



MGS3750-28F

Layer 2 Management Switch

Version 1.0

Edition 2, 09/2016

CLI Reference Guide

Default Login Details

LAN IP Address	http://192.168.1.1
User Name	admin
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the Switch and access the Web Configurator.

- More Information

Go to **support.zyxel.com** to find other information on the Switch.



Contents Overview

Logging in Ethernet Switch	17
Command Line Interface	21
Manage Users	28
Ethernet Port Configuration	34
Ethernet Port Mirroring Configuration	44
Configuring Port Utilization Alarm	48
Link Aggregation Configuration	50
Port Isolation Configuration	60
VLAN	62
GVRP Configuration	69
ARP Configuration	76
IGMP Snooping	86
GMRP Configuration	97
DHCP Configuration	102
DHCP Snooping	109
DHCP Option 82	114
ACL Configuring	117
Storm-control Configuration	127
QoS Configuration	128
STP Configuration	140
Configuring 802.1X	160
Configuring MSTP	168
Configuring SNTP	188
SSH Terminal Services	193
Configuration File Management	198
BootROM and Host Software Loading	200
Basic System Configuration & Debugging	206
LLDP Configuration	221
PPPoE Plus Configuration	225
CFM Configuration	228
Flex Links Configuration	236
Monitor Link Configuration	243
EFM/OAM Configuration	252
L2TP Configuration	259
QinQ Configuration	261
Stack Configuration	265

Table of Contents

Contents Overview	3
Table of Contents	4
Chapter 1	
Logging in Ethernet Switch	17
1.1 Set up Configuration Environment via Console Port	17
1.2 Set up Configuration Environment through Telnet	19
1.2.1 Connect PC to Ethernet Switch through Telnet	19
1.2.2 Telnet Ethernet Switch through Ethernet Switch	20
Chapter 2	
Command Line Interface	21
2.1 Introduction of Command Line Interface	21
2.2 Command Line Configuration Mode	21
2.3 Feature and Functions of Command Line	24
2.3.1 Help of Command Line	24
2.3.2 Displaying Characteristics of Command Line	25
2.3.3 Show history Command of Command Line	25
2.3.4 Common Command Line Error Messages	26
2.4 Symbols in Command	26
2.5 Parameter in command	26
Chapter 3	
Manage Users	28
3.1 System Default User	28
3.2 User's Account Authentication	28
3.3 Local Authentication Configuration	29
3.3.1 Add Users	29
3.3.2 Change Password	29
3.3.3 Modify User's Privilege Level	30
3.3.4 Delete User	31
3.3.5 Show Users	31
3.4 Remote Authentication Configuration	32
3.4.1 Choose RADIUS as Remote Authentication Server	32
3.4.2 Choose TACACS+ Remote Authentication	32
Chapter 4	
Ethernet Port Configuration	34
4.1 Ethernet Port Overview	34

4.1.1 Link Type of Ethernet Ports	34
4.1.2 Configuring Default VLAN ID for an Ethernet Port	34
4.1.3 Handling Packets	34
4.2 Configure Ethernet Port	35
4.2.1 Basic Ethernet Port Configuration	35
4.2.2 Combo Port	38
4.2.3 Enable/Disable Ingress Filtering	39
4.2.4 Acceptable-Frame Type for Ethernet Port	39
4.2.5 Enable/Disable Flow Control for Ethernet Port	40
4.2.6 Display and Debug Ethernet Port	40
Chapter 5	
Ethernet Port Mirroring Configuration.....	44
5.1 Configure Ethernet Port Mirroring	44
5.1.1 Overview	44
5.1.2 Mirroring	44
5.1.3 Configuring Port Mirroring	45
5.1.4 Mirroring Configuration	45
Chapter 6	
Configuring Port Utilization Alarm.....	48
6.1 Brief Introduction to Device Utilization Alarm	48
6.2 Configuring Device Utilization Alarm	48
6.2.1 Configuring Port Utilization Alarm	48
6.2.2 Configuring CPU Utilization Alarm	49
6.2.3 Displaying and Debugging Device Utilization Alarm	49
Chapter 7	
Link Aggregation Configuration.....	50
7.1 Overview	50
7.1.1 Introduction to Link Aggregation	50
7.1.2 Introduction to LACP	51
7.1.3 Operation Key (O-Key)	51
7.1.4 Static Aggregation Group	51
7.1.5 Dynamic LACP Aggregation Group	52
7.2 Redundancy of Interconnected Device	53
7.3 Load-balancing Policy	53
7.4 Link Aggregation Configuration	53
7.4.1 Configuring a Static Aggregation Group	54
7.4.2 Configuring a Dynamic LACP Aggregation Group	54
7.4.3 Displaying and Maintaining Link Aggregation Configuration	55
7.5 LACP Configuration Example	56

