At least one port is connected to PPPoE server, and the port mode is trust.

	The no command disables PPPoE intermediate agent function of the port.
Example	Enable PPPoE intermediate agent function of the port ethernet 1/0/2. Switch(config-if-ethernet1/0/2)#pppoe intermediate agent

13.11.3 pppoe intermediate-agent circuit-id

Command	[no] pppoe intermediate-agent circuit-id <string>
Parameter	string circuit-id, the max character number is 63 bytes
Default	This function is not configured by default.
Mode	Port Configuration Mode
Usage Guide	Configure circuit ID of the port. This command configures circuit-id alone for each port, the priority is higher than pppoe intermediate-agent identifier-string command. The no command cancels this configuration.
Example	Configure circuit-id as abcd/efgh on port ethernet1/0/3 of vlan3. Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id abcd/efgh

13.11.4 pppoe intermediate-agent delimiter

Command

pppoe intermediate-agent delimiter <WORD>
no pppoe intermediate-agent delimiter

Parameter

WORD	the delimiter, its range is (#|.|,|;|:|/|space)

Default

By default，the fields is comparted with ’\0’.

Mode

Global Mode

Usage Guide

Configure the delimiter among the fields in circuit-id and remote-id.
After configuring the delimiter, the added fields of circuit-id and remote-id use the configured delimiter to compart.
Notice: The global pppoe intermediate-agent
function must be enabled.

The no command cancels the configuration.

Example

Configuration delimiter is space.

```
Switch(config)#pppoe intermediate-agent delimiter space
```

13.11.5 pppoe intermediate-agent format

Command

pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii)
no pppoe intermediate-agent format (circuit-id | remote-id)

Parameter

hex	hexadecimal
ascii	ASCII code

Default

This function is not configured by default.

Mode

Global Mode

Usage Guide

Configure the format with hex or ASCII for circuit-id and remote-id.
Encapsulation circuit-id and remote-id with hex ASCII format to vendor tag.
Notice: The global pppoe intermediate-agent function must be enabled.

	The no command cancels the configuration.
Example	Configure the trust port 1/0/1 to enable vendor-tag strip function. Switch(config)#pppoe intermediate-agent format remote-id ascii

13.11.6 pppoe intermediate-agent remote-id

Command	[no] pppoe intermediate-agent remote-id <string>
Parameter	string remote-id, the max character number is 63 bytes
Default	This function is not configured by default.
Mode	Port Configuration Mode
Usage Guide	Configure remote-id of the port. Configure remote-id for each port, if there is no configuration, use switch's MAC as remote-id value. The no command cancels this configuration.
Example	Configure remote-id as abcd on port ethernet1/0/2. Switch(config-if-ethernet1/0/2)# pppoe intermediate-agent remote-id abcd

13.11.7 pppoe intermediate-agent trust

Command

[no] pppoe intermediate-agent trust

Parameter

none	none

Default

By default, the port is a untrust port.

Mode

Port Configuration Mode

Usage Guide

Configure the port as trust port.

The port which connect to server must be configured as trust port.

Note: At least one trust port is connected to PPPoE server.

The no command configures the port as untrust port.

Example

Configure port ethernet1/0/1 as trust port.

```
Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust
```

13.11.8 pppoe intermediate-agent type self-defined circuit-id

Command

pppoe intermediate-agent type self-defined circuit-id {vlan | port | id (switch-id (mac | hostname) | remote-mac) | string WORD}

no pppoe intermediate-agent type self-defined circuit-id

Parameter

vlan	VLAN ID
port	port number
id switch-id mac	the local MAC address
id switch-id hostname	the local host name
remote-mac	the remote MAC address
string WORD	the specified keyword

Default

By default，this configuration is null.

Mode

Global Mode

Usage Guide

Configure the self-defined circuit-id.

This configuration and type tr-101 circuit-id are mutually exclusive, it will clear the corresponding configuration of type tr-101 circuit-id.

The no command cancels the configuration.

Example

Configure the self-defined circuit-id as vlan port id switch-id hostname.

```
Switch(config)#pppoe intermediate-agent type self-defined circuit-id vlan port id switch-id hostname
```

13.11.9 pppoe intermediate-agent type self-defined remoteid

Command

pppoe intermediate-agent type self-defined remoteid {mac | vlan-mac | hostname | string WORD}

no pppoe intermediate-agent type self-defined remote-id

Parameter

mac	Ethernet port MAC address
vlan-mac	IP interface MAC address
hostname	the local host name
string WORD	the specified keyword

Default

By default, this configuration is empty.

Mode

Global Mode

Usage Guide

Configure the self-defined remote-id.

Configuration order of this command according to the fields order in remote-id.

The no command cancels the configuration.

Example

Configure the self-defined remote-id as string abcd mac hostname.

```
Switch(config)#pppoe intermediate-agent type self-defined remoteid string abcd mac hostname
```

13.11.10 pppoe intermediate-agent type tr-101 circuit-id access-node-id

Command

```
pppoe intermediate-agent type tr-101 circuit-id access-node-id <string>
no pppoe intermediate-agent type tr-101 circuit-id access-node-id
```

Parameter

string	access-node-id, the max character number is 47 bytes.

Default

By default，MAC address of the switch.

Mode

Global Mode

Usage Guide

Configure access-node-id field value of circuit ID in the added vendor tag with tr-101 standard.
Use this configuration to create access-node-id of circuit ID in vendor tag.circuit-id value is access-node-id +” eth “+ Slot ID + delimiter + Port Index + delimiter + Vlan ID, access-node-id occupies n bytes (n<48), “ eth “ is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte. In default state, access-node-id value of circuit-id is switch’s MAC, it occupies 6 bytes. For example: MAC address is “0a0b0c0d0e0f”, Slot ID is 12, Port Index is 34, Vlan ID is 567, the default circuit-id value is “0a0b0c0d0e0f eth 12/034:0567”.

The no command unconfigured.

Example

Configure access-node-id value of circuit ID as abcd in vendor tag.

```
Switch(config)#pppoe intermediate-agent access-node-id abcd
```

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is ”abcd eth 01/003:0003”.

13.11.11 pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Command

pppoe intermediate-agent type tr-101 circuit-id identifier-string <string> option {sp | sv | pv | spv} delimiter <WORD> [delimiter <WORD>]

no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter

Parameter

string	identifier-string, the max character number is 47 bytes
{sp | sv | pv | spv}	This option can select the combination format for slot, port, vlan, sp means slot and port, sv means slot and vlan, pv means port and vlan, spv means slot, port and vlan
WORD	The delimiter between slot, port and vlan, the range is (# | . | , | ; | : | / | space). Note: There are two delimiter WORDs in spv combo mode, the first between slot and port, the second between port and vlan

Default

By default, this configuration is empty.

Mode

Global Mode

Usage Guide

Configure circuit-id of the added vendor tag with tr-101 standard.

This command is used to configure global circuit id, the priority is higher than pppoe intermediate-agent access-node-id command. circuit-id value is access-node-id +" eth "+ Slot ID + delimiter + Port Index + delimiter + Vlan ID,

access-node-id occupies n bytes (n<48), " eth " is space + e + t + h + space, it occupies 5 bytes, Slot ID occupies 2 bytes, Port Index occupies 3 bytes, Vlan ID occupies 4 bytes, delimiter occupies 1 byte.

The no command deletes this configuration.

Example

Configure access-node-id as xyz, use spv combination mode, delimiter with"#"between Slot ID and Port ID, delimiter with "/"between Port ID and Vlan ID.

```
Switch(config)#pppoe intermediate-agent identifier-string xyz option spv delimiter #
delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : xyz
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/ "
```

After port ethernet1/0/3 of vlan3 receives PPPoE packets, circuit-id value of the added vendor tag is "xyz eth 01#003/0003".

13.11.12 pppoe intermediate-agent vendor-tag strip

Command	[no] pppoe intermediate-agent vendor-tag strip
Parameter	none none
Default	By default，disable vendor-tag strip function of the port.
Mode	Port Configuration Mode
Usage Guide	Enable vendor-tag strip function of the port. If the received packet includes vendor tag from server to client, strip this vendor tag. Note: 1. Must enable global pppoe intermediate-agent function. 2. It must be configured on trust port. The no command cancels this function.
Example	Trust port ethernet1/0/1 enables vendor tag strip function. Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

show pppoe intermediate-agent access-node-id

Command	show pppoe intermediate-agent access-node-id
Parameter	none none
Default	By default,the configuration information is null.
Mode	Admin mode
Usage Guide	This command is used to show access-node-id configured by user.

Example

Show access-node-id configuration information.

```
Switch#pppoe intermediate-agent access-node-id abcd
Switch#show pppoe intermediate-agent access-node-id
pppoe intermediate-agent access-node-id is : abcd
```

13.11.13 show pppoe intermediate-agent identifier-string option delimiter

Command

show pppoe intermediate-agent identifier-string option delimiter

Parameter

none	none

Default

By default,the configuration information is null.

Mode

Admin mode

Usage Guide

Show the configured identifier-string, the combo format and delimiter of slot, port and vlan.

Example

Show the configuration information for pppoe intermediate-agent identifier-string.

```
Switch#pppoe intermediate-agent identifier-string abcd option spv delimiter # delimiter /
Switch# show pppoe intermediate-agent identifier-string option delimiter
config identifier string is : abcd
config option is : slot , port and vlan
the first delimiter is : "# "
the second delimiter is : "/ "
```

13.11.14 show pppoe intermediate-agent info

Command

show pppoe intermediate-agent info [interface ethernet <interface-name>]

Parameter

interface-name	port name

Default

By default,the configuration information is null.

Mode

Admin mode

Usage Guide

Show the related PPPoE IA configuration information of all ports or the specified port. Check the configuration information of the corresponding port, show whether the port is trust port, strip function is enabled, rate limit is enabled, show the configured circuit ID and remote ID.

Example

Show pppoe intermediate-agent configuration information of port ethernet1/0/2.

```
Switch# show pppoe intermediate-agent info interface ethernet 1/0/2
Interface      IA    Trusted   vendor Strip   Rate limit    circuit id      remote id
----------     ------   ------     -----------      -------       ---------       ----------
Ethernet1/0/2    yes      no          no            no        test1/port1     host1
```

13.12 VLAN-ACL

13.12.1 clear vacl statistic vlan

Command	clear vacl [in | out] statistic vlan [<1-4094>]	
Parameter	in | out	Clear the traffic statistic of the ingress/egress
	1-4094	The VLAN which needs to clear the VACL statistic information. If do not input VLAN ID, then clear all VLAN statistic information
Default	None.	
Mode	Admin mode	
Usage Guide	This command can clear the statistic information of VACL.	
Example	Clear VACL statistic information of Vlan1. Switch#clear vacl statistic vlan 1	

13.12.2 show vacl vlan

Command	show vacl [in | out] vlan [<1-4094>] | [begin | include | exclude <regular-expression>]	
Parameter	in | out	Show ingress/egress configuration and statistic
	1-4094	The VLAN which needs to show the configuration and the statistic information of VACL. If do not input VLAN ID, then show VACL configuration and statistic information of all VLANs.
	begin | include | exclude <regular-expression>	the regular expression . match any characters except the line feed character ^ match the beginning of the row $ match the end of the row | match the character string at the left or right of upright line [0-9] match the number 0 to the number 9 z] match the lowercase a to z [aeiou] match any letter in "aeiou" \ Escape Character is used to match the intervocalic character, for example, \$ will match the $ character, but it is not match the

		end of the character string \w match the letter, the number or the underline \b match the beginning or the end of the words \W match any characters which are not alphabet letter, number and underline \B match the locations which are not the begin or end of the word [^x] match any characters except x [^aeiou] match any characters except including aeiou letters * repeat zero time or many times + repeat one time or many times (n) repeat n times (n，) repeat n or more times (n，m) repeat n to m times At present, the regular expression used does not support the following syntaxes: \s match the blank character \d match the number \S match any characters except blank character \D match non-number character ？ repeat zero time or one time
Default	None.	
Mode	Admin Mode	
Usage Guide	This command shows the configuration and the statistic information of VACL.	
Example	Show vlan2 VACL statistics. Switch (config)#show vacl vlan 2 Vlan 2: IP Ingress access-list used is 100, traffic-statistics Disable.	

13.12.3 vacl ip access-group

Command

```
vacl ip access-group {<1-299> | WORD} {in | out} [traffic-statistic] vlan WORD
no vacl ip access-group {<1-299> | WORD} {in | out} vlan WORD
```

Parameter

<1-299> | WORD	Configure the numeric IP ACL (include: standard ACL rule <1-99>, extended ACL rule <100-299>) or the named ACL.
in | out	Filter the ingress/egress traffic
traffic-statistic	Enable the statistic of matched packets number
vlan WORD	The VLAN will be bound to VACL

Default

None

Mode

Global Mode

Usage Guide

This command configure VACL of IP type on the specific VLAN.
Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and
CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch.

The no command unconfigured.

Example

Configure the numeric IP ACL and enable the statistic function for Vlan 1-5,6,7-9.

```
Switch(config)#vacl ip access-group 1 in traffic-statistic vlan 1-5; 6; 7-9
```

13.12.4 vacl ipv6 access-group

Command

```
vacl ipv6 access-group (<500-699> | WORD) {in } (traffic-statistic|) vlan WORD
no ipv6 access-group {<500-699> | WORD} {in } vlan WORD
```

Parameter

<500-699> | WORD	Configure the IPv6 numeric standard ACL or IPV6 standard ACL rule.
in | out	Filter inlet/ outlet flow
traffic-statistic	Enable the statistic of matched packets number
vlan WORD	The VLAN will be bound to VACL.

Default

None.

Mode

Global Mode

Usage Guide	This command configure VACL of IPv6 on the specific VLAN. Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering and extended IPv6 is not supported by switch. The no command unconfigured.
Example	Configure the numeric IPv6 ACL for Vlan 5. Switch(config)#vacl ipv6 access-group 600 in traffic-statistic vlan 5

13.12.5 vacl mac access-group

Command	vacl mac access-group {<700-1199> | WORD} {in } [traffic-statistic] vlan WORD no vacl mac access-group {<700-1199> | WORD} {in } vlan WORD	
Parameter	<700-1199> | WORD	Configure the numeric IP ACL (include: <700-799> MAC standard access list, <1100-1199> MAC extended access list) or the named ACL
	in	Filter the ingress traffic
	traffic-statistic	Enable the statistic of matched packets number
	vlan WORD	The VLAN will be bound to VACL
Default	None.	
Mode	Global Mode	
Usage Guide	This command configure VACL of MAC type on the specific VLAN. Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch. The no command unconfigured.	
Example	Configure the numeric MAC ACL for Vlan 1-5 Switch(config)#vacl mac access-group 700 in traffic-statistic vlan 1-5	

13.12.6 vacl mac-ip access-group

Command	vacl mac-ip access-group {<3100-3299> | WORD} {in } [traffic-statistic] vlan WORD

	no vacl mac-ip access-group {<3100-3299> | WORD} {in } vlan WORD
Parameter	<3100-3299> | WORD: Configure the numeric MAC-IP ACL or the named ACL in: Filter the ingress traffic traffic-statistic: Enable the statistic of matched packets number vlan WORD: The VLAN will be bound to VACL.
Default	None.
Mode	Global mode
Usage Guide	This command configure VACL of MAC-IP type on the specific VLAN. Use ";" or "-" to input the VLAN or multi-VLANs, but do not exceed 128, and CLI length cannot exceed 80 characters. Egress direction filtering is not supported by switch. The no command unconfigured.
Example	Configure the numeric MAC-IP ACL for Vlan 1, 2, 5. Switch(config)#vacl mac-ip access-group 3100 in traffic-statistic vlan 1;2;5

13.13 SAVI

13.13.1 ipv6 cps prefix

Command	ipv6 cps prefix <ipv6-address> vlan <vid> no ipv6 cps prefix<ipv6-address>	
Parameter	ipv6-address	the address prefix of link, like 2001::/64
	vid	vlan ID of the current link
Default	None.	
Mode	Global Mode	
Usage Guide	Configure IPv6 address prefix of the link manually. Users should configure local address prefix: fe80::/64 of the link before enable the function of matching address prefix of the link, it accepts the packets of which source addresses are the local addresses of the link. The no command deletes IPv6 address prefix.	
Example	Configure IPv6 address prefix of the link manually is 2001::/64。 Switch(config)#ipv6 cps prefix 2001::/64	

13.13.2 ipv6 cps prefix check enable

Command	[no] ipv6 cps prefix check enable	
Parameter	none	none
Default	By default,disable SAVI address prefix check function.	
Mode	Global Mode	
Usage Guide	Enable SAVI address prefix check function. After enable the prefix check function, if the IPv6 address prefix of the packets does not	

	accord with the link prefix, then do not establish the corresponding IPv6 address binding. If users enable the matched address prefix of the link, configure the local address prefix of fe80::/64 first to accept the packets with the source address as local link address. Disable address prefix check function by default. The no command will disable this function.
Example	Enable SAVI address prefix check function. Switch(config)#ipv6 cps prefix check enable

13.13.3 ipv6 dhcp snooping trust

Command	[no] ipv6 dhcp snooping trust
Parameter	none none
Default	By default, this function is disabled.
Mode	Port Mode
Usage Guide	Configure the port as dhcpv6 trust port, it does not establish dynamic DHCPv6 binding again and allows all DHCPv6 protocol packets to pass. Set the port as dhcpv6 trust attribute, enable uplink port of the switch with SAVI function for connecting dhcpv6 server or dhcpv6 relay generally. no command deletes the port trust function.
Example	Set ethernet1/0/1 to be DHCP trust port. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust

13.13.4 ipv6 nd snooping trust

Command	[no] ipv6 nd snooping trust
Parameter	none none
Default	By default, this function is disabled.
Mode	Port Mode
Usage Guide	Configure the port as slaac trust and RA trust port, this port will not establish dynamic slaac binding anymore and forwards RA packets. If the port disables ipv6 nd snooping trust function, it is considered to untrust RA packets port and discards all RA packets. Setting the port as trust attribute, enable the uplink port of the switch with SAVI or the conjoint port between switches with SAVI generally. The no command deletes the port trust function.
Example	Set the port ethernet1/0/1 to be nd trust port. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)#ipv6 nd snooping trust

savi check binding

Command	savi check binding <simple | probe> mode no savi check binding mode	
Parameter	simple	only check the port state for conflict binding, if the state is up,keep the conflict binding and do not set new binding. If the state is down, delete the conflict binding to set a new one
	probe	besides checking the port state for conflict binding, it will send NS packets to probe the usability of the corresponding user when the port state is up. If receiving the responded NA packets from users, it will keep the current conflict binding and does not set new binding, otherwise delete the conflict binding to set new one
Default	Disable the conflict binding check mode by default. It will adopt the mode that	

	delete the conflict binding directly to set new one.
Mode	Global Mode
Usage Guide	Configure the check mode for conflict binding. It is recommended to configure probe mode to prevent the attack that the spurious address conflict binding deletes the legal user binding. The no command deletes the check mode.
Example	Configure the conflict binding check mode to probe mode. Switch(config)#savi check binding probe mode

13.13.5 savi enable

Command	[no] savi enable
Parameter	none none
Default	By default,disable the global SAVI function.
Mode	Global Mode
Usage Guide	Enable the global SAVI function. Command configuration can be processed for SAVI function after enabling the global SAVI function. Because SAVI function has already contained security RA function, global SAVI function and security RA function are mutually exclusive in the global mode. The no command disables this global function.
Example	Enable SAVI function. Switch(config)#savi enable

13.13.6 savi ipv6 binding num

Command	savi ipv6 binding num <limit-num> no savi ipv6 binding num
Parameter	limit-num set the range from 0 to 65535
Default	The default value of the port binding number is 65535.
Mode	Port Mode
Usage Guide	Configure the number of the corresponding binding with the port. The configured binding number only include the dynamic binding type of slaac, dhcp. If the binding sum exceeds the configured number, this port does not create new dynamic binding any more, if the configured number is 0, this port does not create any dynamic binding. The no command restores the default value.
Example	Configure the binding number to be 100 for port ethernet1/0/1. Switch(config)#interface ethernet1/0/1 Switch(config-if-ethernet1/0/1)# savi ipv6 binding num 100

13.13.7 savi ipv6 check source binding

Command

```
savi ipv6 check source binding ip <ip-address> mac <mac-address> interface <if-name>
{type [slaac | dhcp] lifetime <lifetime> | type static}
no savi ipv6 check source binding ip <ip-address> interface <if-name>
```

Parameter

ip-address	the unicast IPv6 address, including local link and global unicast address
mac-address	the mac address of Ethernet
if-name	the port name, like interface ethernet 1/0/1
slaac | dhcp	slaac means create the dynamic binding for slaac type, dhcp means create the dynamic binding for dhcp type
lifetime	configure the lifetime period for the dynamic binding, the unit is second
static	create the binding of the static type

Default

None.

Mode

Global Mode

Usage Guide

Configure the static or dynamic binding function manually。

After the dynamic binding configured by handwork is overtime, the corresponding binding will be deleted but the configuration is still be kept, so the binding still be shown. If the binding needs to take effect again, it should delete it first and configure a new binding again.
When the binding type is static type, do not configure lifetime period, the lifetime period is infinite.

The no command deletes the configured binding.

Example

Configure the dynamic binding of slaac type for SAVI manually.

```
Switch(config)#savi ipv6 check source binding ip 2001::10 mac 00-25-64-BB-8F-04
Interface ethernet1/0/1 type slaac lifetime 2010
```

Configure the static binding for SAVI manually.

```
Switch(config)#savi ipv6 check source binding ip 2001::20 mac 00-25-64-BB-8F-04
Interface ethernet1/0/1 type static
```

13.13.8 savi ipv6 check source ip-address mac-address

Command

savi ipv6 check source [ip-address mac-address | ip-address | mac-address]
no savi ipv6 check source

Parameter

none	none

Default

By default,disable the control filtering function of the port.

Mode

Port Mode

Usage Guide

Enable the control authentication function for the packets of the port.
The global SAVI function must be enabled before configuring this command.

The no command disables this function.

Example

Enable the control filtering function of the packets on port ethernet1/0/1.

```
Switch(config)#interface ethernet1/0/1
Switch(config-if-ethernet1/0/1)# savi ipv6 check source ip-address mac-address
```

13.13.9 savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Command

[no] savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable

Parameter

dhcp-only	dhcp-only application scene
slaac-only	slaac-only application scene
dhcp-slaac	combination application scene of dhcp-only and slaac-only

Default

By default,disable SAVI application scene.

Mode

Global Mode

Usage Guide

Enable SAVI application scene function.
dhcp-only application scene only detects DHCPv6 packets and DAD NS packets of link-local ipv6 address to be IPv6 address with target field, it does not detect DAD NS packets of non-link-local address. slaac-only application scene detects DAD

	NSpackets of all types. dhcp-slaac combination application scene detects all DHCPv6 and DAD NS packets. Disable all kinds of application scene detection function for SAVI by default. The no command disables the function.
Example	Enable the specified dhcp-only application scene for SAVI. Switch(config)#savi ipv6 dhcp-only enable

13.13.10 savi ipv6 mac-binding-limit

Command	savi ipv6 mac-binding-limit <limit-num> no savi ipv6 mac-binding-limit	
Parameter	limit-num	set the ranging from 1 to 10, the default dynamic binding number is 32 for the same MAC address
Default	The default dynamic binding number is 32 for the same MAC address.	
Mode	Global Mode	
Usage Guide	Configure the dynamic binding number of the same MAC address. This command is used to prevent the exhaust attack of the dynamic binding entry for SAVI. The no command restores the default value.	
Example	Set the dynamic binding number to be 5 for the same MAC address. Switch(config)#isavi ipv6 mac-binding-limit 5	

13.13.11 savi max-dad-dalay

Command	savi max-dad-delay <max-dad-delay> no savi max-dad-delay
Parameter	max-dad-delay set the ranging between 1 and 65535 seconds, its default value is 1 second
Default	Its default value is 1 second.
Mode	Global Mode
Usage Guide	Configure the dynamic binding at DETECTION state and send lifetime period of DAD NS packet detection. It is recommended to use the default value. The no command restores the default value.
Example	Set the detection lifetime as 2 seconds. Switch(config)#savi max-dad-delay 2

13.13.12 savi max-dad-prepare-delay

Command	savi max-dad-prepare-delay <max-dad-prepare-delay> no savi max-dad-prepare-delay
Parameter	max-dad-prepare-delay set the ranging between 1 and 65535 seconds, its default value is 1 second
Default	Its default value is 1 second.
Mode	Global Mode
Usage Guide	Configure lifetime period of redetection for the dynamic binding. It is recommended to user the default value. The no command restores the default value.
Example	Set the redetection lifetime as 2 seconds. Switch(config)#savi max-dad-prepare-delay 2

13.13.13 savi max-slaac-life

Command	savi max-slaac-life <max-slaac-life> no savi max-slaac-life	
Parameter	max-slaac-life	set the ranging between 1 and 31536000 seconds, its default value is 4 hours
Default	Its default value is 4 hours.	
Mode	Global Mode	
Usage Guide	Configure lifetime period of slaac dynamic binding at BOUND state. The no command restores the default value.	
Example	Configure lifetime period of slaac binding type as 2010 seconds at BOUND state. Switch(config)#savi max-slaac-life 2000	

13.13.14 savi timeout bind-protect

Command	savi timeout bind-protect <protect-time> no savi timeout bind-protect	
Parameter	protect-time	set the ranging between 1 and 300 seconds, its default value is 30 seconds
Default	Its default value is 30 seconds.	
Mode	Global Mode	
Usage Guide	Configure the bind-protect lifetime period for a port after its state from up to down. After the configured lifetime period is overtime, the port is still at down state, the binding of this port will be deleted. If the port state is changed from down to up state during the configured lifetime period, the binding of the port will reset it as lifetime period	

of BOUND state. If the configured parameter is 0 second, all binding of the port will be deleted immediately.

The no command restores the default value.

Example

Set bind-protect lifetime period to be 20 seconds.

```
Switch(config)#savi timeout bind-protect 20
```

13.13.15 show savi ipv6 check source binding

Command

show savi ipv6 check source binding [interface<if-name>]

Parameter

if-name	port name such as interface ethernet 1/0/1

Default

None.

Mode

Admin Mode

Usage Guide

Show the global SAVI binding entry list.

Example

Show the global binding state of SAVI.

```
Switch(config)#show savi ipv6 check source binding
Static binding count: 0
Dynamic binding count: 3
Binding count: 3

MAC                       IP              VLAN      Port          Type     State       Expires
------------------------------------------------------------------------------------------------------------------
00-25-64-bb-8f-04    fe80::225:64ff:febb:8f04   1     Ethernet1/0/5    slaac    BOUND    14370
00-25-64-bb-8f-04    2001::13:1                  1     Ethernet1/0/5    slaac    BOUND    14370
00-25-64-bb-8f-04    2001::10:1                  1     Ethernet1/0/5    slaac    BOUND    14370
------------------------------------------------------------------------------------------------------------------
```

Chapter 14 Reliability

14.1 MRPP

14.1.1 control-vlan

Command	**control-vlan <*vid*>** **no control-vlan**	
parameter	***vid***	expresses control VLAN ID, the valid range is from 1 to 4094
default	-	
Mode	MRPP ring mode	
Usage Guide	The command specifies Virtual VLAN ID of MRPP ring, currently it can be any value in 1-4094. To avoid confusion, it is recommended that the ID is non-configured VLAN ID, and the same to MRPP ring ID. In configuration of MRPP ring of the same MRPP loop switches, the control VLAN ID must be the same, otherwise the whole MRPP loop may not be able to work normally or form broadcast. The mrpp enable command must be start before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, the mrpp-ring function is enabled.	
Example	Configure control VLAN of mrpp ring 4000 is 4000. Switch(config)#mrpp ring 4000 Switch(mrpp-ring-4000)#control-vlan 4000	

14.1.2 clear mrpp statistics

Command	**clear mrpp statistics [<*ring-id*>]**	
parameter	***ring-id***	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it clears all of MRPP ring statistic information.
default	-	
Mode	Admin Mode.	

Usage Guide

Clears statistics for MRPP packets received and transmitted by the MRPP loop.

Example

Clear switch MRP P ring 4000 statistics.

```
Switch#clear mrpp statistics 4000
```

14.1.3 enable

Command

enable

no enable

parameter

-

default

Default disable MRPP ring

Mode

MRPP ring mode

Usage Guide

This command is used to enable the configured MRPP ring ," no enable" command disables this enabled MRPP ring.

Example

Configure MRPP ring 4000 of switch to primary node, and enable the MRPP ring.

```
Switch(config)#mrpp enable
Switch(config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)# node-mode master
Switch(mrpp-ring-4000)#fail-timer 18
Switch(mrpp-ring-4000)#hello-timer 6
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(config)#in ethernet1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config)#in ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port
```

14.1.4 errp domain

Command	**errp domain <*domain-id*>** **no errp domain <*domain-id*>**	
parameter	***domain-id***	domain ID of ERRP, the range between 1 and 15.
default	Default Unconfigured ID	
Mode	Global mode	
Usage Guide	If domain ID of ERRP needs to be configured, the compatible mode of ERRP should be enabled firstly. When executing this command, it should create a new ERRP domain if there is no ERRP domain. However, the no command is used to delete the corresponding domain ID of ERRP.	
Example	Configure domain ID for ERRP globally. Switch(Config)#errp domain 1	

14.1.5 fail-timer

Command	**fail-timer <*timer*>** **no fail-timer**	
parameter	***timer***	valid range is from 1 to 300s.
default	Default configure timer interval 3s	
Mode	MRPP ring mode	
Usage Guide	If primary node of MRPP ring doesn't receives Hello packet from primary port of primary node on configured fail timer, the whole loop is fail. Transfer node of MRPP doesn't need this timer and configure. To avoid time delay by transfer node forwards Hello packet, the value of fail timer must be more than or equal to 3 times of Hello timer. On time delay loop, it needs to modify the default and increase the value to avoid primary node doesn't receive Hello packet on fail timer due to time delay.	
Example	Configure fail timer of MRPP ring 4000 to 10s. Switch(config)# mrpp ring 4000 Switch(mrpp-ring-4000)#fail-timer 10	

14.1.6 hello-timer

Command

hello-timer <*timer*>
no hello-timer

parameter

timer	valid range is from 1 to 100s.

default

Default configuration timer interval is 1s.

Mode

MRPP ring mode

Usage Guide

The primary node of MRPP ring continuously sends Hello packet on configured Hello timer interval, if secondary port of primary node can receive this packet in configured period; the whole loop is normal, otherwise fail. Transfer node of MRPP ring doesn't need this timer and configure.

Example

Configure hello-timer of MRPP ring 4000 to 3 seconds.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#hello-timer 3
```

14.1.7 mrpp eaps compatible

Command

mrpp eaps compatible
no mrpp eaps compatible

parameter

-

default

Disable the compatible function of EAPS

Mode

Global mode

Usage Guide

If the compatible function of EAPS needs to be configured, MRPP protocol should be enabled firstly. When executing no mrpp eaps compatible command, it should ensure that the switch has enabled MRPP protocol.

Example

Enable the compatible function of EAPS globally

```
Switch(Config)#mrpp enable
Switch(Config)#mrpp eaps compatible
```

14.1.8 mrpp enable

Command	**mrpp enable** **no mrpp enable**
parameter	-
default	The system doesn't enable MRPP protocol module
Mode	Global Mode
Usage Guide	If it needs to configure MRPP ring, it enables MRPP protocol. Executing "no mrpp enable" command, it ensures to disable the switch enabled MRPP ring.
Example	Globally enable MRPP. Switch(config)#mrpp enable

14.1.9 mrpp errp compatible

Command	**mrpp errp compatible** **no mrpp errp compatible**
parameter	-
default	Disable the compatible function of ERRP.
Mode	Global mode
Usage Guide	If the compatible function of ERRP needs to be configured, MRPP protocol should be enabled firstly. Furthermore, the port with ERRP compatible mode should be configured as hybrid or trunk mode and allow the packets with Control Vlan information.
Example	Enable the compatible function of ERRP globally. Switch(Config)#mrpp enable Switch(Config)#mrpp errp compatible Switch(Config)#mrpp ring 2 Switch(mrpp-ring-2)#control-vlan 4000 Switch(config-if-ethernet1/51)#switchport mode hybrid Switch(config-if-ethernet1/51)#switchport hybrid allowed vlan 4000 tag Switch(config-if-ethernet1/52)#switchport mode hybrid Switch(config-if-ethernet1/52)#switchport hybrid allowed vlan 4000 tag

14.1.10 mrpp poll-time

Command	**mrpp poll-time <20-2000>**
parameter	**<20-2000>** Enquiry Time, Unit: ms
default	Default configuration ms 100
Mode	Global mode.
Usage Guide	Configure the query time to adjust the query interval of MRPP, the default interval is 100ms.
Example	Set the query time as 200ms. Switch(Config)# mrpp poll-time 200

14.1.11 mrpp ring

Command	**mrpp ring <*ring-id*>** **no mrpp ring <*ring-id*>**
parameter	***ring-id*** is MRPP ring ID, the valid range is from 1 to 4096
default	Default does not configure ring id
Mode	Global mode
Usage Guide	If this MRPP ring doesn't exist it create new MRPP ring when executing the command, and then it enter MRPP ring mode. It needs to ensure disable this MRPP ring when executing the "no mrpp ring" command.
Example	Create a mrpp ring 100. Switch(config)#mrpp ring 100

14.1.12 mrpp ring primary-port

Command	**mrpp ring <*ring-id*> primary-port {cos <cos>|}**

no mrpp ring <*ring-id*> primary-port

parameter

ring-id	is the ID of MRPP ring; range is <1-4096>.
cos <cos>	is the cos value in the packet head; range is <0-7>

default

There is no configuration and the cos value is 0 as default.

Mode

Port mode

Usage Guide

The command specifies MRPP ring primary port. Primary node uses primary port to send Hello packet, secondary port is used to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

Example

Configure the primary of MRPP ring 4000 to Ethernet 1/0/1

```
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
```

14.1.13 mrpp ring secondary-port

Command

mrpp ring < *ring-id* > secondary-port {cos <cos>|}
no mrpp ring < *ring-id* > secondary-port

parameter

ring-id	is the ID of MRPP ring; range is <1-4096>.
cos <cos>	is the cos value in the packet head; range is <0-7>.

default

There is no configuration and the cos value is 0 as default

Mode

Port mode

Usage Guide

The command specifies secondary port of MRPP ring. The primary node uses secondary port to receive Hello packet from primary node. There are no difference on function between primary port and secondary of secondary node.

The mrpp enable command must be enabled before the control-vlan command be used. If primary port, secondary port, node-mode and enable commands all be configured after control-vlan, then the mrpp-ring function is enabled.

Example

Configure secondary port of MRPP ring to 1/0/3.

```
Switch(config)#interface ethernet1/0/3
Switch(Config-If-Ethernet1/0/3)#mrpp ring 4000 secondary-port
```

14.1.14 node-mode

Command

node-mode {maser | transit}

parameter

-

default

Default the node mode is secondary node.

Mode

MRPP ring mode

Usage Guide

This command configures the node type as the primary or secondary node.

Example

Configure the switch to primary node. MRPP ring 4000.

```
Switch(config)# mrpp ring 4000
Switch(mrpp-ring-4000)#node-mode master
```

14.1.15 show mrpp

Command

show mrpp [<*ring-id*>]

parameter

ring-id	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it display all of MRPP ring configuration.

default

-

Mode

Admin and Configuration Mode

Usage Guide

This command is used to view the MRPP ring configuration.

Example

Display configuration of MRPP ring 4000 of switch

```
Switch# show mrpp 4000
```

14.1.16 show mrpp statistics

Command

show mrpp statistics [<*ring-id*>]

parameter	***ring-id***	is MRPP ring ID, the valid range is from 1 to 4096, if not specified ID, it displays all of MRPP ring statistic information.

default

-

Mode

Admin and Configuration Mode.

Usage Guide

This command is used to display the statistics of the MRPP loop receiving and transmitting packets.

Example

Display statistic information of MRPP ring 4000 of switch.

```
Switch# show mrpp statistic 4000
```

14.2 ULPP

14.2.1 clear ulpp flush counter interface

Command	**clear ulpp flush counter interface <*name*>**	
parameter	***name***	is the name of the port
default	-	
Mode	Admin mode	
Usage Guide	Clear the statistics of the packets.	
Example	Clear the statistic information of the flush packets for the port1/0/1 Switch#clear ulpp flush counter interface e1/0/1	

14.2.2 control vlan

Command	**control vlan <*integer*>** **no control vlan**	
parameter	***integer***	is the control VLAN ID that sends the flush packets, range from 1 to 4094.
default	The default is VLAN 1	
Mode	ULPP group configuration mode.	
Usage Guide	Configure the control VLAN of ULPP group. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted. It must belong to the VLAN protected by ULPP group to avoid flush packets loopback.	
Example	Configure the sending control VLAN of ULPP group as 10. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# control vlan 10	

14.2.3 description

Command	**description <*string*>** **no description**	
parameter	***string***	is the name of ULPP group, the max number of the characters is 128.
default	Do not configure ULPP name by default.	
Mode	ULPP group configuration mode.	
Usage Guide	Configure the description string for the ULPP group. Delete description no command.	
Example	Configure the description of ULPP group as switch. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# description switch	

14.2.4 flush {enable |disable} arp

Command	**flush {enable|disable} arp**
parameter	-
default	By default, enable the sending function of the flush packets which are deleted by ARP.
Mode	ULPP group configuration mode.
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the entries of ARP.
Example	Disable sending the flush packets of deleting ARP. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable arp

14.2.5 flush {enable |disable} mac

Command	**flush {enable|disable}mac**
parameter	-
default	By default, enable sending the flush packets of updating MAC address.
Mode	ULPP group configuration mode.
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to update the MAC address table.
Example	Disable sending the flush packets of updating MAC address. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# flush disable mac

14.2.6 flush {enable |disable} mac-vlan

Command	**flush {enable|disable}mac-vlan**
parameter	-
default	Disable.
Mode	ULPP group configuration mode
Usage Guide	If configure this command, when the link is switched, it will not actively send the flush packets to notify the upstream device to delete the dynamic unicast mac according to vlan.
Example	Disable sending the flush packets deleted by mac-vlan. Switch(config)#ulpp group 1 Switch(ulpp-group-1)#flush disable mac-vlan

14.2.7 preemption delay

Command	**preemption delay <*integer*>** **no preemption delay**	
parameter	***integer***	the preemption delay, range from 1 to 600, in second.
default	The default preemption delay is 30.	
Mode	ULPP group configuration mode.	
Usage Guide	The preemption delay is the delay time before the master port is preempted as the forwarding state, for avoiding the link oscillation in a short time. After the preemption mode is enabled, the preemption delay takes effect.	
Example	Configure the preemption delay as 50s for ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption delay 50	

14.2.8 preemption mode

Command	**preemption mode** **no preemption mode**
parameter	-
default	Do not preempt.
Mode	ULPP group configuration mode.
Usage Guide	If the preemption mode configured by ULPP group, and the slave port is in forwarding state, and the master port is in the standby state, the master port will turn into the forwarding state and the slave port turn into the standby state after the preemption delay.
Example	Configure the preemption mode of ULPP group. Switch(config)# ulpp group 20 Switch(ulpp-group-20)# preemption mode

14.2.9 protect vlan-reference-instance

Command

protect vlan-reference-instance <*instance-list*>

no protect vlan-reference-instance <*instance-list*>

parameter

instance-list	is MSTP instance list, such as: i; j-k. The number of the instances is not limited in the list.

default

Do not protect any VLANs by default that means any instances are not quoted.

Mode

ULPP group configuration mode.

Usage Guide

Quote the instances of MSTP to protect the VLANs. The VLAN corresponds to this instance is at the forwarding state on one port of this group, and at the blocked state on another port of this group. Each ULPP group can quotes all instances of MSTP. And it can quotes the inexistent MSTP instances that means any VLANs are not protected, the different ULPP groups can't quote the same instance.

Example

Configure the protective VLAN quoted from instance 1 for ULPP group.

```
Switch(config)# ulpp group 20
Switch(ulpp-group-20)# protect vlan-reference-instance 1
```

14.2.10 show ulpp flush counter interface

Command

show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}

parameter

IFNAME	is the name of the ports.

default

-

Mode

Admin mode.

Usage Guide

Show the statistic information of the flush packets, such as: the information of the flush packets number which has been received, the time information that receive the flush packets finally.

Example

Show the statistic information of the flush packets for ULPP group1.

```
Switch# show ulpp flush counter interface e1/0/1
Received flush packets: 10
```

14.2.11 show ulpp flush-receive-port

Command **show ulpp flush-receive-port**

parameter -

default -

Mode Admin mode.

Usage Guide displays the port that receives the flush packet, flush type, and control VLAN.

Example Show the information that the port receives flush packets.

```
Switch# show ulpp flush-receive-port
ULPP flush-receive portlist:
Portname Type Control Vlan
-----------------------------------------------
Ethernet1/0/1 ARP 1
Ethernet1/0/3 MAC 1;3;5-10
```

14.2.12 show ulpp group

Command **show ulpp group [group-id]**

parameter **group-id** Show the information of the specific ULPP group

default By default, show the information of all ULPP groups which have been configured

Mode Admin mode.

Usage Guide Show the configuration information of ULPP groups which have been configured, such as: the state of the master port and the slave port, the preemption mode, the preemption delay, etc.

Example Show the configuration information of ULPP group1.