Chapter 8	
Port Isolation Configuration	60
8.1 Introduction to Port Isolation	60
8.2 Port Isolation Configuration	60
8.2.1 Port Isolation Configuration	60
8.3 Port-isolation Configuration Example	61
8.3.1 Port-isolation Configuration Example	61
Chapter 9	
VLAN	62
9.1 VLAN Overview	62
9.2 VLAN Principles	63
9.3 802.1Q VLAN	64
9.3.1 VLAN Link Type of Ethernet Ports	64
9.3.2 Default VLAN	64
9.3.3 Handling Packets	64
9.4 VLAN Configuration	65
9.4.1 Default VLAN Configuration	65
9.4.2 Create and Modify VLAN	65
9.4.3 Configure VLAN Access Port	65
9.4.4 Configure VLAN Trunk Port	66
9.4.5 Configure VLAN Hybrid Port	66
9.4.6 Delete Port Members from a VLAN	67
9.4.7 Delete VLAN	67
9.4.8 VLAN Configuration Example	67
Chapter 10	
GVRP Configuration	69
10.1 Brief Introduction to GVRP	69
10.1.1 GARP	69
10.1.2 GVRP	69
10.2 Configuring GVRP	70
10.2.1 Brief Introduction to GVRP Configuration	70
10.2.2 Port Configuration	70
10.2.3 Startup GVRP	70
10.2.4 Configuring VLAN Forwarded by GVRP	71
10.2.5 Displaying and Debugging	71
10.2.6 GVRP Configuration Examples	71
Chapter 11	
ARP Configuration.....	76
11.1 ARP Overview	76
11.1.1 ARP Function	76

11.1.2 ARP Message Format	77
11.2 Configuring ARP	78
11.2.1 Brief Configuration Guide of ARP	78
11.2.2 ARP Table	78
11.2.3 ARP Peer	79
11.2.4 ARP Overwrite	79
11.2.5 Linkup Gratuitous-ARP	80
11.2.6 ARP-Reply-Repeat	80
11.2.7 ARP Probe	80
11.2.8 ARP Proxy	81
11.3 Configuring ARP Attack Spoofing	81
11.3.1 Brief Introduction to ARP Spoofing	81
11.3.2 ARP Anti-Spoofing Protection	82
11.3.3 Configuring Anti-Spoofing	82
11.3.4 Configuring ARP Packet Source MAC Address Consistency Check	83
11.3.5 Anti-Spoofing Default Configuration Values	83
11.3.6 Displaying and Maintain Anti-Spoofing	84
11.4 Configuring ARP Anti-Flood	84
11.4.1 ARP Flood	84
11.4.2 ARP Anti-Flood	84
11.4.3 Configuring ARP Anti-Flood	85
11.4.4 Displaying and Maintain ARP Anti-Flood	85
Chapter 12	
IGMP Snooping	86
12.1 Brief Introduction to IGMP Snooping	86
12.2 IGMP Snooping Configuration	86
12.2.1 Brief Configuration guide of IGMP Snooping	86
12.2.2 Enable IGMP Snooping	87
12.2.3 Configuring IGMP Snooping Timer	87
12.2.4 Configuring Port Fast-Leave	87
12.2.5 Configuring Number of Multicast Group Allowed Learning	88
12.2.6 Configuring IGMP Snooping Querier	88
12.2.7 Configuring IGMP Snooping Multicast Learning Strategy	89
12.2.8 Configuring IGMP Snooping Router-Port	89
12.2.9 Configuring IGMP Snooping Port Multicast VLAN	90
12.2.10 Configuring Host Port Record MAC Functions	90
12.2.11 Configuring Port of Dropped Query Packets or Not	90
12.2.12 Configuring Port of Discarded Packets Report or Not	91
12.2.13 Configuring Multicast Preview	91
12.2.14 Configuring Profile of Black and White List	91
12.2.15 Displaying and Maintenance of IGMP Snooping	92
12.3 IGMP Snooping Configuration Examples	92