```
Switch# show ulpp group 1
ULPP flush-receive portlist:
Portname            Type                    Control Vlan
---------------------------------------------------
---------------------------------------------------
Switch#show ulpp group 20
```

```
ULPP group 20 information:
Description: switch
Preemption mode: ON
Preemption delay: 50s
Control VLAN: 10
Flush packet: NONE
Protected VLAN: Reference Instance 1
Member              Role          State          Track-cfm-level
---------------------------------------------------------------
---------------------------------------------------------------
```

14.2.13 ulpp control vlan

Command

ulpp control vlan <*vlan-list*>

no ulpp control vlan <*vlan-list*>

parameter

vlan-list	specify the control VLAN list that receives the flush packets, such as: i; j-k. The number of VLANs in Each character string cannot exceed 100. The receiving control VLAN of the port can be added.

default

The default is VLAN 1.

Mode

Port mode

Usage Guide

Configure the receiving control VLAN for the port. This VLAN must correspond the existent VLAN, after it is configured, this VLAN can't be deleted.

Example

Configure the receiving control VLAN as 10

```
Switch(config)# interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10
```

14.2.14 ulpp flush {enable|disable} arp

Command	**ulpp flush {|enable|disable} arp**
parameter	-
default	By default, disable receiving the flush packets of deleting ARP
Mode	Port mode.
Usage Guide	If this command is configured, then it will not receive the flush packets of deleting ARP.
Example	Disable receiving the flush packets of deleting ARP. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable arp

14.2.15 ulpp flush {enable|disable} mac

Command	**ulpp flush {enable|disable} mac**
parameter	-
default	By default, disable receiving the flush packets of updating MAC address.
Mode	Port mode.
Usage Guide	If this command is configured, then it will not receive the flush packets of updating MAC address.
Example	Disable receiving the flush packets of updating MAC address. Switch(config)# interface ethernet 1/0/1 Switch(config-If-Ethernet1/0/1)# ulpp flush disable mac

14.2.16 ulpp flush {enable|disable} mac-vlan

Command	**ulpp flush {enable|disable} mac-vlan**
parameter	-
default	Disable
Mode	Port mode.
Usage Guide	If enabling this function, forward the hardware of the flush packets with mac-vlan type received in port. It will not be analyzed.
Example	Disable receiving the flush packets deleted by mac-vlan of port. Switch(config)#interface e1/0/2 Switch(config-if-ethernet1/0/2)#ulpp flush disable mac-vlan

14.2.17 ulpp group

Command	**ulpp group <*integer*>** **no ulpp group <*integer*>**
parameter	***integer*** is the ID of ULPP group, range from 1 to 48.
default	Any ULPP groups are not configured.
Mode	Global Mode.
Usage Guide	Create a ULPP group. If the group exists, enter the configuration mode of the ULPP group. no command delete ULPP group.
Example	Configure ulpp group 20 or enter the mode of ulpp group 20. Switch(config)# ulpp group 20 Switch(ulpp-group-20)#

14.2.18 ulpp group {master|slave}

Command

14.3 ulpp group <*integer*> {master|slave}

14.4 no ulpp group <*integer*> {master|slave}

parameter

integer	is the ID of ULPP group, range from 1 to 48.

default

There is no master port configured by default.

Mode

Port mode

Usage Guide

There is no sequence requirement for the master and slave port configuration in a group, but the protective VLANs must be configured before the member ports. Each group has only one master port, if the master port exists, then the configuration fail.

Example

Configure the master port of ULPP group.

```
Switch(config)# interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 20 slave
```

14.5 ULSM

14.5.1 show ulsm group

Command	**show ulsm group [group-id]**	
parameter	**group-id**	the ID of ULSM group.
default	By default, show the information of all ULSM groups which have been configured	
Mode	Admin Mode	
Usage Guide	This command is used to display configuration information for ULSM groups.	
Example	Show the configuration information of ULSM group1. Switch# show ulsm group 1	

14.5.2 ulsm group

Command	**ulsm group <*group-id*>** **no ulsm group <*group-id*>**	
parameter	***group-id***	is the ID of ULSM group, range from 1 to 32.
default	There is no ULSM group configured by default.	
Mode	Global Mode.	
Usage Guide	This command is used to create a ULSM group. no command delete ULSM group.	
Example	Create ULSM group 10. Switch(config)# ulsm group 10	

14.5.3 ulsm group {uplink | downlink}

Command

ulsm group <*group-id*> {uplink | downlink}

no ulsm group <*group-id*>

parameter

group-id	The ID of ULSM group, the range from 1 to 32.
uplink	Configure the port as the uplink port
downlink	Configure the port as the downlink port.

default

The port does not belong to any ULSM group

Mode

Port Mode

Usage Guide

Configure the uplink/downlink ports of ULSM group. Each ULSM group can configure 8 uplink ports and 16 downlink ports at most。

Example

Configure port1/0/3 as the uplink port of ULSM group10.

```
Switch(config)# interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)# ulsm group 10 uplink
```

Chapter 15 Mirroring Configuration

15.1 Mirroring Configuration

15.1.1 monitor session source interface

Command

monitor session <*session*> source {interface <*interface-list*> | cpu} {rx| tx| both}

no monitor session <*session*> source {interface <*interface-list*> | cpu}

parameter

session	is the session number for the mirror. Currently only 1 is supported
interface-list	is the list of source interfaces of the mirror which can be separated by "-" and ";".
cpu	means the CPU on the board to be the source of the mirror for debugging. Datagram received by or sent by the CPU
rx	means to filter the datagram received by the interface
tx	for the datagram sent out
both	means both of income and outcome datagram

default

Default does not match any mirror source port

Mode

Global mode

Usage Guide

This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. Both of the income and outcome datagram can be mirrored, or they can be mirrored selectively. If no [rx | tx | both] is specified, both are made to be the default. When multiple interfaces are mirrored, the direction of the mirror can be different, but they should be configured separately.

Example

Configure to mirror the datagram sent out by interface 1/0/1-4 and to mirror the datagram received by interface1/0/5。

```
Switch(config)#monitor session 1 source interface ethernet 1/0/1-4 tx
Switch(config)#monitor session 1 source interface ethernet1/0/5 rx
```

15.1.2 monitor session source interface access-list

Command

monitor session <*session*> source {interface <*interface-list*>} access-list <*num*> {rx|tx|both}

no monitor session <*session*> source {interface <*interface-list*>} access-list <*num*>

parameter

session	is the session number for the mirror. Currently only 1 is supported
interface-list	is the list of source interfaces of the mirror which can be separated by '-' and ';'
num	is the number of the access list
rx	means to filter the datagram received by the interface
tx	for the datagram sent out
both	means both of income and outcome datagram

default

Default not configured

Mode

Global Mode

Usage Guide

This command is used to configure the source interfaces for the mirror. It is not restricted the source interface of the mirror on the switch. The source can be one interface, or can be multiple interfaces. For flow mirror, only datagram received can be mirrored. The parameters can be rx, tx, both. The related access list should be prepared before this command is issued. For how to configure the access list, please refer to ACL configuration. The mirror can only be created after the destination interface of the corresponding session has been configured. In the moment, the command only IP ACL and MAC ACL

Example

Configure the mirror interface 1/0/6 to filter with access list 120 in session 1.

```
Switch(config)#monitor session 1 source interface 1/0/6 access-list 120 rx
```

15.1.3 monitor session destination interface

Command

monitor session <*session*> destination interface <*interface-number*>

no monitor session <*session*> destination interface <*interface-number*>

parameter

session	is the session number of the mirror, which is currently limited to 1-4
interface-number	is the destination interface of the mirror.

default Default does not match mirror destination port

Mode Global mode

Usage Guide

Only four destination mirror interface is supported on the switch. To be mentioned. The interface which is configured as the destination of the mirror should not be configured as the member of the interface trunk. And the maximum throughput of the interface is recommended to be larger than the total throughput of the interfaces to be mirrored. If the destination is removed, the mirror path configured will be removed at the same time. And if the destination interface is reconfigured, the interface, CPU mirror pathwill be recovered. To be mentioned, the flow mirror can only be recovered after the destination of the interface is re-configured.

Example

Configure interface 1/0/7 as the destination of the mirror.

```
Switch(config)#monitor session 1 destination interface ethernet 1/0/7
```

15.1.4 show monitor

Command **show monitor**

parameter -

default -

Mode Admin Mode

Usage Guide

This command is used to display the source and destination ports for the configured mirror sessions. For port mirroring, CPU mirroring, and flow mirroring, the mirror mode of the source can be displayed.

Example

View configuration information for the current image.

```
Switch#show monitor
```

15.1.5 mirror sample rate

Command

monitor session <*session*> sample rate <num>

no monitor session <*session*> sample rate

parameter

session	is mirror session value, and it supports 1 to 4 at moment
num	is sampled value, and ranges from 0 to 65535

default

Default Unconfigured Sampling Rate

Mode

Global Mode

Usage Guide

It represents how many packets mirror to destination port and it ranges from 0 to 65535, such as, when rate value equals 100, the first, 101, 201 packets can mirror destination port, when rate value equal 0, it does not configure samping rate, the default is notconfigured samping rate.

Example

The sampling rate for configuring mirror session 1 is 100.

```
switch(config)#monitor session 1 sample rate 100
```

15.2 sFlow

15.2.1 sflow agent-address

Command	**sflow agent-address <*agent-address*>** **no sflow agent-address**
parameter	***agent-address*** is the sample proxy IP address which is shown in dotted decimal notation
default	None default value
Mode	Global Mode
Usage Guide	For configuring sflow proxy address,The proxy address is used to mark the sample proxy which is similar to OSPF or the Router ID in the BGP. However it is not necessary to make the sFlow sample proxy work properly.
Example	Sample the proxy address at global mode. switch (config)#sflow agent-address 192.168.1.200

15.2.2 sflow analyzer

Command	**sflow analyzer sflowtrend** **no sflow analyzer sflowtrend**
parameter	-
default	Do not configure
Mode	Global Mode
Usage Guide	This command is used to configure sFlow analyzer, no the command disables the analyzer,Configure this command when using sFlowTrend.
Example	Enable sFlow analyzer. Switch(config)#sflow analyzer sflowtrend

15.2.3 sflow counter-interval

Command	**sflow counter-interval <*interval-value*>**

	no sflow counter-interval	
parameter	***interval-value***	is the value of the interval with a valid range of 20~120 and shown in second.
default	No default value	
Mode	Port Mode	
Usage Guide	If no statistic sampling interval is configured, there will not be any statistic sampling on the interface.	
Example	Set the statistic sampling interval on the interface e1/0/1 to 20 seconds. Switch(Config-If-Ethernet1/0/1)#sflow counter-interval 20	

15.2.4 sflow data-len

Command	**sflow data-len <*length-value*>** **no sflow data-len**	
parameter	***length-value***	is the value of the length with a value range of 500-1470
default	The value is 1400 by default.	
Mode	Port Mode	
Usage Guide	For configuring sflow packet length.When combining several samples to a sFlow group to be sent, the length of the group excluding the MAC head and IP head parts should not exceed the configured value.	
Example	Configure the max length of the sFlow packet data to 1000. switch (Config-If-Ethernet1/0/2)#sflow data-len 1000	

15.2.5 sflow destination

Command	**sflow destination <*collector-address*> [<*collector-port*>]**

no sflow destination

parameter	***collector-address***	is the IP address of the analyzer, shown in dotted decimal notation
	collector-port	is the destination port of the sent sFlow packets.
default	The destination port of the sFlow packet is defaulted at 6343, and the analyzer has no default address.	
Mode	Global Mode and Port Mode.	
Usage Guide	If the analyzer address is configured at Port Mode, this IP address and port configured at Port Mode will be applied when sending the sample packet. Or else the address and port configured at global mode will be applied. The analyzer address should be configured to let the sFlow sample proxy work properly.	
Example	Configure the analyzer address and port at global mode. switch (config)#sflow destination 192.168.1.200 1025	

15.2.6 sflow header-len

Command	**sflow header-len <*length-value*>** **no sflow header-len**	
parameter	***length-value***	is the value of the length with a valid range of 32-256.
default	128 by default.	
Mode	Port Mode.	
Usage Guide	Configure the length of header packets copied in sFlow data sampling. no" form reduction default value for this command. If the packet sample can not be identified whether it is IPv4 or IPv6 when sent to the CPU, certain length of the head of the group has to be copied to the sFlow packet and sent out. The length of the copied content is configured by this command.	
Example	Configure the length of the packet data head copied in the sFlow data sampling to 50. Switch(Config-If-Ethernet1/0/2)#sflow header-len 50	

15.2.7 sflow priority

Command	**sflow priority <*priority-value*>** **no sflow priority**

parameter

priority-value	is the priority value with a valid range of 0-3.

default

The default value is 0.

Mode

Global Mode.

Usage Guide

This command is used to set the priority of the sample message.When sample packet is sent to the CPU, it is recommended not to assign high priority for the packet so that regular receiving and sending of other protocol packet will not be interfered. The higher the priority value is set, the higher its priority will be.

Example

Configure the priority when sFlow receives packet from the hardware at global mode.

switch (config)#sflow priority 1

15.2.8 sflow rate

Command

sflow rate { input <*input-rate*> | output <*output-rate* >}

no sflow rate [input | output]

parameter

input-rate	is the rate of ingress group sampling, the valid range is 1000~16383500.
output-rate	is the rate of egress group sampling, the valid range is 1000~16383500

default

No default value.

Mode

Port Mode.

Usage Guide

The traffic sampling will not be performed if the sampling rate is not configured on the port. And if the ingress group sampling rate is set to 10000, this indicates there will be one group be sampled every 10000 ingress groups.

Example

Configure the ingress sample rate on port e1/0/1 to 10000 and the egress sample rate to 20000.

Switch(Config-If-Ethernet1/0/1)#sflow rate input 10000

```
Switch(Config-If-Ethernet1/0/1)#sflow rate output 20000
```

15.2.9 show sflow

Command **show sflow**

parameter -

default -

Mode All Modes.

Usage Guide This command is used to acknowledge the operation state of sFlow.

Example View sFlow configuration information.

```
Switch#show sflow

Sflow version 1.2
Agent address is 172.16.1.100
Collector address have not configured
Collector port is 6343
Sampler priority is 2
Sflow DataSource: type 2, index 194(Ethernet1/0/2)
Collector address is 192.168.1.200
Collector port is 6343
Counter interval is 0
Sample rate is input 0, output 0
Sample packet max len is 1400
Sample header max len is 50
Sample version is 4
```

Display information	describe
Sflow version 1.2	Indicates sFlow version 1.2
Agent address is 172.16.1.100	sFlow agent address :172.16.1.1100
Collector address have not configured	the sFlow global analyzer address is not configured
Collector port is 6343	the sFlow global destination port is the defaulted 6343
Sampler priority is 2	The priority of sFlow when receiving packets

	from the hardware is 2.
Sflow DataSource: type 2, index 194(Ethernet1/0/1)	One sample proxy data source of the sFlow is the interface e1/0/1 and its type is 2 (Ethernet), the interface index is 194.
Collector address is 192.168.1.200	The analyzer address of the sampling address of the E1/0/1 interface is 192.168.1.200
Collector port is 6343	Default value of the port on E1/0/1 interface sampling proxy is 6343.
Counter interval is 20	The statistic sampling interval on e1/0/1 interface is 20 seconds
Sample rate is input 10000, output 0	The ingress traffic rate of e1/0/1 interface sampling proxy is 10000 and no egress traffic sampling will be performed
Sample packet max len is 1400	The length of the sFlow group data sent by the e1/0/1 interface should not exceed 1400 bytes.
Sample header max len is 50	The length of the packet data head copied in the data sampling of the e1/0/1 interface sampling proxy is 50
Sample version is 4	The datagram version of the sFlow group sent by the E1/0/1 interface sampling proxy is 4.

15.3 RSPAN Configuration

15.3.1 remote-span

Command	**remote-span** **no remote-span**

parameter -

default Not configured

Mode VLAN Configuration Mode

Usage Guide This command is used to configure the existing VLAN as RSPAN VLAN. Dedicated RSPAN VLAN should be configured before RSPAN can function. When configuring RSPAN VLAN, it should be made sure that specialized VLAN, such as the default VLAN, dynamic VLAN, private VLAN, multicast VLAN, and layer 3 interface enabled VLAN, should not be configured as RSPAN VLAN. If any existing sessions are still working when RSPAN is disabled, these sessions will be still working regardless the configuration change. However, if any layer 3 interface is configure in the VLAN after RSPAN is disable, the existing RSPAN session will be stopped.

Example RSPAN VLAN. VLAN 5 configured.

Switch(Config-Vlan5)#remote-span

15.3.2 monitor session remote vlan

Command **monitor session <*session*> remote vlan <*vid*>**

no monitor session <*session*> remote vlan

parameter

session	session ID, range between 1~4
vid	The id of RSPAN VLAN

default Not configured

Mode Global Mode

Usage Guide To configure local mirror session to RSPAN. The VLAN id is the RSPAN VLAN. The mirrored data grams will be attached with RSPAN tags.

Example Configure the remote vlan of mirror session 1 to 5.

Switch(config)#monitor session 1 remote vlan 5

15.3.3 monitor session reflector-port

Command **monitor session <*session*> reflector-port <*interface-number*>**

no monitor session <*session*> reflector-port <*interface-number*>

parameter

session	Session ID, range between 1~4
interface-number	Interface number

default

Not configured

Mode

Global Mode.

Usage Guide

This command configures the reflector port for the destination of mirror data grams, and disables the MAC learning function of the specified port. The configuration of reflector port is to change the mode of the local port from the destination port mode to be the reflector mode. Hence, the configuration of reflector port and the destination port are exclusive. The no command is used to restore the reflector port to normal port. The source port, in access or trunk mode, should not be added to RSPAN VLAN. When the reflector port is configured as springboard of CPU TX direction mirroring, it must be configured as TRUNK port and allows the RSPAN VLAN data passing, the Native VLAN should not be configured as RSPAN VLAN. After configured RSPAN, the vlan tag will be added on the packet of the egress mirror. It will cause the abort error frame on the reflection port, so the default MTU value of the switch should be modified.

Example

Configure port 1/0/5 as a reflection port.

```
Switch(config)#monitor session 1 reflector-port ethernet1/0/5
```

Chapter 16 Network Time Management

16.1 SNTP

16.1.1 clock timezone

Command

clock timezone WORD {add | subtract} <0-23> [<0-59>]

no clock timezone WORD

Parameter

WORD	timezone name, the length should not exceed 16
add | subtract	the action of timezone
<0-23>	the hour value
<0-59>	the minute value

Default

None.

Mode

Global Mode

Usage Guide

This command configures timezone in global mode.

The timezone name is invalid with the blank, the hour and minute value must be in the specific range.

The no command deletes the configured timezone.

Example

Configure the action as add for the eighth timezone globally.

```
Switch(config)#clock timezone aaa add 8
```

16.1.2 sntp polltime

Command

sntp polltime <interval>

no sntp polltime

Parameter

<interval>	is the interval value from 16 to 16284

Default

The default polltime is 64 seconds.

Mode

Global Mode

Usage Guide

Sets the interval for SNTP clients to send requests to NTP/SNTP.

The no command cancels the polltime sets and restores the default setting.

Example

Setting the client to send request to the server every 128 seconds.

```
Switch(config)#sntp polltime128
```

16.1.3 sntp server

Command

sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

no sntp server {<ip-address> | <ipv6-address>} [source {vlan <vlan no> | loopback <loopback no>}] [version <version_no>]

Parameter

<ip-address>	IPv4 address of time server
<ipv6-address>	IPv6 address of time server
<vlan no>	Virtual LAN number, ranging from 1 to 4094
<loopback no>	Loopback identifier, ranging from 1 to 1024
<version_no>	Version number, ranging from 1 to 4, the default is 4

Default

By default,do not configure the time server.

Mode

Global Mode

Usage Guide

Enable the specified time server as clock source

The no command deletes the specified time server.

Example

Configure the time server address as 1.1.1.1, specify the interface of the source address as vlan1:

```
Switch(config)#sntp server 1.1.1.1 source vlan 1
```

16.1.4 show sntp

Command	**show sntp**
Parameter	**none** none
Default	None.
Mode	Admin/Global mode
Usage Guide	Displays current SNTP client configuration and server status.
Example	Displaying current SNTP configuration. **Switch(config)#show sntp**

16.2 NTP

16.2.1 ntp access-group

Command	**ntp access-group server <acl>** **no ntp access-group server <acl>**	
Parameter	**<acl>**	ACL number, range is from 1 to 99
Default	Not configure the access control of NTP Server by default.	
Mode	Global Mode	
Usage Guide	To configure/cancel the access control list of NTP Server. The no command delete configuration.	
Example	To configure access control list 2 on the switch. **Switch(config)#ntp access-group server 2**	

16.2.2 ntp authenticate

Command	**ntp authenticate** **no ntp authenticate**	
Parameter	**none**	none
Default	By default, NTP authentication is cancelled.	
Mode	Global Mode	
Usage Guide	To enable/cancel NTP authentication function. The no command cancel NTP authentication function.	
Example	To enable NTP authentication function. **Switch(config)#ntp authenticate**	

16.2.3 ntp authentication-key

Command

ntp authentication-key <key-id> md5 <value>

no ntp authentication-key <key-id>

Parameter

<key-id>	The id of key, range is from 1 to 4294967295
<value>	The value of key, range between 1 to 16 of ascii code

Default

The authentication key of NTP authentication is not configured by default.

Mode

Global Mode

Usage Guide

To enable/cancel NTP authentication function, and defined NTP authentication key.

The no command cancel NTP authentication function

Example

To define the authentication key of NTP authentication, the key-id is 20, the md5 is abc.

```
Switch(config)#ntp authentication-key 20 md5 abc
```

16.2.4 ntp broadcast server count

Command

ntp broadcast server count <number>

no ntp broadcast server count

Parameter

<number>	the max number of broadcast servers, 1-100

Default

The default max number of broadcast servers is 50.

Mode

Global Mode

Usage Guide

Set the max number of broadcast or multicast servers supported by the NTP client.

The no operation will cancel the configuration and restore the default value.

Example

Configure the max number of broadcast servers is 70 on the switch.

```
Switch(config)#ntp broadcast server count 70
```

16.2.5 ntp disable

Command

ntp disable
no ntp disable

Parameter

none	none

Default

By default, NTP function are enabled on all ports.

Mode

VLAN Configuration Mode

Usage Guide

To disable/enable the NTP function on port.

The no command disables the NTP function on the port.

Example

To disable the NTP function on vlan1 interface.

```
Switch(config)# interface vlan 1
Switch(config-if-Vlan1)#ntp disable
```

16.2.6 ntp enable

Command

ntp enable
ntp disable

Parameter

none	none

Default

By default, global disable NTP function.

Mode

Global Mode

Usage Guide

To enable/disable NTP function globally.

Disable command global disable NTP function.

Example

Configure switch global enable NTP function.

```
Switch(config)# ntp enable
```

16.2.7 ntp ipv6 multicast client

Command	**ntp ipv6 multicast client** **no ntp ipv6 multicast client**
Parameter	**none** none
Default	By default,Interface does not receive IPv6 NTP multicast packets.
Mode	VLAN Configuration mode
Usage Guide	Configure the specified interface to receive IPv6 NTP multicast packets The no command will cancels the specified interface to receive IPv6 NTP multicast packets.
Example	Enable the function for receiving IPv6 NTP multicast packets on vlan1 interface. **Switch(config)# interface vlan 1** **Switch(config-if-Vlan1)#ntp ipv6 multicast client**

16.2.8 ntp multicast client

Command	**ntp multicast client** **no ntp multicast client**
Parameter	**none** none
Default	By default,Interface does not receive NTP multicast packets.
Mode	VLAN Configuration mode
Usage Guide	Configure the specified interface to receive NTP multicast packets. The no command will cancels the specified interface to receive NTP multicast packets.
Example	Enable the function for receiving NTP multicast packets on vlan1 interface. **Switch(config)# interface vlan 1** **Switch(config-if-Vlan1)#ntp multicast client**

16.2.9 ntp server

Command

ntp server {<ip-address> | <ipv6-address>} [version <version_no>] [key <key-id>]
no ntp server {<ip-address>|<ipv6-address>}

Parameter

<ip-address>	IPv4 address of time server
<ipv6-address>	IPv6 address of time server
<version_no>	The version number of server, range is from 1 to 4, default is 4
<key-id>	The key id

Default

By default,disable。

Mode

Global Mode

Usage Guide

To enable specified time server of time source.

The no form of this command cancels the specified time server of time source.

Example

To configure time server address as 1.1.1.1 on switch.

Switch(config)# ntp server 1.1.1.1

16.2.10 ntp syn-interval

Command

ntp syn-interval <1-3600>
no ntp syn-interval

Parameter

<1-3600>	the request packet sending interval of ntp client as 1s-3600s

Default

By default,64s interval.

Mode

Global Mode

Usage Guide

Configure the request packet sending interval of ntp client as 1s-3600s.
For responding the risk of ntp adjusting the system time under the high latency network, ntp client will select the time information with the smallest latency for the system time synchronization after sent 8 ntp time requisitions. So at the default configuration, ntp client sends the requisition packet once every 64s, after 8 times, it will adjust the time. It

means to adjust the system time every 8 minutes. If user wants to configure the interval, such as one hour, user should adjust the packet sending interval as 450(3600/8) s.

The no command recovers to be the default value of 64s.

Example

Configure to adjust the system time once an hour, and the packet sending time is 450s.

Switch(config)# ntp syn-interval 450

16.2.11 ntp trusted-key

Command

ntp trusted-key <key-id>
no ntp trusted-key <key-id>

Parameter

<key-id>	The id of key, range is from 1 to 4294967295

Default

Trusted key is not configured by default.

Mode

Global Mode

Usage Guide

To configure the trusted key.

The no command cancels the trusted key.

Example

To configure the specified key 20 to trusted key.

Switch(config)# ntp trusted-key 20

16.2.12 show ntp status

Command	**show ntp status**	
Parameter	**none**	none
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	To display time synchronization status, include synchronized or not, layers, address of time source and so on.	

Example

Display time synchronization status.

```
Switch(config)# show ntp status
Clock status: synchronized
Clock stratum: 3
Reference clock server: 1.1.1.2
Clock offset: 0.010 s
Root delay: 0.012 ms
Root dispersion: 0.000 ms
Reference time: TUE JAN 03 01:27:24 2006
```

16.2.13 show ntp session

Command	**show ntp session [<ip-address> | <ipv6-address>]**	
Parameter	**<ip-address>**	The IPv4 address of some specifics configured time server
	<ipv6-address>	The IPv6 address of some specifics configured time server
Default	None.	
Mode	Admin/Global Mode	
Usage Guide	To display the information of all NTP session or one specific session, include server ID, server layer, and the local offset according to server. (The symbol * means this server is the selected local time source)	

Example

To display the information of all NTP session.

```
Switch(config)# show ntp session
    server    stream    type    rootdelay    rootdispersion    trustlevel
*   1.1.1.2     2      unicast   0.010s          0.002s            10
    2.2.2.2     3      unicast   0.005s          0.000s            10
```

16.3 Summer Time

16.3.1 clock summer-time absolute

Command

clock summer-time <word> absolute <HH:MM> <YYYY.MM.DD> <HH:MM> <YYYY.MM.DD> [<offset>]
no clock summer-time

Parameter

<word>	the time zone name of summer time
<HH:MM>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)
<YYYY.MM.DD>	the start date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)
<HH:MM>	the end time, the format is hour (from 0 to 23):minute (from 0 to 59)
<YYYY.MM.DD>	the end date, the format is year (from 1970 to 2038).month (from 1 to 12).date (from 1 to 31)
<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes

Default

By default,there is no summer time range.

Mode

Global Mode

Usage Guide

Configure summer time range, the time in this range is summer time.
This command sets the absolute start and end time for summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the system time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. Note: the end time should be bigger than the start time for configuring summer time.

The no command deletes the configuration.

Example

Configure the time range of summer time at 12:10 from april 6th to augest 6th in 2010, offset value as 70 minutes, summer time is named as aaa.

```
Switch(config)#clock summer-time aaa absolute 12:10 2010.4.6 12:10 2010.8.6 70
```

16.3.2 clock summer-time recurring

Command

clock summer-time <word> recurring <HH:MM> <MM.DD> <HH:MM> <MM.DD> [<offset>]

no clock summer-time

Parameter

<word>	the time zone name of summer time
<HH:MM>	the start time, the format is hour (from 0 to 23):minute (from 0 to 59)
<MM.DD>	the start date, the format is month(from 1 to 12).date(from 1 to 31)
<HH:MM>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)
<MM.DD>	the end date, the format is month(from 1 to 12).date(from 1 to 31)
<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes.

Default

By default,there is no summer time range.

Mode

Global Mode

Usage Guide

Configure the recurrent summer time range, the time in this range is summer time.
This command sets the start and the end time for the recurrent summer time. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the syst em time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relationbetween the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports the summer time of southern hemisphere.

The no command delete summer time configuration.

Example

Configure the time range of summer time at 12:10 from april 6th to augest 6th year after year, offset value as 70 minutes, summer time is named as aaa.

```
Switch(config)#clock summer-time aaa recurring 12:10 4.6 12:10 8.6 70
```

16.3.3 clock summer-time recurring

Command	**clock summer-time <word> recurring<HH:MM> <week> <day> <month>< HH:MM > <week> <day> <month> [<offset>]** **no clock summer-time**	
Parameter	**<word>**	the time zone name of summer time
	<HH:MM>	the start time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<week>	the week from 1 to 4, first or last
	<day>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"
	<month>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"
	<HH:MM>	the end time, the format is hour(from 0 to 23):minute(from 0 to 59)
	<week>	the week from 1 to 4, first or last
	<day>	the week value, the value as "Sun", "Mon", "Tue", "Wed", "Thu", "Fri", "Sat"
	<month>	the month, the value as "Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec"
	<offset>	the time offset, the range from 1 to 1440, unit is minute, default value is 60 minutes
Default	By default,there is no summer time range.	
Mode	Global Mode	
Usage Guide	Configure the recurrent summer time range, the time in this range is summer time. This command sets the start and end time for the recurrent summer time flexibly. When the system time reaches to the start time point of summer time, the clock is changed and increase <offset> value, the system enters summer time. When the syst em time reaches to the end time point of summer time, the clock is changed again, subtract <offset> value from system time, the system finishes summer time. There is no relation between the recurrent summer time to the year, the system clock will be changed when it reaches to the start and the end time point of summer time year after year. This command supports summer time of southern hemisphere. The no command delete summer time configuration.	
Example	Configure summer time at 12:10 from the first Monday of april to the last Saturday of augest year after year, offset value as 70 minutes, summer time is named as aaa. **Switch(config)#clock summer-time aaa recurring 12:10 1 mon apr 12:10 last sat aug 70**	

Chapter 17 Debugging and Diagnosis

17.1 SHOW

17.1.1 clear history all-users

Syntax	**clear history all-users**
Parameter	none
Default	none
Mode	Admin mode
Usage	Using this command can clear the command history of all users.
Example	Switch#clear history all-users

17.1.2 clear logging

Syntax	**clear logging sdram**
Parameter	none
Default	none
Mode	Admin mode
Usage	When the old information in the log buffer zone is no longer concerned, we can use this command to clear all the information.
Example	Clear all information in the log buffer zone sdram. Switch#clear logging sdram

17.1.3 history all-users max-length

Syntax	**history all-users max-length <count>**	
Parameter	**<count>**	the command history number can be saved, ranging from 100 to 1000
Default	The system can save 100 recent command history of all users at best by default	
Mode	Global mode	
Usage	using this command can set the max command history number	
Example	Switch#config Switch(config)#history all-users max-length 500	

17.1.4 logging

Syntax	**logging { <ipv4-addr> | <ipv6-addr> } [facility <local-number>] [level <severity>]** **no logging { <ipv4-addr> | <ipv6-addr> } [facility <local-number>]**	
Parameter	**<ipv4-addr>**	IPv4 address of the host
	<ipv6-addr>	IPv6 address of the host
	<local-number>	recording equipment of the host with a valid range of local0～local7, which is in accordance with the facility defined in the RFC3164
	<severity>	severity threshold of the log information severity level. The rule of the log information output is explained as follows: only those with a level equal to or higher than the threshold will be outputted. For detailed description on the severity please refer to the operation manual.
Default	No log information output to the log host by default. The default recorder of the log host is the local0; the default severity level is warnings.	
Mode	Global mode	
Usage	The command is used to configure the output channel of the log host. The "no" form of this command will disable the output at the log host output channel. Only when the log host is configured by the logging command, this command will be available. We can configure many IPv4 and IPv6 log hosts.	
Example	Send the log information with a severity level equal to or higher than warning to the log server with an IPv4 address of 100.100.100.5, and save to the log recording equipment local1. Switch#config Switch(config)#logging 100.100.100.5 facility local1 level warnings	

17.1.5 logging executed-commands

Syntax	**logging executed-commands {enable | disable}**
Parameter	**none**
Default	Disable state.
Mode	Global mode
Usage	After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log, so it should be used with the logging LOGHOST command.
Example	Enable the command and send the commands executed by user into log host (10.1.1.1) Switch#config Switch(config)#logging 10.1.1.1 Switch(config)#logging executed-commands enable

17.1.6 logging loghost sequence-number

Syntax	**logging loghost sequence-number** **no logging loghost sequence-number**
Parameter	**none**
Default	Do not include the sequence-number.
Mode	Global mode
Usage	Add the loghost sequence-number for the log; the no command does not include the loghost sequence-number. Use logging command to configure the loghost before this command is set.
Example	Open the loghost sequence-number Switch#config Switch(config) #logging loghost sequence-number

17.1.7 logging source-ip

Syntax	**logging source-ip { <A.B.C.D> | <X:X::X:X> }**	
Parameter	**<ipv4-addr>**	IPv4 address of the host
	<ipv6-addr>	IPv6 address of the host
Default	None0000	
Mode	Global mode	
Usage	Appoint the source IP address of the log packet which is sent to the log server, the ipv4 or ipv6 addresses can be configured. After configured this command, the log information sent to the server has the IP address; if this command is not configured, the log information does not have the IP address.	
Example	Configure the source IP address of the log packet which is sent to the log server. Switch#config Switch(config)#logging source-ip 2010::10	

17.1.8 ping

Syntax	**ping [[src <source-address>] { <destination-address> | host <hostname> }]**	
Parameter	**<source-address>**	***<source-address>*** is the source IP address where the ping command is issued, with IP address in dotted decimal format.
	<destination-address>	***<destination-address>*** is the target IP address of the ping command, with IP address in dotted decimal format
	<hostname>	***<hostname>*** is the target host name of the ping command, which should not exceed 64 characters.
Default	5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.	
Mode	Admin mode	
Usage	Issue ICMP request to remote devices, check whether the remote device can be reached by the switch. When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.	
Example	**Example** 1：To ping with default parameters. Switch#ping 10.1.128.160 Type ^c to abort. Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds. ...!!	

```
Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms
```

In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2：Ping with parameters entered interactively.

```
Switch#ping
VRF name：
Use IP Address[y]: y
Target IP address：10.1.128.160
Use source address option[n]: y
Source IP address: 10.1.128.161
Repeat count [5]: 100
Datagram size in byte [56]：1000
Timeout in milli-seconds [2000]: 500
Extended commands [n]: n
```

Display Information	Explanation
VRF name	VRM name. If MPLS is not enabled, this field will be left empty.
Target IP address：	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.
Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

17.1.9 ping6

Syntax **ping6 [<dst-ipv6-address> | host <hostname> | src <src-ipv6-address>**

	{<dst-ipv6-address > | host <hostname>}]	
Parameter	**<dst-ipv6-address>**	target IPv6 address of the ping command
	<src-ipv6-address>	source IPv6 address where the ping command is issued
	<hostname>	arget host name of the ping command, which should not exceed 64 characters.
Default	Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default timeout to be 2 seconds.	
Mode	Admin mode	
Usage	To check whether the destination network can be reached. When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.	

Example

Example 1：To issue ping6 command with default parameters.

```
Switch#ping6 2001:1:2::4
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms
```

Example 2：To issue the ping6 command with parameters input interactively.

```
Switch#ping6
Target IPv6 address:fe80::2d0:59ff:feb8:3b27
Output Interface: vlan1
Use source address option[n]:y
Source IPv6 address: fe80::203:fff:fe0b:16e3
Repeat count [5]:
Datagram size in byte [56]:
Timeout in milli-seconds [2000]:
Extended commands [n]:
Type ^c to abort.
Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address
fe80::203:fff:fe0b:16e3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms
```

Display Information	Explanation

ping6	The ping6 command
Target IPv6 address	The target IPv6 address of the command
Output Interface	The name of he VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]:	Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address.
Repeat count[5]	Number of the ping packets.
Datagram size in byte[56]	Packet size of the ping command. 56 byte by default.
Timeout in milli-seconds[2000]	Timeout for ping command. 2 seconds by default.
Extended commands[n]	Extended configuration. Disabled by default.
!	The network is reachable.
.	The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Statistic information, success rate is 100 percent of ping packet.

17.1.10 show boot-files

Syntax **show boot-files**

Parameter none

Default none

Mode Admin and Configuration Mode.

Usage Display the first and second IMG files and the CFG file enabled by switch.

After implementing this command, the booting sequence of IMG files in the corresponding storage device, which IMG file is currently used in booting, the configuration information of the CFG file in the storage device and the CFG file currently booted.

Example Display the first and second IMG files and the CFG file enabled by switch.

```
Switch#show boot-files
Booted files on switch
The primary img file at the next boot time: flash:/nos.img
The backup img file at the next boot time: flash:/nos.img
Current booted img file: flash:/nos.img
The startup-config file at the next boot time: flash:/startup.cfg
Current booted startup-config file: flash:/startup.cfg
```

If the CFG file of the next booting is set as NULL, the CFG part mentioned above will be displayed as follows:

```
The startup-config file at the next boot time: NULL
Current booted startup-config file: flash:/startup.cfg
```

17.1.11 show flash

Syntax **Show flash**

Parameter **none**

Default none

Mode Admin and Configuration Mode.

Usage Show the size of the files which are reserved in the system flash memory.

Example To list the files and their size in the flash.

```
Switch#show flash

total    12227K
-rw-          12516553          nos.img
-rw-          3224             startup.cfg

Drive : flash:
Size:30.0M    Used:13.0M    Available:17.0M    Use:43%
```

17.1.12 show history

Syntax **show history**

Parameter **none**

Default none

Mode Admin Mode

Usage Display the recent user command history.

The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example

```
Switch# show history
enable
config
interface ethernet 1/0/3
enable
dir
show ftp
```

17.1.13 show history all-users

Syntax **show history all-users [detail]**

Parameter **detail** shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH

Default none

Mode Admin and configuration mode

Usage This command is used to show the recent command history of all users, including time, logging type, executing command, etc.

Notice: The user can only check the command history of other users whose purview should not be higher than oneself.

Example

```
Switch# show history all-users detail
Time Type User Command
0w 0d 0h 2m Telnet/SSH admin show history all-users detail 192.168.1.2:1419
0w 0d 0h 1m Telnet/SSH admin show history all-users 192.168.1.2:1419
0w 0d 0h 1m Console Null show history all-users
0w 0d 0h 1m Console Null end
0w 0d 0h 1m Console Null ip address 192.168.1.1 255.255.255.0
0w 0d 0h 0m Console Null in v 1
0w 0d 0h 0m Console Null telnet-server enable
```

17.1.14 show logging buffered

Syntax	**show logging buffered [level {critical | warnings} | range <begin-index> <end-index>]**	
Parameter	**level {critical | warnings}**	level of critical information
	<begin-index>	index start value of the log message, the valid range is 1-65535
	<end-index>	index end value of the log message, and the valid range is 1-65535. When only display logging buffered information of the line card must be added range parameter, but the main control has not the reques
Default	No parameter specified indicates all the critical log information will be displayed.	
Mode	Admin and configuration mode	
Usage	This command displays the detailed information in the log buffer channel. This command is not supported on low end switches. Warning and critical log information is saved in the buffer zone. When displayed to the terminal, their display format should be: index ID time <level> module ID [mission name] log information.	
Example	Display the critical log information in the log buffer zone channel and related to the main control with index ID between 940 and 946. Switch# show logging buffered level critical range 940 946 Current messages in SDRAM:0	

17.1.15 show logging executed-commands state

Syntax	**show logging executed-commands state**
Parameter	**none**
Default	none
Mode	Admin Mode
Usage	Use this command to display the state (enable or disable).
Example	Switch#show logging executed-commands state Logging executed command state is enable

17.1.16 show logging source

Syntax	**show logging source mstp**
Parameter	**None**
Default	None
Mode	Admin and configuration mode
Usage	Show the log information source of MSTP module.
Example	Show the log information source of MSTP. Switch#show logging source mstp system module log switch status: Channel Onoff Severity logbuff on warning loghost on warning terminal on warning

17.1.17 show running-config

Syntax	**show running-config**
Parameter	**none**
Default	None
Mode	Admin Mode
Usage	Display the current active configuration parameters for the switch. When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters. 。
Example	Switch#show running-config

17.1.18 show running-config current-mode

Syntax	**show running-config current-mode**
Parameter	none
Default	none
Mode	All configuration modes.
Usage	Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.
Example	Switch(config-if-ethernet1/0/1)#show run c ! Interface Ethernet1/0/1 switchport access vlan 2 !

17.1.19 show startup-config

Syntax **show startup-config**

Parameter **none**

Default If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Mode Admin Mode

Usage The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

Example

```
Switch#show startup-config
```

17.1.20 show switchport interface

Syntax **show switchport interface [ethernet] <IFNAME>**

Parameter **<IFNAME>** port number

Default none

Mode Admin and configuration mode

Usage Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

Example Show VLAN messages of port ethernet 1/0/1

```
Switch#show switchport interface ethernet 1/0/1
Ethernet1/0/1
Type :Universal
Mode :Trunk
Port VID :1
Trunk allowed Vlan :1-4094
```

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan : ALL	VLAN permitted by Trunk

17.1.21 show tcp

Syntax **show tcp**

Parameter **none**

Default none

Mode Admin Mode

Usage Display the current TCP connection status established to the switch.

Example

```
Switch#show tcp
LocalAddress LocalPort ForeignAddress ForeignPort State
0.0.0.0 23 0.0.0.0 0 LISTEN
0.0.0.0 80 0.0.0.0 0 LISTEN
```

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local pot number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

17.1.22 show tcp ipv6

Syntax **show tcp ipv6**

Parameter **none**

Default none

Mode Admin and configuration mode

Usage Show the current TCP connection.

Example

```
Switch#show tcp ipv6
LocalAddress                                        LocalPort    RemoteAddress
RemotePort   State        IF   VRF
::                                                      80                  ::
0            LISTEN        0    0
::                                                      23                  ::
0            LISTEN        0    0
```

Displayed Information	Explanation

LocalAddress	Local IPv6 address of TCP connection
LocalPort	Local port of TCP connection
RemoteAddress	Remote IPv6 address of TCP connection
RemotePort	Remote Port of TCP connection
State	The current state of TCP connection
IF	Local port index of TCP connection
VRF	Virtual route forward instance

17.1.23 show telnet login

Syntax **show telnet login**

Parameter **none**

Default none

Mode Admin and configuration mode

Usage This command used to list the information of currently available telnet clients which are connected to the switch

Example

```
Switch#show telnet login
Authenticate login by local.
Login user:
aa
```

17.1.24 show udp

Syntax **show udp**

Parameter **none**

Default none

Mode Admin Mode

Usage Display the current UDP connection status established to the switch.

Example

```
Switch#show udp
LocalAddress       LocalPort   ForeignAddress    ForeignPort       State
0.0.0.0            32768       0.0.0.0           0                 CLOSE
0.0.0.0            3071        0.0.0.0           0                 CLOSE
```

Displayed Information	Description
LocalAddress	Local address of the UDP connection.
LocalPort	Local pot number of the UDP connection.
ForeignAddress	Remote address of the UDP connection.
ForeignPort	Remote port number of the UDP connection.
State	Current status of the UDP connection.

17.1.25 show udp ipv6

Syntax **show udp ipv6**

Parameter **none**

Default none

Mode Admin and configuration mode

Usage Show the current UDP connection

Example

```
Switch#show udp ipv6
LocalAddress                                              LocalPort     RemoteAddress
RemotePort    State
::                                                                 3071              ::
0                 CLOSE
```

Displayed Information	Description
LocalAddress	Local IPv6 address of the UDP connection.
LocalPort	Local port number of the UDP connection.
RemoteAddress	Remote IPv6 address of the UDP connection.
RemotePort	Remote port number of the UDP connection.
State	Current status of the UDP connection.

17.1.26 show version

Syntax **show version**

Parameter **none**

Default

none

Mode

Admin Mode

Usage

Display the switch version.

Use this command to view the version information for the switch, including hardware version and software version.

Example

```
Switch#show version
```

17.1.27 traceroute

Syntax

traceroute [source <ipv4-addr>] { <ip-addr> | host <hostname> } [hops <hops>] [timeout <timeout>]

Parameter

<ipv4-addr>	assigned source host IPv4 address in dot decimal format
<ip-addr>	target host IP address in dot decimal format
<hostname>	hostname for the remote host
<hops>	maximum gateway number allowed by Traceroute command
<timeout>	timeout value for test packets in milliseconds, between 100 -10000

Default

The default maximum gateway number is 30, timeout in 2000 ms.

Mode

Admin mode

Usage

This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Traceroute is usually used to locate the problem for unreachable network nodes.

Example

```
Switch#traceroute 192.168.2.36
Type ^c to abort.
Traceroute to host 192.168.2.36, maxhops is 30, timeout is 2000ms.
  1     0ms       192.168.2.36
Traceroute completed.
```

17.1.28 traceroute6

Syntax

traceroute6 [source <addr>] {<ipv6-addr> | host <hostname>} [hops <hops>] [timeout <timeout>]

Parameter

<ipv4-addr>	assigned source host IPv6 address in colonned hex notation.
<ip-addr>	IPv6 address of the destination host, shown in colonned hex notation
<hostname>	name of the remote host
<hops>	max number of the gateways the traceroute6 passed through, ranging between 1-255
<timeout>	timeout period of the data packets, shown in millisecond and ranging between 100~10000

Default

Default number of the gateways passes by the data packets is 30, and timeout period is defaulted at 2000ms.

Mode

Admin mode

Usage

This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.

Traceroute6 is normally used to locate destination network inaccessible failures.

Example

```
Switch#traceroute6 2004:1:2:3::4
Type ^c to abort.
Traceroute to IPv6 host 2004:1:2:3::4, maxhops is 30, timeout is 2000ms.
Traceroute6 error occured.
```

17.1.29 reload after

Syntax

reload after {[<HH:MM:SS>] [days <days>]}

Parameter

<HH:MM:SS>	specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59
<days>	specified days, unit is day, range from 1 to 30.

Default

none

Mode

Admin mode

Usage

With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.

Example

Set the switch to automatically reload after 2 days, 10 hours and 1 second.

```
Switch#reload after 10:00:01 days 2
Process with reboot after? [Y/N] y
```

17.1.30 reload cancel

Syntax	**reload cancel**
Parameter	**none**
Default	none
Mode	Admin mode
Usage	Cancel the specified time period to reload the switch. With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command "reload after". This command will not be reserved.
Example	Prevent the switch to automatically reboot after the specified time. Switch#reload cancel Reload cancel successful.

17.1.31 show reload

Syntax	**show reload**
Parameter	none
Default	none
Mode	Admin and configuration mode
Usage	Display the user's configuration of command "reload after". With this command, users can view the configuration of command "reload after" and check how long a time is left before rebooting the switch.
Example	View the configuration of command "reload after". In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it. Switch#show reload The original reload after configuration is 10:00:01. System will be rebooted after 09:59:48 from now.

17.1.32 clear cpu-rx-stat protocol

Syntax	**clear cpu-rx-stat protocol [<protocol-type>]**	
Parameter	**<protocol-type>**	type of the protocol of the packet**,** , including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
Default	none	
Mode	Admin mode	
Usage	This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.	
Example	Clear the statistics of the CPU receives ARP packets. Switch#config Switch(config)#clear cpu-rx-stat protocol arp	

17.1.33 cpu-rx-ratelimit protocol

Syntax	**cpu-rx-ratelimit protocol <protocol-type> <packets>** **no cpu-rx-ratelimit protocol <protocol-type>**	
Parameter	**<protocol-type>**	type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh
	<packets>	max rate of CPU receiving packets of the protocol type, its range is 1-2000 pps.
Default	A different default rate is set for the different type of protocol.	
Mode	Global mode	
Usage	Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default. The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.	
Example	set the rate of the ARP packets to 500pps. Switch#config Switch(config)#cpu-rx-ratelimit protocol arp 500	

17.1.34 cpu-rx-ratelimit total

Syntax	**cpu-rx-ratelimit total <packets>** **no cpu-rx-ratelimit total**	
Parameter	<packets>	max number of CPU receiving packets per second
Default	1200pps	
Mode	Global mode	
Usage	Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default. The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.	
Example	Set the total rate of the CPU receive packets to 1500pps. Switch#config Switch(config)# cpu-rx-ratelimit total 1500	

17.1.35 show cpu-rx protocol

Syntax	**show cpu-rx protocol [<protocol-type>]**	
Parameter	**<protocol-type>**	protocol type of the packets, if do not input parameters, show all statistic packets.
Default	none	
Mode	Admin and configuration mode	
Usage	Show the statistics of the CPU received packets of the specified protocol type. This command is used to debug, it is supposed to be used with the help of the technical support.	
Example	Show the statistics of CPU receiving ARP packets. Switch#show cpu-rx protocol arp Type Rate-limit TotPkts DropPkts DelayCount CurState ARP 300 0 0 0 allowed	

Chapter 18 PoE

18.1 PoE Configuration

18.1.1 power inline enable (Global)

Command	**power inline enable** **no power inline enable**
parameter	-
default	Disable.
Mode	Global Mode
Usage Guide	This command enables/disables global PoE.With PoE globally disabled, there would be no power output no matter what the power state of a specified port is.
Example	Globally disable PoE. Switch(Config)#no power inline enable

18.1.2 power inline enable (Port)

Command	**power inline enable** **no power inline enable**
parameter	-
default	Disable.
Mode	Port Mode.
Usage Guide	This command is used to enable/disable the specified port PoE, when the port disables the POE, there will be no power output regardless of the power state of the specified port.
Example	Disable power supply on ports1/0/1. Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#no power inline enable

18.1.3 power inline high-inrush

Command	**power inline high-inrush enable** **no power inline high-inrush enable**
parameter	-
default	The allowed high-inrush current is not enabled
Mode	Global mode
Usage Guide	Power for non-standard PD instantaneously, this command is used to enable allowed high inrush output, no the command disables high inrush output. High-inrush current will be brought when nonstandard PD is powered instantaneously, it will result PSE self-protection to make PD power failure. Here, if this nonstandard PD must be powered, it needs to allow the high-inrush current.
Example	Enable the allowed high-inrush current when nonstandard PD is powered instantaneously. Switch(config)#power inline high-inrush enable

18.1.4 power inline legacy

Command	**power inline legacy enable** **no power inline legacy enable**
parameter	-
default	Do not provide power supply for non-standard IEEE PD
Mode	Global Mode
Usage Guide	This command is used to enable non-standard IEEE PD detection functionality. No command disables non-standard IEEE PD detection function.
Example	Set the switch to provide power supply for non-standard IEEE PD. Switch(config)#power inline legacy enable

18.1.5 power inline max (Global)

Command

power inline max <*max-wattage*>

no power inline max

parameter

max-wattage	value of the max output power, in W. Any integer from 37 to 130 is valid

default

Default maximum output power 370W

Mode

Global Mode

Usage Guide

This command is used to set the global maximum output power of the POE no restore the default configuration.

Example

Set the global max output power to 50W.

```
Switch(Config)#power inline max 50
```

18.1.6 power inline max (Port)

Command

power inline max <*max-wattage*>

no power inline max

parameter

max-wattage	the value of the max output power, in mW, ranging from 1 to 15400mW, with a granularity of 100mW. Any value less than 100mW will be taken as 100mW, that is, 1~100 equals 100, 15301~15400 equals 15400. But the value set by users will be maintained without being rounded up.

default

Default port maximum output power 32000mW

Mode

Port Mode

Usage Guide

This command can be used to set the maximum output power of the specified port.

Example

Set the max output power of Port 1 to 0.8W.

```
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)#power inline max 800
```

18.1.7 power inline police

Command	**power inline police enable** **no power inline police enable**
parameter	-
default	The power priority management policy mode is disabled
Mode	Global Mode
Usage Guide	This command is used to enable or disable priority management policy mode. In priority mode, when not enough PSE power is available, ports with low priority will be closed to satisfy the power supply for ports with high priority, no matter how long the access time of a PD is. If two ports have same priority, the one with smaller sequence number is higher privileged. In first-come-first-served mode, new PDs will not get power supply if available PSE power is not enough.
Example	Enable the power priority policy mode. Switch(Config)#power inline police enable

18.1.8 power inline priority

Command	**power inline priority {critical | high | low}**	
parameter	**critical**	the highest-level priority
	high	high-level priority
	low	low-level priority
default	Port priority is low	
Mode	Port Mode	
Usage Guide	This command is used to set the priority level of the port.This command will take effect in the mode of "power inline police enable". Without enough available power for newly connected PD, ports with higher priority will get power supply first.	
Example	Set the priority of Port 1 to high and that of Port 2 to critical. Switch(Config)#interface ethernet 1/0/1 Switch(Config-Ethernet1/0/1)#power inline priority high Switch(Config)#interface ethernet 1/0/2 Switch(Config-Ethernet1/0/2)#power inline priority critical	

18.1.9 power inline monitor interval

Command	**power inline monitor interval <30-36000>**	
parameter	<30-36000>	Monitoring interval, size range :30-36000, per second
default	The default configuration interval is 150 seconds	
Mode	Global mode	
Usage Guide	this command is used to configure poe monitor interval time.	
Example	The interval between switches is 3600 seconds. Switch(config)#power inline monitor interval 3600	

18.1.10 power inline monitor {on|off }

Command	**18.2 power inline monitor {on|off}**
parameter	-
default	Default disable poe monitor function
Mode	Port Configuration Mode
Usage Guide	This command is used to enable or disable poe monitoring function.
Example	enable poe detection function on port 1/0/1. Switch(config-if-ethernet1/0/1)#power inline monitor on

18.2 power inline monitor {on|off}

18.2.1 power inline power-off

Command	**power inline power-off time-range <*name*>**	
parameter	**<*name*>**	Time range name: This name is defined by the user and the character length is 1-64 bits
default	Default not configured	
Mode	Port Mode	
Usage Guide	this command is used to set poe timing off.	
Example	The poe setting switch port 1/0/1 closes at t1. Switch(config-if-ethernet1/0/1)#power inline power-off time-range t1	

18.2.2 power inline reset interval

Command	**power inline reset interval <1-600>**	
parameter	**<1-600>**	Refresh time interval size :1-600 per second
default	Default refresh time is 5 seconds	
Mode	Global mode	
Usage Guide	this command can be used to set poe refresh interval time.	
Example	Sets the refresh interval poe the switch to 20 seconds. Switch(config)#power inline reset interval 20	

18.3 PoE Monitoring and Debugging

18.3.1 show power inline

Command	**show power inline**
parameter	-
default	-
Mode	Admin Mode
Usage Guide	This command is used to view POE global configuration and state。
Example	View global POE configuration and status.Switch#show power inline。

```
PoE Work Status          : online
PoE Port Max Number       : 24
PoE Support Type         : 802.3at/802.3af
PoE MCU Software Version : V2.1
PoE Power Available     : 370 W
PoE Power Used            : 0 W
PoE Power Remaining       : 370 W
PoE Main Voltage         : 54.8 V
PoE Min Voltage          : 44 V
PoE Max Voltage          : 57 V
PoE Police               : Enable
PoE Legacy                : Enable
PoE High-inrush Status  : Disable
PoE Monitor Interval   : 150 s
PoE Reset Interval      : 5 s
```

Display entries	describe
PoE Work Status	POE working status
PoE Power Available	Global maximum of available power
PoE Power Used	Power currently in use
PoE Power Remaining	Remaining available power
PoE Min Voltage	minimum voltage
PoE Max Voltage	maximum voltage
PoE Police	Power Priority Policy Enable Status
PoE Legacy	Status of non-standard PD detection function
PoE High-inrush Status	Poe high inrush state

18.3.2 show power inline interface ethernet

Command	**show power inline interface [ethernet <*interface-number*> | <*interface-name*>]**	
parameter	***interface-number***	Ethernet port number
default	-	
Mode	Admin Mode	
Usage Guide	This command is used to view the configuration and status displayed on POE specified port.	
Example	View POE information on port 1/0/1.	

```
Switch#show power inline interface ethernet 1/0/1

Interface         Status   Oper    Power(mW)  Max(mW)  Current(mA)  Volt(V)  Priority
Class
-------------- ------- ------ --------- ------- ----------- ------- -------- -----
Ethernet1/0/1    Disable     Off            0       800              0        54         Low
N/A
```

Display entries	describe
Oper	Working status: On：PD normal connection Off：PD no connection Faulty：PD detection failure Deny：Not enough power available or required to exceed the limit
Current(mA)	Current current at port
Volt(V)	Current voltage at port
Class	PD input power used: 0 Default 0.44~12.95 1 Optional 0.44~3.84 2 Optional 3.84~6.49 3 Optional 6.49~12.95 4 Reserved treated as class 0 and reserved for future use It is impossible for a compatible PD to provide a class 4 signal

Chapter 19 Routing Protocol

19.1 RIP

19.1.1 accept-lifetime

Command	**accept-lifetime <start-time> {<end-time>| duration<seconds>| infinite}** **no accept-lifetime** Use this command to specify a key accept on the key chain as a valid time period. The "no accept-lifetime" command deletes this configuration.
Parameter	**<start-time>** parameter specifies the start time of the time period, of which the form should be: **<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}** **<hh:mm:ss>** specify the concrete valid time of accept-lifetime in hours, minutes and second **<day>** specifies the date of valid, ranging between 1 -31 **<month>** specifies the month of valid shown with the first three letters of the month, such as Jan **<year>** specifies the year of valid start, ranging between 1993 - 2035 **<end-time>** specifies the due of the time period, of which the form should be: **<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}<hh:mm:ss>** specify the concrete valid time of accept-lifetime in hours, minutes and second **<day>** specifies the date of valid, ranging between 1 -31 **<month>** specifies the month of valid shown with the first three letters of the month, such as Jan **<year>** specifies the year of valid start, ranging between 1993 - 2035 **<seconds>** the valid period of the key in seconds, ranging between 1-2147483646 **Infinite** means the key will never be out of date.
Default	No default configuration.
Mode	keychain-key Mode。
Usage Guide	If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication

type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.

Example

The example below shows the accept-lifetime configuration of key 1 on the keychain named mychain.

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

19.1.2 clear ip rip route

Command

clear ip rip route {<A.B.C.D/M>|kernel|static|connected|rip|ospf|isis|bgp|all}

Clear specific route in the RIP route table.

Parameter

<A.B.C.D/M> Clear the routes which match the destination address from the RIP route table. Specifies the IP address prefix and its length of the destination address

kernel delete kernel routes from the RIP route table

static delete static routes from the RIP route table

connected delete direct routes from the RIP route table

rip only delete RIP routes from the RIP route table

ospf only delete OSPF routes from the RIP route table

isis only delete ISIS routes from the RIP route table

bgp only delete BGP routes from the RIP route table

all delete all routes from the RIP route table

Default

No default configuration

Mode

Admin mode

Usage Guide

Use this command with the all parameter will delete all learnt route in the RIP route which will be immediately recovered except for rip route. The dynamic learnt RIP route can only be recovered by studying one more time.

Example

```
Switch# clear ip rip route 10.0.0.0/8
Switch# clear ip rip route ospf
```

19.1.3 default-information originate

Command

default-information originate
no default-information originate

Allow the network 0.0.0.0 to be redistributed into the RIP. The "**no default-information originate**" disables this function.

Parameter

-

Default

Disabled

Mode

Router mode and address-family mode

Usage Guide

This command tells the router to insert the default route with the destination of 0.0.0.0 into the RIP routing database, and advertise the route as other routes.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# default-information originate
```

19.1.4 default-metric

Command

default-metric <value>
no default-metric

Set the default metric value of the introduced route. The "**no default-metric**" command restores the default value to 1.

Parameter

<value> is the metric value to be set, ranging between 1~16.

Default

Default route metric value is 1.

Mode

Router mode and address-family mode。

Usage Guide

default-metric command is used for setting the default route metric value of the routes from other routing protocols when distributed into the RIP routes. When using the **redistribute** commands for introducing routes from other protocols, the default route metric value specified by **default-metric** will be adopted if no specific route metric value is set.

Example

Set the default route metric value to 3 for introducing routes from other routing protocols into the RIP routes.

```
Switch(config-router)#default-metric 3
```

19.1.5 distance

Command	**distance <number> [<A.B.C.D/M>] [<access-list-name|access-list-number >]** **no distance [<A.B.C.D/M>]** Set the managing distance with this command. The "**no distance [<A.B.C.D/M>]**" command restores the default value to 120.
Parameter	**<number>** specifies the distance value, ranging from 1 to 255. **<A.B.C.D/M>** specifies the network prefix and its length. **<access-list-name|access-list-number >** specifies the access-list number or name applied.
Default	The default managing distance of RIP is 120.
Mode	Router mode and address-family mode。
Usage Guide	In case there are routes from two different routing protocols to the same destination, the managing distance is then used for selecting routes. The less the managing distance of the route protocol is, the more reliable will be the route acquired from the protocol.
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# distance 8 10.0.0.0/8 mylist

19.1.6 distribute-list

Command	**distribute-list{<access-list-number|access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>]** **no distribute-list{<access-list-number|access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>]** This command uses access-list or prefix-list to filter the route update packets sent and received. The "**no distribute-list {<access-list-number| access-list-name> |prefix<prefix-list-name>} {in|out} [<ifname>]**" command cancels this route filter function.
Parameter	**<access-list-number |access-list-name>** is the name or access-list number to be applied. **<prefix-list-name>** is the name of the prefix-list to be applied. **<ifname>** specifies the name of interface to be applied with route filtering.

Default

The function in default situation is disabled.

Mode

Router mode and address-family mode。

Usage Guide

The filter will be applied to all the interfaces in case no specific interface is set.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# distribute-list prefix myfilter in vlan 1
```

19.1.7 ip rip aggregate-address

Command

ip rip aggregate-address A.B.C.D/M
no ip rip aggregate-address A.B.C.D/M

To configure RIP aggregation route. The no form of this command will delete this configuration.

Parameter

A.B.C.D/M:IPv4 address and mask length.

Default

Disabled.

Mode

Router Mode or Interface Configuration Mode.

Usage Guide

If to configure aggregation route under router mode, RIP protocol must be enabled. If configured under interface configuration mode, RIP protocol may not be enabled, but the aggregation router can operation after the RIP protocol be enabled on interface.

Example

To configure aggregation route as 192.168.20.0/22 globally.

```
Switch(config)#router rip
Switch(config-router)#ip rip agg 192.168.20.0/22
```

19.1.8 ip rip authentication key-chain

Command

ip rip authentication key-chain <name-of-chain>
no ip rip authentication key-chain

Use this command to enable RIPV2 authentication on an interface and further configures the adopted key chain. The "**no ip rip authentication key-chain**" command cancels the authentication.

Parameter

<name-of-chain> is the name of the adopted key chain. There may be spaces in the string. The input ends with an enter and the string should not be longer than 256 bytes.

Default

Not configured.

Mode

Interface Configuration Mode.

Usage Guide

If the authentication is only configured without configuring the key chain or password used by the interface, the authentication does no effect. If mode has not been configured prior to configuring this command, the mode will be set to plaintext authentication. The "no ip rip authentication key" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode.

Example

```
Switch#config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip authentication key-chain my key
```

19.1.9 ip rip authentication mode

Command

ip rip authentication mode {text|md5}
no ip rip authentication mode {text|md5}

Configure the authentication mode; the "**no ip rip authentication mode {ext|md5}**" command restores the default authentication mode namely text authentication mode.

Parameter

text means text authentication;
md5 means MD5 authentication.

Default

Not configured authentication.

Mode

Interface Configuration Mode.

Usage Guide

RIP-I do not support authentication which the RIP-II supports two authentication modes:

text authentication (i.e. Simple authentication) and data packet authentication (i.e. MD5 authentication). This command should be used associating the ip rip authentication key or ip rip authentication string. Independently configuration will not lead to authentication process.

Example

```
Switch#config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip authentication mode md5
```

19.1.10 ip rip authentication string

Command

```
ip rip authentication string <text>
no ip rip authentication string
```

Set the password used in RIP authentication. The "no ip rip authentication string" cancels the authentication.

Parameter

<text> is the password used in authentication of which the length should be 1-16 characters with space available. The password should end with enter.

Default

-

Mode

Interface mode

Usage Guide

The ip rip authentication key will not be able to be configured when this command is configured, key id value is required in MD5 authentication which is 1 when use this command. The mode will be set to plaintext authentication in case no mode configuration is available. The "no ip rip authentication string" command will cancel the authentication which only cancels the authentication process when sending or receiving data packet other than set non authentication mode. Input ip rip authentication string aaa aaa to set the password as aaa aaa which is 7 characters.

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip authentication string guest
```

19.1.11 ip rip authentication cisco-compatible

Command	**ip rip authentication cisco-compatible** **no ip rip authentication cisco-compatible** After configured this command, the cisco RIP packets will be receivable by configuring the plaintext authentication or MD5 authentication
Parameter	-
Default	Not configured
Mode	Interface mode
Usage Guide	After authentication is configured on the cisco router, the RIP packets will exceeds the length of the defined standard length of the protocol once the number of route items is greater than 25. By configuring this command the over-lengthen RIP packets will be receivable other than denied.
Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip authentication cisco-compatible

19.1.12 ip rip receive-packet

Command	**ip rip receive-packet** **no ip rip receive-packet** Set the interface to be able to receivable RIP packets; the "**no ip rip receive-packet**" command sets the interface to be unable to receivable RIP packets.
Parameter	-
Default	Interface receives RIP packets.
Mode	Interface Configuration Mode.
Usage Guide	-
Example	Switch# config terminal Switch(config)# interface vlan 1 Switch(config-if-vlan1)# ip rip receive-packet

19.1.13 ip rip receive version

Command

ip rip receive version { 1 | 2|1 2 }

no ip rip receive version

Set the version information of the RIP packets the interface receives. The default version is 2; the "**no ip rip receive version**" command restores the value set by using the version command.

Parameter

1 and **2** respectively stands for RIP version 1 and RIP version 2,

1 2 stands for the RIP versions 1, 2.

Default

Version 2 。

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip receive version 1 2
```

19.1.14 ip rip send-packet

Command

ip rip send-packet

no ip rip send-packet

Set the Interface to be able to receive the RIP packets; the "**no ip rip send-packet**" sets the interface to be unable to receive the RIP packets.

Parameter

-

Default

Interface sends RIP packets.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip send-packet
```

19.1.15 ip rip send version

Command

ip rip send version { 1 | 2 | 1-compatible | 1 2}

no ip rip send version

Set the version information of the RIP packets the interface receives. The default version is 2; the “**no ip rip send version**” command restores the value set by using the version command.

Parameter

1 and **2** respectively stands for RIP version 1 and RIP version 2,

1 2 stands for the RIP versions 1, 2.

Default

Version 2 。

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan1)# ip rip send version 1
```

19.1.16 ip rip split-horizon

Command

ip rip split-horizon [poisoned]

no ip rip split-horizon

Enable split horizon. The “**no ip rip split-horizon**” disables the split horizon.

Parameter

[poisoned] means configure the split horizon with poison reverse.

Default

Split Horizon with poison reverse by default.

Mode

Interface Configuration Mode.

Usage Guide

The split horizon is for preventing the Routing Loops, namely preventing the layer 3 switches from broadcasting the routes which is learnt from the same interface on which the route to be broadcasted.

Example

```
Switch# config terminal
Switch(config)# interface vlan 1
Switch(Config-if-Vlan1)# ip rip split-horizon poisoned
```

19.1.17 key

Command

key <keyid>
no key <keyid>

This command is for managing and adding keys in the key chain. The "**no key <keyid>**" command deletes one key.

Parameter

<keyid>is key ID, ranging between 0-2147483647.

Default

-

Mode

keychainMode and keychain-keyMode。

Usage Guide

The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example

```
Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#key 1
Switch(config-keychain-key)#
```

19.1.18 key chain

Command

key chain <name-of-chain>
no key chain < name-of-chain >

This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < name-of-chain >**" deletes one keychain.

Parameter

<name-of-chain>is the name string of the keychain the length of which is not specifically limited.

Default

-

Mode

Global Mode

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#key chain mychain
Switch(config-keychain)#
```

19.1.19 key-string

Command

key-string <text>

no key-string <text>

Configure a password corresponding to a key. The "**no key-string <text>**"command deletes the corresponding password.

Parameter

<text> is a character string without length limit. However when referred by RIP authentication only the first 16 characters will be used.

Default

-

Mode

keychain-key Mode ◦

Usage Guide

This command is for configure different passwords for keys with different ID.

Example

```
Switch# config terminal
  Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string prime
```

19.1.20 maximum-prefix

Command

maximum-prefix <maximum-prefix> [<threshold>]

no maximum-prefix

Configure the maximum number of RIP routes in the route table. The "**nomaximum-prefix**" command cancels the limit.

Parameter

<maximum-prefix>the maximum number of RIP route, ranging between 1-65535; a warning is given when the number rate of current route exceeds **<threshold>**ranging between 1-100, default at 75.

Default

-

Mode

router mode

Usage Guide

The maximum RIP route only limits the number of routes learnt through RIP but not includes direct route or the RIP static route configured by the route command. The base on which the comparison is performed is the number of route marked R in the show ip route database, and also the number of RIP routes displayed in the show ip route statistics command.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# maximum-prefix 150
```

19.1.21 neighbor

Command

neighbor <A.B.C.D>

no neighbor <A.B.C.D>

Specify the destination address requires targeted-peer sending. The "**no neighbor <A.B.C.D>**" command cancels the specified address and restores all gateways to trustable.

Parameter

<A.B.C.D>is the specified destination address for the sending, shown in dotted decimal notation.

Default

Not sending to any targeted-peer destination address.

Mode

router mode

Usage Guide

When used accompany with passive-interface command it can be configured to only sending routing messages to specific neighbor.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# neighbor 1.1.1.1
```

19.1.22 network

Command

network <A.B.C.C/M|ifname>

no network <A.B.C.C/M|ifname>

Configure the RIP protocol network.

Parameter

<A.B.C.C/M|>is the IP address prefix and its length in the network.

<ifname> is the name of a interface.

Default

Not running RIP protocol

Mode

Router mode and address-family mode。

Usage Guide

Use this command to configure the network for sending or receiving RIP update packets. If the network is not configured, all interfaces of the network will not be able to send or receive data packets.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0/8
Switch(config-router)# network vlan 1
```

19.1.23 offset-list

Command

offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]
no offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]

Add an offset value to the metric value of the routes learnt by RIP. The "**no offset-list <access-list-number |access-list-name> {in|out} <number > [<ifname>]**" command disables this function.

Parameter

< access-list-number |access-list-name>is the access-list or name to be applied
<number >is the added offset value, ranging between 0-16;
<ifname>is the specific interface name;

Default

Default offset value is the metric value defined by the system.

Mode

Router mode and address-family mode。

Usage Guide

-

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# offset-list 1 in 5 vlan 1
```

19.1.24 passive-interface

Command	**passive-interface <ifname>** **no passive-interface <ifname>** Set the RIP layer 3 switch blocks RIP broadcast on specified interface, on which the RIP data packets will only be sent to layer 3 switches configured with neighbor.
Parameter	**<ifname>** is the name of specific interface.
Default	Not configured
Mode	router mode
Usage Guide	-
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# passive-interface vlan 1

19.1.25 recv-buffer-size

Command	**recv-buffer-size<size>** **no recv-buffer-size** This command configures the size of UDP receiving buffer zone of RIP; the "**no recv-buffer-size**" command restores the system default.
Parameter	**<size>**is the buffer zone size in bytes, ranging between 8192-2147483647.
Default	8192 bytes.
Mode	router mode
Usage Guide	-
Example	Switch# config terminal Switch(config)# router rip Switch(config-router)# recv-buffer-size 23456789

19.1.26 redistribute

Command

redistribute {kernel |connected| static| ospf [<process-id>]| isis| bgp} [metric<value>] [route-map<word>]

no redistribute {kernel |connected| static| ospf [<process-id>]| isis| bgp} [metric<value>] [route-map<word>]

Introduce the routes learnt from other routing protocols into RIP.

Parameter

kernel introduce from kernel routes;

connected introduce from direct routes;

static introduce from static routes;

ospf introduce from OSPF routes. process-id is OSPF process ID, if there is no parameter that means the process by default, range between 1 to 65535;

isis introduce from ISIS routes;

bgp introduce from BGP routes;

<value> is the metric value assigned to the introduced route, ranging between 0 to 16;

<word> is the probe pointing to the route map for introducing routes.

Default

-

Mode

Router mode and address-family mode。

Usage Guide

Under the address-family mode, the parameter kernel and ISIS is unavailable.

Example

```
Switch#config terminal
Switch(config)#router rip
Switch(config-router)#redistribute kernel route-map ipi
```

To redistribute OSPFv2 routing information to RIP.

```
Switch(config)#router rip
Switch(config-router)#redistribute ospf 2
```

19.1.27 route

Command

route <A.B.C.D/M>
no route <A.B.C.D/M>

This command configures a static RIP route. The "**no route <A.B.C.D/M>**"command deletes this route.

Parameter

<A.B.C.D/M>Specifies this destination IP address prefix and its length.

Default

-

Mode

router mode

Usage Guide

The command adds a static RIP route, and is mainly used for debugging. Routes configured by this command will not appear in kernel route table but in the RIP route database.

Example

```
Switch# config terminal
Switch(config)# router rip
Switch(config-router)# route 1.0.0.0/8
```

19.1.28 router rip

Command

router rip
no router rip

Enable the RIP routing process and enter the RIP mode; the "**no router rip**" command closes the RIP routing protocol.

Parameter

-

Default

Not running RIP route.

Mode

Global mode

Usage Guide

This command is the switch for starting the RIP routing protocol which is required to be open before configuring other RIP protocol commands.

Example

Enable the RIP protocol mode

```
Switch(config)#router rip
Switch(config-router)#
```

19.1.29 send-lifetime

Command

send-lifetime <start-time> {<end-time>| duration<seconds>| infinite}

no send-lifetime

Use this command to specify a key on the keychain as the time period of sending keys. The "no send-lifetime" cancels this configuration.

Parameter

<start-time>> parameter specifies the starting time of the time period, which is:**<start-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}**

<hh:mm:ss>Specify the concrete valid time of accept-lifetime in hours, minutes and second；

<day>Specifies the date of valid, ranging between 1 -31；

<month>Specifies the month of valid shown with the first three letters of the month, such as Jan；

<year>Specifies the year of valid start, ranging between 1993 - 2035；

<end-time>Specifies the due of the time period, of which the form should be:

<end-time>={<hh:mm:ss> <month> <day> <year>|<hh:mm:ss> <day> <month> <year>}

<hh:mm:ss>Specify the concrete valid time of **send-lifetime** in hours, minutes and secon；

<seconds>is the valid period of the key in seconding and ranging between 1-2147483646；

infinite means the key will never be out of date.

Default

No default configuration.

Mode

keychain-key Mode。

Usage Guide

If only the authentication mode is configured and the key chain or password used by the interface is not configured, authentication will not work at all. If the mode is not configured before configuring this command, the mode will be set to clear text authentication after configuring this command. The no operation of this command will cancel the authentication, but it does not mean that the mode will be set to the non-authentication type, only that the authentication processing will not be performed when sending or receiving packets. You can enter ip rip authentication key-chain my key to indicate that the key chain name is my key, which is 6 characters in total.

Example

The example below shows the send-lifetime configuration on the keychain named mychain for key 1.

```
Switch# config terminal
Switch(config)# key chain mychain
Switch(config-keychain)# key 1
Switch(config-keychain-key)# send-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

19.1.30 timers basic

Command

timers basic <update> <invalid> <garbage>

no timers basic

Adjust the RIP timer update, timeout, and garbage collecting time. The "**no timers basic**" command restores each parameter to their default values.

Parameter

<update> time interval of sending update packet, shown in seconds and ranging between 5-2147483647;

<invalid> time period after which the RIP route is advertised dead, shown in seconds and ranging between 5-2147483647；

<garbage> is the hold time in which the a route remains in the routing table after advertised dead, shown in seconds and ranging between 5-2147483647.

Default

<update> defaulted at 30；

<invalid> defaulted at 180；

<garbage> defaulted at 120

Mode

router mode

Usage Guide

The system is defaulted broadcasting RIPng update packets every 30 seconds; and the route is considered invalid after 180 seconds but still exists for another 120 seconds before it is deleted from the routing table.

Example

Set the RIP update time to 20 seconds and the timeout period to 80 second, the garbage collecting time to 60 seconds.

```
Switch(Config-Router)#timers basic 20 80 60
```

19.1.31 version

Command

version {1| 2}

no version

Configure the version of all RIP data packets sent/received by router interfaces: the "**no version**" restores the default configuration.

Parameter

1 is version 1 rip;

2 is version 2 rip.

Default

Sent and received data packet is version 2 by default.

Mode

Router mode and address-family mode。

Usage Guide

1 refers to that each interface of the layer 3 switch only sends/receives the RIP-I data packets. 2 refers to that each interface of the layer 3 switch only sends/receives the RIP-II data packets. The RIP-II data packet is the default version.

Example

Configure the version of all RIP data packets sent/received by router interfaces to version 2.

```
Switch(config-router)#version 2
```

19.1.32 show ip protocols rip

Command

show ip protocols rip

Show the RIP process parameter and statistics information.

Parameter

-

Default

-

Mode

Any mode.

Usage Guide

-

Example

```
show ip protocols rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 8 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
```

```
Default redistribution metric is 1
Redistributing: static
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
Vlan1        2    2
Routing for Networks:
Vlan1
Vlan2
Routing Information Sources:
Gateway Distance Last Update Bad Packets Bad Routes
20.1.1.1 120 00:00:31 0 0
```

Displayed information	Explanation
Sending updates every 30 seconds with +/-50%, next due in 8 seconds	Sending update every 30 secs
Timeout after 180 seconds, garbage collect after 120 seconds	The route time-out event period is 180 secs, the garbage collect time is 120 seconds
Outgoing update filter list for all interface is not set	Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set	Incoming update filter list for all interface is not set
Default redistribution metric is 1	Default redistribution metric is 1
Redistributing: static	Redistributing the static route into the RIP route
Default version control: send version 2, receive version 2 Interface Send Recv Key-chain Ethernet1/3 2 2	The configuration of interface receiving and sending packets. Receive version is 2, keychain 1 not configured.
Routing for Networks: Vlan1 Vlan2	The segment running RIP is the Vlan 1 and Vlan 2
Routing Information Sources: Gateway Distance Last Update BadPackets Bad Routes 20.1.1.1 120 00:00:31 0 0	Routing information sourcesThe badpacketand bad routes from the gateway 20.1.1.1 are all 0. 31 seconds have passed since the last route update. The manage distance is 120
Distance: (default is 120)	Default manage distance is 120

19.1.33 show ip rip

Command	show ip rip Show the routes in the RIP route data base.
Parameter	-
Default	-
Mode	Any mode.
Usage Guide	-
Example	show ip rip Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP Network Next Hop Metric From If Time R 12.1.1.0/24 20.1.1.1 2 20.1.1.1 Vlan1 02:51 R 20.1.1.0/24 1 Vlan1 Amongst R stands for RIP route, namely a RIP route with the destination network address 12.1.1.0, the network prefix length as 24, next-hop address at 20.1.1.1. It is learnt from the Ethernet port E1/3 with a metric value of 2, and still has 2 minutes 51 seconds before time out.

19.1.34 show ip rip database

Command	show the routes in the RIP route database.
Parameter	-
Default	-
Mode	Any mode.
Usage Guide	-
Example	Switch# show ip rip database Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP Network Next Hop Metric From If Time R 10.1.1.0/24 1 Vlan1 R 20.1.1.0/24 1 Vlan2

19.1.35 show ip rip interface

Command

show ip rip interface [<ifname>]

Show the RIP related messages.

Parameter

<ifname> is the name of the interface to show the messages.

Default

-

Mode

Any mode.

Usage Guide

-

Example

```
Switch# show ip rip interface vlan 1
Vlan1 is up, line protocol is up
Routing Protocol: RIP
Receive RIP packets
  Send RIP packets
  Passive interface: Disabled
  Split horizon: Enabled with Poisoned Reversed
  IP interface address:
  10.1.1.1/24
```

19.1.36 show ip rip aggregate

Command

show ip rip aggregate

To display the information of IPv4 aggregation route.

Parameter

-

Default

-

Mode

Admin and Configuration Mode.

Usage Guide

This command is used to display which interface the aggregation route be configured, Metric, Count, Suppress and so on. If configured under global mode, then the interface display "----", "Metric" is metric. "Count" is the number of learned aggregation routes. "Suppress" is the times of aggregation.

Example

To display the information of IPv4 aggregation route.

```
Switch(Config-if-Vlan1)#show ip rip agg
Aggregate information of rip
  Network      Aggregated Ifname     Metric   Count   Suppress
192.168.0.0/16     Vlan1                  1        2        0
192.168.4.0/22       ----                 1        2        0
  192.168.4.0/24     ----                 1        1        1
                   Vlan1                  1        1        1
```

Displayed information	Explaination
Network	Route prefix and prefix length.
Aggregated Ifname	To configure the interface name of the aggregation route. If the route aggregated globally, then display "----".
Metric	Metric of aggregation route.
Count	The number of learned aggregation route.
Suppress	The times of aggregated for aggregation route.

19.1.37 show ip rip redistribute

Command

show ip rip redistribute

To display the routing information introduced from external process of RIP.

Parameter

-

Default

Not shown by default.

Mode

Admin Mode and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip rip redistribute
```

19.2 OSPF

19.2.1 area authentication

Command

area <id> authentication [message-digest]

no area <id> authentication

Configure the authentication mode of the OSPF area; the "**no area <id> authentication**" command restores the default value.

Parameter

<id> is the area number which could be shown in digit, ranging from 0 to 4294967295, or in IP address

message-digest is proved by MD5 authentication, or be proved by simple plaintext authentication if not choose this parameter.

Default

No authentication.

Mode

OSPF protocol mode

Usage Guide

Set the authentication mode to plaintext authentication or MD5 authentication. The authentication mode is also configurable under interface mode of which the priority is higher than those in the area. It is required to use **ip ospf authentication-key** to set the password while no authentication mode configured at the interface and the area is plaintext authentication, and use ip ospf message-digest key command to configure MD5 key if is MD5 authentication. The area authentication mode could not affect the authentication mode of the interface in this area.

Example

Set the authentication mode in area 0 to MD5.

Switch(config-router)#area 0 authentication message-digest

19.2.2 area default-cost

Command

area <id> default-cost <cost>

no area <id> default-cost

Configure the cost of sending to the default summary route in stub or NSSA area; the "**no area <id> default-cost**" command restores the default value.

Parameter

<id> is the area number which could be shown as digits 0～4294967295, or as an IP address；

<cost> ranges between <0-16777215>

Default

Default OSPF cost is 1.

Mode

OSPF protocol mode

Usage Guide

The command is only adaptive to the ABR router connected to the stub area or NSSA area.

Example

Set the default-cost of area 1 to 10.

```
Switch(config-router)#area 1 default-cost 10
```

19.2.3 area filter-list

Command

[no] area <id> filter-list {access|prefix} {in|out}

Configure the filter broadcasting summary routing on the ABR; the "**no area <id> filter-list {access|prefix} {in|out}**" command restores the default value.

Parameter

<id>is the area number which could be shown in digits ranging between 0～4294967295, or as an IP address; access-list is appointed for use in access, so is prefix-list for prefix； **<name>** is the name of the filter, the length of which is between 1-256; in means from other areas to this area, out means from this area to other areas.

Default

No filter configured.

Mode

OSPF protocol mode

Usage Guide

This command is used for restraining routes from specific area from spreading between this area and other areas.

Example

Set a filter on the area 1.

```
Switch(config)#access-list 1 deny 172.22.0.0 0.0.0.255
Switch(config)#access-list 1 permit any-source
Switch(config)#router ospf 100
Switch(config-router)#area 1 filter-list access 1 in
```

19.2.4 area nssa

Command

area <id> nssa [TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE |no-summary]

no area <id> nssa[TRANSLATOR| no-redistribution |DEFAULT-ORIGINATE |no-summary]

Set the area to Not-So-Stubby-Area (NSSA) area.

Parameter

<id> is the area number which could be digits ranging between 0~4294967295, and also as an IP address.

TRANLATOR = translator-role {candidate|never|always}, specifies the LSA translation mode for routes: **candidate** means if the router is elected translator, Type 7 LSA can be translated to Type-5 LSA, the default is **candidate**.

never means the router will never translate Type 7 LSA to Type 5 LSA.

always means the route always translate Type 7 LSA to Type 5 LSA.

no-redistribution means never distribute external-LSA to NSSA.

DEFAULT-ORIGINATE=default-information-originate [metric <0-16777214>] [metric-type <1-2>] , generate the Type-7 LSA.

metric <0-16777214> specifies the metric value.

metric-type <1-2> specifies the metric value type of external-LSA , default value is 2.

no-summary shows not injecting area route to the NSSA.

Default

No NSSA area defined by default.

Mode

OSPF protocol mode

Usage Guide

The same area can not be both NSSA and stub at the same time.

Example

Set area 3 to NSSA.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#area 0.0.0.51 nssa
Switch(config-router)#area 3 nssa default-information-originate metric 34 metric-type 2 translator-role candidate no-redistribution
```

19.2.5 area range

Command

area <id> range <address> [advertise| not-advertise| substitute]
no area <id> range <address>

Aggregate OSPF route on the area border. The "**no area <id> range <address>**" cancels this function.

Parameter

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.；
<address>=<A.B.C.D/M>, specifies the area network prefix and its length.；
advertise：Advertise this area, which is the default；
not-advertise ：Not advertise this area；
substitute= substitute <A.B.C.D/M>：advertise this area as another prefix；
<A.B.C.D/M>：Replace the network prefix to be advertised in this area.

Default

Not set.

Mode

OSPF protocol mode

Usage Guide

Use this command to aggregate routes inside an area. If the network IDs in this area are not configured continuously, a summary route can be advertised by configuring this command on ABR. This route consists of all single networks belong to specific range.

Example

```
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 range 192.16.0.0/24
```

19.2.6 area stub

Command

area <id> stub [no-summary]
no area <id> stub [no-summary]

Define an area to a stub area. The "**no area <id> stub [no-summary]**" command cancels this function.

Parameter

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address；
no-summary：The area border routes stop sending link summary announcement to the stub area.

Default

Not defined.

Mode

OSPF protocol mode

Usage Guide

Configure area stub on all routes in the stub area. There are two configuration commands for the routers in the stub area: stub and default-cost. All routers connected to the stub area should be configured with area stub command. As for area border routers connected to the stub area, their introducing cost is defined with area default-cost command.

Example

```
Switch # config terminal
Switch (config)# router ospf 100
Switch (config-router)# area 1 stub
```

19.2.7 area virtual-link

Command

area <id> virtual-link A.B.C.D {AUTHENTICATION|AUTH_KEY|INTERVAL}

no area <id> virtual-link A.B.C.D [AUTHENTICATION|AUTH_KEY|INTERVAL]

Configure a logical link between two backbone areas physically divided by non-backbone area. The "**no area <id> virtual-link A.B.C.D [AUTHENTICATION | AUTH_KEY | INTERVAL]**" command removes this virtual-link.

Parameter

<id> is the area number which could be digits ranging between 0～4294967295, and also as an IP address.

AUTHENTICATION = authentication [message-digest[message-digest-key <1-255> md5 <LINE>] |null|AUTH_KEY].

authentication : Enable authentication on this virtual link.

message-digest：Authentication with MD-5.

null : Overwrite password or packet summary with null authentication.

AUTH_KEY= authentication-key <key>.

<key>: A password consists of less than 8 characters.

INTERVAL= [dead-interval | hello-interval | message-digest-key<1-255>md5<LINE> | retransmit-interval | transmit-delay] <value>.

<value>:>: The delay or interval seconds, ranging between 1~65535.

<dead-interval>: A neighbor is considered offline for certain dead interval without its group messages which the default is 40 seconds.

<hello-interval>: The time interval before the router sends a hello group message, default is 10 seconds.

<message-digest-key>: Authentication key with MD-5.

<retransmit-interval>: The time interval before a router retransmitting a group message, default is 5 seconds.

<transmit-delay>: The time delay before a router sending a group messages, default is 1 second.

Default

No default configuration.

Mode

OSPF protocol mode

Usage Guide

In the OSPF all non-backbone areas will be connected to a backbone area. If the connection to the backbone area is lost, virtual link will repair this connection. You can configure virtual link between any two backbone area routers connected with the public non-backbone area. The protocol treat routers connected by virtual links as a point-to-point network.

Example

```
Switch#config terminal
Switch(config) #router ospf 100
Switch(config-router) #area 1 virtual-link 10.10.11.50 hello 5 dead 20
```

19.2.8 auto-cost reference-bandwidth

Command

auto-cost reference-bandwidth <bandwith>

no auto-cost reference-bandwidth

This command sets the way in which OSPF calculate the default metric value. The "**no auto-cost reference-bandwidth**" command only configures the cost to the interface by types.

Parameter

<bandwith>：reference bandwidth in Mbps, ranging between 1~4294967.

Default

Default bandwidth is 100Mbps.

Mode

OSPF protocol mode

Usage Guide

The interface metric value is acquired by divide the interface bandwith with reference bandwidth. This command is mainly for differentiate high bandwidth links. If several high bandwidth links exist, their cost can be assorted by configuring a larger reference bandwidth value.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#auto-cost reference-bandwidth 50
```

19.2.9 compatible rfc1583

Command	**compatible rfc1583** **no compatible rfc1583** This command configures to rfc1583 compatible. The "**no compatible rfc1583**" command close the compatibility.
Parameter	-
Default	Rfc 2328 compatible by default.
Mode	OSPF protocol mode
Usage Guide	-
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)#compatible rfc1583

19.2.10 clear ip ospf process

Command	**clear ip ospf [<process-id>] process** Use this command to clear and restart OSPF routing processes. One certain OSPF process will be cleared by specifying the process ID, or else all OSPF processes will be cleared.
Parameter	-
Default	No default configuration.
Mode	Admin mode。
Usage Guide	-
Example	Switch#clear ip ospf process

19.2.11 default-information originate

Command

default-information originate [always|METRIC|METRICTYPE|ROUTEMAP]

no default-information originate

This command create a default external route to OSPF route area; the "**no default-information originate**" closes this feature.

Parameter

always：Whether default route exist in the software or not, the default route is always advertised.

METRIC = metric <value>：Set the metric value for creating default route，

<value> ranges between 0~16777214, default metric value is 0.

METRICTYPE = metric-type {1|2}set the OSPF external link type of default route.

1 Set the OSPF external type 1 metric value.

2 Set the OSPF external type 2 metric value.

ROUTEMAP = route-map <WORD>

<WORD> specifies the route map name to be applied.

Default

Default metric value is 10; default OSPF external link type is 2.

Mode

OSPF protocol mode

Usage Guide

When introducing route into OSPF route area with this command, the system will behaves like an ASBR.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-information originate always metric 23 metric-type 2 route-map myinfo
```

19.2.12 default-metric

Command

default-metric <value>

no default-metric

The command set the default metric value of OSPF routing protocol; the "**no default-metric**" returns to the default state.

Parameter

<value>，metric value, ranging between 0~16777214.

Default

Built-in, metric value auto translating.

Mode

OSPF protocol mode

Usage Guide

When the default metric value makes the metric value not compatible, the route introducing still goes through. If the metric value can not be translated, the default value provides alternative option to carry the route introducing on. This command will result in that all introduced route will use the same metric value. This command should be used associating redistribute.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#default-metric 100
```

19.2.13 distance

Command

distance {<value>|ROUTEPARAMETER}

no distance ospf

Configure OSPF manage distance base on route type. The "**no distance ospf**" command restores the default value.

Parameter

<value>，OSPF routing manage distance, ranging between 1~235

ROUTEPARAMETER= ospf {ROUTE1|ROUTE2|ROUTE3}

ROUTE1= external <exernal-distance>, Configure the distance learnt from other routing area.

<exernal-distance> distance value, ranging between 1~255.

ROUTE2= inter-area <inter-distance>，configure the distance value from one area to another area.

<inter-distance> manage distance value, ranging between 1~255.

ROUTE3= intra-area <intra-distance> Configure all distance values in one area. **<intra-distance>** Manage distance value, ranging between 1~255.

Default

Default distance value is 110.

Mode

OSPF protocol mode

Usage Guide

Manage distance shows the reliability of the routing message source. The distance value may range between 1~255. The larger the manage distance value is, the lower is its reliability.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

19.2.14 distribute-list

Command

distribute-list <access-list-name> out {kernel |connected| static| rip| isis| bgp}

no distribute-list out {kernel |connected| static| rip| isis| bgp}

Filter network in the routing update. The "**no distribute-list out {kernel |connected| static| rip| isis| bgp}**" command disables this function.

Parameter

< access-list-name> is the access-list name to be applied.

out: Filter the sent route update.

kernel Kernel route.

connected Direct route；

static Static route；

rip RIP route；

isis ISIS route；

bgp BGP route.

Default

No default configuration.

Mode

OSPF protocol mode

Usage Guide

When distributing route from other routing protocols into the OSPF routing table, we can use this command.

Example

Example below is the advertisement based on the access-list list 1 of the BGP route.

```
Switch#config terminal
Switch(config)#access-list l1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf 100
Switch(config-router)#redistribute rip
Switch(config-router)#distribute-list 1 out rip
```

19.2.15 filter-policy

Command

filter-policy <access-list-name>

no filter-policy

Use access list to filter the route obtained by OSPF, the no command cancels the route filtering.

Parameter

<access-list-name> Access list name will be applied, it can use numeric standard IP access list and naming standard IP access list to configure.

Default No default configuration.

Mode OSPF protocol mode

Usage Guide This command is used to filter the route obtained by OSPF. Do not filter any routes when the specified access list is not exist, for the routes which do not match permit rule of access list, they will be filtered. One access list can be set for this command, only the last configuration takes effect when configuring many times.

Example Use access list 1 to filter the routes which do not belong to 172.10.0.0/16 segment.

```
Switch#config terminal
Switch(config)#access-list 1 permit 172.10.0.0 0.0.255.255
Switch(config)#router ospf
Switch(config-router)#filter-policy 1
```

19.2.16 host area

Command **host <host-address> area <area-id> [cost <cost>]**

no host <host-address> area <area-id> [cost <cost>]

Use this command to set a stub host entire belongs to certain area. The "**[no] host <host-address> area <area-id> [cost <cost>]**" command cancels this configuration.

Parameter **<host-address>** is host IP address show in dotted decimal notation.

<area-id> area ID shown in dotted decimal notation or integer ranging between 0~4294967295.

<cost> specifies the entire cost, which is a integer ranging between 0~65535 and defaulted at 0.

Default No entire set.

Mode OSPF protocol mode

Usage Guide With this command you can advertise certain specific host route out as stub link. Since the stub host belongs to special router in which setting host is not important.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#host 172.16.10.100 area 1
Switch(config-router)#host 172.16.10.101 area 2 cost 10
```

19.2.17 ip ospf authentication

Command

ip ospf [<ip-address>] authentication [message-digest|null]
no ip ospf [<ip-address>] authentication

Specify the authentication mode required in sending and receiving OSPF packets on the interfaces; the "**no ip ospf [<ip-address>] authentication**" command cancels the authentication.

Parameter

<ip-address> is the interface IP address, shown in dotted decimal notation.
message-digest：Use MD5 authentication.
null ：no authentication applied, which resets the password or MD5 authentication applied on the interface.

Default

Authentication not required in receiving OSPF packets on the interface.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf authentication message-digest
```

19.2.18 ip ospf authentication-key

Command

ip ospf [<ip-address>] authentication-key <0 LINE | 7 WORD | LINE>
no ip ospf [<ip-address>] authentication

Specify the authentication key required in sending and receiving OSPF packet on the interface; the no command cancels the authentication key.

Parameter

<ip-address> is the interface IP address shown in dotted decimal notation;
<LINE> specifies authentication key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.

Default

Authentication not required in receiving OSPF packets on the interface.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip ospf authentication-key 0 password
```

19.2.19 ip ospf cost

Command

ip ospf [<ip-address>] cost <cost>
no ip ospf [<ip-address>] cost

Specify the cost required in running OSPF protocol on the interface; the “**no ip ospf [<ip-address>] cost**” command restores the default value.

Parameter

<ip-address> is the interface IP address shown in dotted decimal notation.
<cost > is the cost of OSPF protocol ranging between 1~65535.

Default

Default OSPF cost on the interface is auto-figure out based bandwidth.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf cost 3
```

19.2.20 ip ospf database-filter

Command

ip ospf [<ip-address>] database-filter all out

no ip ospf [<ip-address>] database-filter

The command opens LSA database filter switch on specific interface; the "**no ip ospf [<ip-address>] database-filter**" command closes the filter switch.

Parameter

<ip-address> is the interface IP address shown in dotted decimal notation;

all：All LSAs.

out：Sent LSAs.

Default

Filter switch Closed.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf database-filter all out
```

19.2.21 ip ospf dead-interval

Command

ip ospf [<ip-address>] dead-interval <time >

no ip ospf [<ip-address>] dead-interval

Specify the dead interval for neighboring layer 3 switch; the "**no ip ospf [<ip-address>] dead-interval**" command restores the default value.

Parameter

<ip-address>is the interface IP address shown in dotted decimal notation;

<time > is the dead interval length of the neighboring layer 3 switches, shown in seconds and ranging between 1~65535.

Default

The default dead interval is 40 seconds (normally 4 times of the hello-interval).

Mode

Interface Configuration Mode.

Usage Guide

If no Hello data packet received after the dead-interval period then this layer 3 switch is considered inaccessible and invalid. This command modifies the deadinterval value of neighboring layer 3 switch according to the actual link state. The set dead-interval value is written into the Hello packet and transmitted. To ensure the normal operation of the

OSPF protocol, the dead-interval between adjacent layer 3 switches should be in accordance or at least 4 times of the hello-interval value.

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf dead-interval 80
```

19.2.22 ip ospf disable all

Command

ip ospf disable all

no ip ospf disable all

Stop OSPF group process on the interface.

Parameter

-

Default

- 。

Mode

Interface Configuration Mode.

Usage Guide

This command resets the network area command and stops group process on specific interface.

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf disable all
```

19.2.23 ip ospf hello-interval

Command

ip ospf [<ip-address>] hello-interval <time>

no ip ospf [<ip-address>] hello-interval

Specify the hello-interval on the interface; the "**no ip ospf [<ip-address>] hello-interval**" restores the default value.

Parameter

<ip-address> is the interface IP address shown in dotted decimal notation;

<time>is the interval sending HELLO packet, shown in seconds and ranging between 1～65535.

Default

The hello-interval on the interface is 10 seconds.

Mode

Interface Configuration Mode.

Usage Guide

HELLO data packet is the most common packet which is periodically sent to adjacent layer 3 switch to discover and maintain adjacent relationship, elect DR and BDR. The user set hello-interval value will be written into the HELLO packet and transmitted. The less the hello-interval value is, the sooner the network topological structure is discovered as well larger the cost. The ensure the normal operation of OSPF protocol the hello-interval parameter between the layer 3 switches adjacent to the interface must be in accordance.

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf hello-interval 20
```

19.2.24 ip ospf message-digest-key

Command

ip ospf [<ip-address>] message-digest-key <key_id> MD5 <0 LINE |7 WORD | LINE>
no ip ospf [<ip-address>] message-digest-key <key_id>

Specify the key id and value of MD5 authentication on the interface; the no command restores the default value.

Parameter

<ip-address>is the interface IP address show in dotted decimal notation;
<key_id>ranges between 1-255;
<LINE>is OSPF key. If key option is 0, specify plaintext key. If key option is 7, specify encrypted string. If no option, specify plaintext key by default.

Default

MD5 key is not configured.

Mode

Interface Configuration Mode.

Usage Guide

MD5 key encrypted authentication is used for ensure the safety between the OSPF routers on the network. Same key id and key should be configured between neighbors when using this command, or else no adjacent relationship will not be created.

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf message-digest-key 2 MD5 0 yourpassword
```

19.2.25 ip ospf mtu

Command

ip ospf mtu <mtu>
no ip ospf mtu

Specify the mtu value of the interface as the OSPF group structure according; the "no ip ospf mtu" command restores the default value.

Parameter

<mtu > is the interface mtu value ranging between 576~65535

Default

Use the interface mtu acquired from the kernel.

Mode

Interface Configuration Mode.

Usage Guide

The interface value configured by this command is only used by OSPF protocol other than updated into kernel.

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf mtu 1480
```

19.2.26 ip ospf mtu-ignore

Command

ip ospf <ip-address> mtu-ignore
no ip ospf <ip-address> mtu-ignore

Use this command so that the mtu size is not checked when switching DD; the "**no ip ospf <ip-address> mtu-ignore**" will ensure the mtu size check when performing DD switch.

Parameter

<ip-address>is the interface IP address show in dotted decimal notation.

Default

Check mtu size in DD switch.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf mtu-ignore
```

19.2.27 ip ospf network

Command

ip ospf network {broadcast|non-broadcast|point-to-point|point-to-multipoint}

no ip ospf network

This command configures the OSPF network type of the interface; the "**no ip ospf network**" command restores the default value.

Parameter

broadcast：Set the OSPF network type to broadcast.

non-broadcast：Set the OSPF network type to NBMA.

point-to-point：Set the OSPF network type to point-to-point.

point-to-multipoint：Set the OSPF network type to point-to-multipoint.

Default

The default OSPF network type is broadcast.

Mode

Interface Configuration Mode.

Usage Guide

-

Example

The configuration below set the OSPF network type of the interface vlan 1 to point-to-point.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf network point-to-point
```

19.2.28 ip ospf priority

Command

ip ospf [<ip-address>] priority <priority>

no ip ospf [<ip-address>] priority

Configure the priority when electing "Defined layer 3 switch" at the interface. The "**no ip ospf [<ip-address>] priority**" command restores the default value.

Parameter

<ip-address>is the interface IP address show in dotted decimal notation.

<priority> is the priority of which the valid value ranges between 0～255.

Default

The default priority when electing DR is 1.

Mode

Interface Configuration Mode.

Usage Guide

When two layer 3 switches connected to the same segments both want to be the

"Defined layer 3 switch", the priority will decide which one should be chosen. Normally the one with higher priority will be elected, or the one with larger router-id number if the priorities are the same. A layer 3 switch with a priority equal to 0 will not be elected as "Defined layer 3 switch" or "Backup Defined layer 3 switch".

Example

Configure the priority of DR electing. Configure the interface vlan 1 to no election right, namely set the priority to 0.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf priority 0
```

19.2.29 ip ospf retransmit-interval

Command

ip ospf [<ip-address>] retransmit-interval <time>
no ip ospf [<ip-address>] retransmit-interval

Specify the retransmit interval of link state announcements between the interface and adjacent layer 3 switches. The "**no ip ospf [<ip-address>] retransmit-interval**" command restores the default value.

Parameter

<ip-address>is the interface IP address show in dotted decimal notation.
<time>is the retransmit interveral of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535.

Default

Default retransmit interval is 5 seconds.

Mode

Interface Configuration Mode.

Usage Guide

When a layer 3 switch transmits LSA to its neighbor, it will maintain the link state announcements till confirm from the object side is received. If the confirm packet is not received within the interval, the LSA will be retransmitted. The retransmit interval must be larger than the time it takes to make a round between two layer 3 switches.

Example

Configure the LSA retransmit interval of interface vlan 1 to 10 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf retransmit-interval 10
```

19.2.30 ip ospf transmit-delay

Command

ip ospf [<ip-address>] transmit-delay <time>

no ip ospf [<ip-address>] transmit-delay

Set the transmit delay value of LSA transmitting; the "**no ip ospf [<ip-address>] transmit-delay**" restores the default value.

Parameter

<ip-address>is the interface IP address show in dotted decimal notation.

<time>is the transmit delay value of link state announcements between the interface and adjacent layer 3 switches, shown in seconds ang raning between 1～65535.

Default

Default transmit delay value of link state announcements is 1 second.

Mode

Interface Configuration Mode.

Usage Guide

The LSA ages with time in the layer 3 switches, but not in the network transmitting process. By adding the transit-delay prior to sending the LSA, the LSA will be sent before aged.

Example

Set the LSA transmit delay of interface vlan1 to 3 seconds.

```
Switch#config terminal
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip ospf transmit-delay 3
```

19.2.31 key

Command

key <keyid>

no key <keyid>

This command is for managing and adding keys in the key chain. The "**no key <keyid>**" command deletes one key.

Parameter

<keyid>is key ID, ranging between 0-2147483647.

Default

-。

Mode

keychainMode and keychain-keyMode。

Usage Guide

The command permits entering the keychain-key mode and set the passwords corresponding to the keys.

Example

```
Switch#config terminal
```

	Switch(config)#key chain mychain Switch(config-keychain)#key 1 Switch(config-keychain-key)#

19.2.32 key chain

Command	**key chain <name-of-chain>** **no key chain < name-of-chain >** This command is for entering a keychain manage mode and configure a keychain. The "**no key chain < name-of-chain >**" command deletes one keychain.
Parameter	**<name-of-chain>**is the name string of the keychain the length of which is not specifically limited.
Default	-。
Mode	Global Mode and keychain Mode。
Usage Guide	-
Example	Switch#config terminal Switch(config)#key chain mychain Switch(config-keychain)#

19.2.33 log-adjacency-changes detail

Command	**log-adjacency-changes detail** **no log-adjacency-changes detail** Configure to keep a log for OSPF adjacency changes or not.
Parameter	-
Default	Don't I keep a log for OSPF adjacency changes by default.
Mode	OSPF Protocol Configuration Mode
Usage Guide	When this command is configured, the OSPF adjacency changes information will be recorded into a log.
Example	Switch#config terminal Switch(config)#router ospf 100 Switch(config-router)# log-adjacency-changes detail

19.2.34 max-concurrent-dd

Command

max-concurrent-dd <value>
no max-concurrent-dd

This command set the maximum concurrent number of dd in the OSPF process; the "no max-concurrent-dd" command restores the default.

Parameter

<value>ranges between **<1-65535>**, which is the capacity of processing the concurrent dd data packet.

Default

Not set, no concurrent dd limit.

Mode

OSPF protocol mode

Usage Guide

Specify the max concurrent number of dd in the OSPF process.

Example

Set the max concurrent dd to 20.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#max-concurrent-dd 20
```

19.2.35 neighbor

Command

neighbor A.B.C.D [<cost>| priority <value> | poll-interval <value>]
no neighbor A.B.C.D [<cost>| priority <value> | poll-interval <value>]

This command configures the OSPF router connecting NBMA network. The "**no neighbor A.B.C.D [<cost>| priority <value> | poll-interval <value>]**" command removes this configuration.

Parameter

<cost>, OSPF neighbor cost value ranging between 1-65535；
priority <value> , neighbor priority defaulted at 0 and ranges between 0-255；
poll-interval <value>, 120s by default, which the polling time before neighbor relationship come into shape , ranging between 1-65535.

Default

No default configuration.

Mode

OSPF protocol mode

Usage Guide

Use this command on NBMA network to configure neighbor manually. Every known non-broadcasting neighbor router should be configured with a neighbor entry. The configured neighbor address should be the main address of the interface. The poll-interval should be much larger than the hello-interval.

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
Switch(config-router)#neighbor 1.2.3.4 cost 15
```

19.2.36 network area

Command

network NETWORKADDRESS area <area-id>

no network NETWORKADDRESS area <area-id>

This command enables OSPF routing function one the interface with IP address matched with the network address. The "**no network NETWORKADDRESS area <area-id>**" command removes the configuration and stop OSPF on corresponding interface.

Parameter

NETWORKADDRESS = A.B.C.D/M | A.B.C.D X.Y.Z.W, Shown with the network address prefix or the mask. Wildcast mask if shown in mask;

<area-id>is the ip address or area number shown in point divided demical system, if shown in demcial integer, it ranges between 0~4294967295.

Default

No default configuration

Mode

OSPF protocol mode

Usage Guide

When certain segment belongs to certain area, interface the segment belongs will be in this area, starting hello and database interaction with the connected neighbor.

Example

Configuration 10.1.1.0/24 is in area 1.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#network 10.1.1.0/24 area 1
```

19.2.37 ospf abr-type

Command

ospf abr-type {cisco|ibm|shortcut|standard}

no ospf abr-type

Use this command to configure an OSPF ABR type. The "**no ospf abr-type**" command restores the default value.

Parameter

cisco , Realize through cisco ABR;

ibm , Realize through ibm ABR;

shortcut , Specify a shortcut-ABR;

standard , Realize with standard(RFC2328)ABR.

Default

Cisco by default.

Mode

OSPF protocol mode

Usage Guide

For Specifying the realizing type of abr. This command is good for interactive operation among different OSPF realizing method and is especially useful in the multiple host environment.

Example

Configure abr as standard.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#ospf abr-type standard
```

19.2.38 ospf router-id

Command

ospf router-id <address>

no ospf router-id

Specify a router ID for the OSPF process. The "**no ospf router-id**" command cancels the ID number.

Parameter

<address> , IPv4 address format of router-id.

Default

No default configuration

Mode

OSPF protocol mode

Usage Guide

The new router-id takes effect immediately.

Example

Configure router-id of ospf 100 to 2.3.4.5.

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#ospf router-id 2.3.4.5
```

19.2.39 overflow database

Command

overflow database <maxdbsize > [{hard|soft}]

no overflow database

This command is for configuring the max LSA number. The "no overflow database" command cancels the limit.

Parameter

< maxdbsize > Max LSA numbers, ranging between 0~4294967294.

soft：Soft limit, warns when border exceeded.

hard：Hard limit, directly close ospf instance when border exceeded.

If there is not soft or hard configured, the configuration is taken as hard limit.

Default

Not configured

Mode

OSPF protocol mode

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database 10000 soft
```

19.2.40 overflow database external

Command

overflow database external [<maxdbsize > <maxtime>]

no overflow database external [<maxdbsize > <maxtime>]

The command is for configuring the size of external link database and the waiting time before the route exits overflow state. The "**no overflow database external [<maxdbsize > <maxtime>]**" restores the default value.

Parameter

< maxdbsize > size of external link database, ranging between 0~4294967294, defaulted at 4294967294.

< maxtime > the seconds the router has to wait before exiting the database overflow, ranging between 0~65535.

Default

-

Mode

OSPF protocol mode

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#overflow database external 5 3
```

19.2.41 passive-interface

Command

passive-interface<ifname> [<ip-address>]

no passive-interface<ifname> [<ip-address>]

Configure that the hello group not sent on specific interfaces. The "**no passive-interface <ifname> [<ip-address>]**"command cancels this function.

Parameter

<ifname> is the specific name of interface.

<ip-address> IP address of the interface in dotted decimal format.

Default

Not configured

Mode

OSPF protocol mode

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#passive-interface vlan1
```

19.2.42 redistribute

Command

redistribute {kernel |connected| static| rip| isis| bgp} [metric<value>] [metric-type {1|2}][route-map<word>][tag<tag-value>]

no redistribute {kernel |connected| static| rip| isis| bgp} [metric<value>] [metric-type {1|2}][route-map<word>][tag<tag-value>]

Introduce route learnt from other routing protocols into OSPF.

Parameter

kernel introduce from kernel route.

connected introduce from direct route.

static introduce from static route.

rip introduce from the RIP route.

isis introduce from ISIS route.

bgp introduce from BGP route.

metric <value> is the introduced metric value, ranging between 0-16777214.

metric-type {1|2} is the metric value type of the introduced external route, which can be 1 or 2, and it is 2 by default.

route-map <word> point to the probe of the route map for introducing route.

tag<tag-value> external identification number of the external route, ranging between 0~4294967295, defaulted at 0.

Default

-

Mode

OSPF protocol mode

Usage Guide

Learn and introduce other routing protocol into OSPF area to generate AS-external_LSAs.

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#redistribute bgp metric 12
```

19.2.43 redistribute ospf

Command

redistribute ospf [<process-id>] [metric<value>] [metric-type {1|2}][route-map<word>]

no redistribute ospf [<process-id>] [metric<value>] [metric-type {1|2}] [route-map<word>]

To redistribute of process ID routing to this process. The no form of command deletes the redistribution of process ID routing to this process. When input the optional parameters of metric, metric type and routermap, then restores default configuration.

Parameter

process-id is OSPF process ID, 0 by default.

metric <value> is the metric for redistributed routing, range between 0 to 16777214.

metric-type {1|2} is the metric type for redistributed routing, only can be 1 or 2, and 2 by default.

route-map <word> is the pointer to the introduced routing map.

Default

Not redistributed any OSPF routing by default.

Mode

OSPF protocol mode

Usage Guide

When process-id is not input, that means OSPF routing will be redistributed by default (Process-id is 0).

Example

```
Switch(config-router)#redistribute ospf
```

19.2.44 router ospf

Command

router ospf <process_id>

no router ospf <process_id>

This command is for relating the OSPF process.

Parameter

<process_id> specifies the ID of the OSPF process to be created, the ranging from 1 to 65535.

Default

-

Mode

Global Mode。

Usage Guide

-

Example

```
Switch#config terminal
Switch(config)#router ospf 100
Switch(config-router)#network 10.1.1.0/24 area 0
```

19.2.45 summary-address

Command

summary-address <A.B.C.D/M> [{not-advertise|tag<tag-value>}]

Summarize or restrain external route with specific address scope.

Parameter

<A.B.C.D/M> address scope, shown in dotted decimal notation IPv4 address plus mask length.

not-advertised restrain the external routes.

tag<tag-value> is the identification label of the external routes, which ranges between 0~4294967295, and is defaulted at 0.

Default

-

Mode

OSPF protocol mode

Usage Guide

When routes are introduced into OSPF from other routing protocols, it is required to advertise every route in a external LSA. This command is for advertise one summary route for those introduced routes contained in specific network address and masks, which could greatly reduces the size of the link state database.

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#summary-address 172.16.0.0/16 tag 3
```

19.2.46 timers spf

Command

timers spf <spf-delay> <spf-holdtime>

no timers spf

Adjust the value of the route calculating timer. The "**no timers spf**" command restores relevant values to default.

Parameter

<spf-delay> 5 seconds by default.

<spf-holdtime> 10 seconds by default.

Default

-

Mode

OSPF protocol mode

Usage Guide

This command configures the delay time between receiving topology change and SPF calculation, further configured the hold item between two discontinuous SPF calculation.

Example

```
Switch#config terminal
Switch(config)#router ospf
Switch(config-router)#timers spf 5 10
```

19.2.47 show ip ospf

Command

show ip ospf [<process-id>]

Display OSPF main messages.

Parameter

<process-id> is the process ID, ranging between 0~65535.

Default

Not displayed

Mode

Admin and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip ospf
Routing Process "ospf 0" with ID 192.168.1.1
Process bound to VRF default
Process uptime is 2 days 0 hour 30 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
  Area 0 (BACKBONE) (Inactive)
  Number of interfaces in this area is 0(0)
  Number of fully adjacent neighbors in this area is 0
  Area has message digest authentication
  SPF algorithm executed 0 times
  Number of LSA 0. Checksum Sum 0x000000

Routing Process "ospf 10" with ID 0.0.0.0
Process bound to VRF test
Process uptime is 4 days 23 hours 51 minutes
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 1
  Area 0 (BACKBONE) (Inactive)
  Number of interfaces in this area is 0(0)
  Number of fully adjacent neighbors in this area is 0
  Area has no authentication
  SPF algorithm executed 0 times
  Number of LSA 0. Checksum Sum 0x000000
```

19.2.48 show ip ospf border-routers

Command

show ip ospf [<process-id>] border-routers

Display the intra-domain route entries for the switch to reach ABR and ASBR of all instances.

Parameter

<process-id> is the process ID, ranging between 0~65535.

Default

Not displayed

Mode

Admin and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip ospf border-routers
OSPF process 0 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, Vlan1, ASBR, Area 0.0.0.0
i 172.16.10.1 [10] via 10.10.11.50, Vlan2, ABR, ASBR, Area 0.0.0.0
```

19.2.49 show ip ospf database

Command

show ip ospf [<process-id>] database[{adv-router [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|asbr-summary[{<linkstate_id> |self-originate |adv-router <advertiser_router>}] |externel [{<linkstate_id>| self-originate |adv-router <advertiser_router>}] |network [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|nssa-external [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|opaque-area [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|opaque-as [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|opaque-link [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|router [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|summary [{<linkstate_id>|self-originate |adv-router <advertiser_router>}]|self-originate | max-age }]

Display the OSPF link state data base messages.

Parameter

<process-id> is the process ID, ranging between 0~65535

<linkstate_id> Link state ID, shown in point divided demical system

<advertiser_router> is the ID of Advertising router, shown in point divided demcial IP address forma

Default

Not displayed

Mode

Admin and Configuration Mode.

Usage Guide

According to the output messages of this command, we can view the OSPF link state database messages.

Example

```
Switch#show ip ospf database
  Router Link States (Area 0.0.0.2)
Link ID ADV Router Age Seq# CkSum Link count
192.168.1.2 192.168.1.2 254 0x80000031 0xec21 1
192.168.1.3 192.168.1.3 236 0x80000033 0x0521 2

  Net Link States (Area 0.0.0.2)
Link ID ADV Router Age Seq# CkSum
20.1.1.2 192.168.1.2 254 0x8000002b 0xece4

  Summary Link States (Area 0.0.0.2)
Link ID ADV Router Age Seq# CkSum Route
6.1.0.0 192.168.1.2 68 0x8000002b 0x5757 6.1.0.0/22
6.1.1.0 192.168.1.2 879 0x8000002a 0xf8bc 6.1.1.0/24
22.1.1.0 192.168.1.2 308 0x8000000c 0xc8f0 22.1.1.0/24

  ASBR-Summary Link States (Area 0.0.0.2)
Link ID ADV Router Age Seq# CkSum
192.168.1.1 192.168.1.2 1702 0x8000002a 0x89c7

  AS External Link States
Link ID ADV Router Age Seq# CkSum Route
2.2.2.0 192.168.1.1 1499 0x80000056 0x3a63 E2 2.2.2.0/24 [0x0]
2.2.3.0 192.168.1.1 1103 0x8000002b 0x0ec3 E2 2.2.3.0/24 [0x0]
```

19.2.50 show ip ospf interface

Command	**show ip ospf interface <interface>** Display the OSPF interface messages.
Parameter	**<interface>** is the name of interface
Default	Not displayed
Mode	Admin and Configuration Mode.
Usage Guide	-

Example

```
Switch#show ip ospf interface
Loopback is up, line protocol is up
  OSPF not enabled on this interface
Vlan1 is up, line protocol is up
  Internet Address 10.10.10.50/24, Area 0.0.0.0
  Process ID 0, Router ID 10.10.11.50, Network Type BROADCAST, Cost: 10
  Transmit Delay is 5 sec, State Waiting, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 35, Dead 35, Wait 35, Retransmit 5
  Hello due in 00:00:16
Neighbor Count is 0, Adjacent neighbor count is 0
```

19.2.51 show ip ospf neighbor

Command

show ip ospf [<process-id>] neighbor [{<neighbor_id> |all |detail [all] |interface<ifaddress>}]

Display the OSPF adjacent point messages.

Parameter

<process-id> is the process ID ranging between 0~65535

<neighbor_id> is the dotted decimal notation neighbor ID

all：Display messages of all neighbors

detail：Display detailed messages of all neighbors

<ifaddress> Interface IP address

Default

Not displayed

Mode

Admin and Configuration Mode.

Usage Guide

OSPF neighbor state can be checked by viewing the output of this command.

Example

```
Switch#show ip ospf neighbor
OSPF process 0:
Neighbor ID Pri State Dead Time Address Interface
192.168.1.1 1 Full/Backup 00:00:32 6.1.1.1 Vlan1
192.168.1.3 1 Full/DR 00:00:36 20.1.1.3 Vlan2
192.168.1.3 1 Full/ - 00:00:30 20.1.1.3 VLINK2
```

Displayed information	Explanation
Neighbor ID	ID Neighbor ID
Priority	Priority
State	Neighbor relation state
Dead time	Neighbor dead time
Address	Interface Address
Interface	Interface name

19.2.52 show ip ospf redistribute

Command

show ip ospf [<process-id>] redistribute

To display the routing message redistributed from external process of OSPF.

Parameter

<process-id> is the process ID ranging between 0~65535.

Default

-

Mode

Admin Mode and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip ospf redistribute
ospf process 1 redistribute information：
ospf process 2
ospf process 3
bgp
ospf process 2 redistribute information：
ospf process 1
bgp
ospf process 3 redistribute information：
ospf process 1
bgp
Switch#show ip ospf 2 redistribute
ospf process 2 redistribute information：
ospf process 1
bgp
```

19.2.53 show ip ospf route

Command	**show ip ospf [<process-id>] route** Display the OSPF routing table messages.
Parameter	**<process-id>** is the process ID ranging between 0~65535
Default	-
Mode	Admin and Configuration Mode.
Usage Guide	-

Example

```
Switch#show ip ospf route
O 10.1.1.0/24 [10] is directly connected, Vlan1, Area 0.0.0.0
O 10.1.1.4/32 [10] via 10.1.1.4, Vlan1, Area 0.0.0.0
IA 11.1.1.0/24 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 11.1.1.2/32 [20] via 10.1.1.1, Vlan1, Area 0.0.0.0
IA 12.1.1.0/24 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
IA 12.1.1.2/32 [20] via 10.1.1.2, Vlan1, Area 0.0.0.0
O 13.1.1.0/24 [10] is directly connected, Vlan4, Area 0.0.0.3
O 14.1.1.0/24 [10] is directly connected, Vlan5, Area 0.0.0.4
IA 15.1.1.0/24 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
IA 15.1.1.2/32 [20] via 13.1.1.2, Vlan4, Area 0.0.0.3
E1 100.1.0.0/16 [21] via 10.1.1.1, Vlan1
E1 100.2.0.0/16 [21] via 10.1.1.1, Vlan1
```

19.2.54 show ip ospf virtual-links

Command	**show ip ospf [<process-id>] virtual-links** Display the OSPF virtual link message.
Parameter	**<process-id>** is the process ID ranging between 0~65535.
Default	-
Mode	Admin and Configuration Mode.
Usage Guide	-

Example

```
Switch#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface Vlan1
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in inactive
  Adjacency state Down
```

19.2.55 show ip route process-detail

Command

show ip route [database] process-detail

Display the IP routing table with specific process ID or Tag.

Parameter

The parameter of **database** means displaying all the routers, no parameter means only displaying effective routers.

Default

Not importing any router of OSPF process by default.

Mode

Admin and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip route database process-detail
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
  O - OSPF, IA - OSPF inter area
  N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
  E1 - OSPF external type 1, E2 - OSPF external type 2
  i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
  > - selected route, * - FIB route, p - stale info
C *> 127.0.0.0/8 is directly connected, Loopback
O 192.168.2.0/24 [110/10] is directly connected, Vlan2, 00:06:13,process 12
C *> 192.168.2.0/24 is directly connected, Vlan2
```

19.2.56 show ip protocols

Command

show ip protocols

Display the running routing protocol messages.

Parameter

Default

-

Mode

Admin and Configuration Mode.

Usage Guide

-

Example

```
Switch#show ip protocols
```

Use “show ip protocols” command will show the messages of the routing protocol running on current layer 3 switch

For example, the displayed messages are:

```
Routing Protocol is "ospf 0"
 Invalid after 0 seconds, hold down 0, flushed after 0
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing:
 Routing for Networks:
 10.1.1.0/24
 12.1.1.0/24
 Routing Information Sources:
 Gateway Distance Last Update
 Distance: (default is 110)
 Address Mask Distance List
Routing Protocol is "bgp 0"
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 IGP synchronization is disabled
 Automatic route summarization is disabled
  Neighbor(s):
 Address FiltIn FiltOut DistIn DistOut Weight RouteMap
 Incoming Route Filter:
```