Chapter 13	
GMRP Configuration	97
13.1 Brief Introduction to GMRP	97
13.2 GMRP Configuration	97
13.2.1 Enabling GMRP	97
13.2.2 Add Requisite Static Route Forwarded by GMRP	97
13.2.3 Displaying and Maintain GMRP	98
13.2.4 GMRP Configuring Examples	98
Chapter 14	
DHCP Configuration	102
14.1 DHCP Overview	102
14.2 DHCP IP Address Assignment	102
14.2.1 IP Address Assignment Policy	102
14.2.2 Obtaining IP Addresses Dynamically	103
14.2.3 DHCP Packet Format	104
14.3 DHCP Relay	105
14.3.1 Usage of DHCP Relay	105
14.3.2 DHCP Relay Fundamentals	106
14.4 DHCP Server and Relay Configuration	106
14.4.1 Configure DHCP Server	106
14.4.2 Configure DHCP Address Pool	107
14.4.3 Configure DHCP Relay	107
14.4.4 Display DHCP Server and Relay Configuration	108
Chapter 15	
DHCP Snooping	109
15.1 Introduction to DHCP Snooping	109
15.2 DHCP Snooping Configuration	109
15.3 DHCP-Snooping Security Configuration	110
15.3.1 Configure Max Clients Number	110
15.3.2 Configure IP-Source-Guard	110
15.4 Displaying and Debugging DHCP-Snooping	112
15.5 DHCP-Snooping Configuration Example	112
15.5.1 Network requirements	112
15.5.2 Network diagram	112
15.5.3 Configuration procedure	112
Chapter 16	
DHCP Option 82	114
16.1 Introduction to option 82 supporting	114
16.2 DHCP Option82 Configuration	114
16.2.1 Enable DHCP Option82	114

16.2.2 Displaying and Debugging DHCP Option82	115
16.3 DHCP Option82 Configuration Example	115
Chapter 17	
ACL Configuring.....	117
17.1 Brief Introduction to ACL	117
17.1.1 Matching Order	117
17.1.2 Switch Support ACL	118
17.2 Configuring Time Range	118
17.2.1 Configuration Procedure	118
17.2.2 Configuration Examples	119
17.2.3 Configuring a Basic ACL	120
17.2.4 Configuration Procedure	120
17.2.5 Configuration Examples	120
17.3 Define Extended ACL	121
17.3.1 Configuration Procedure	121
17.3.2 Configuration Procedure	123
17.4 Define Layer 2 ACL	123
17.4.1 Configuring Layer 2 ACL	123
17.4.2 Configuration Examples	124
17.5 Activate ACL	125
17.5.1 Configuration Examples	125
17.5.2 Activate ACL successfully .Active ACL Binding	126
17.6 Displaying and Debugging ACL	126
Chapter 18	
Storm-control Configuration.....	127
18.1 Storm-control Overview	127
18.2 Storm-Control Configuration	127
18.2.1 Configure Storm-Control	127
18.2.2 Storm-control Monitor and Maintenance	127
Chapter 19	
QoS Configuration.....	128
19.1 Brief Introduction to QoS	128
19.1.1 Traffic	128
19.1.2 Traffic Classification	128
19.1.3 Priority	129
19.1.4 Access Control List	131
19.1.5 Packet Filtration	131
19.1.6 Flow Monitor	131
19.1.7 Interface Speed Limitation	131
19.1.8 Redirection	131

19.1.9 Priority Mark	132
19.1.10 Choose Interface Outputting Queue for Packet	132
19.1.11 Queue Scheduler	132
19.1.12 Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol ..	133
19.1.13 Flow Mirror	133
19.1.14 Statistics Based on Flow	133
19.1.15 Copy Packet to CPU	133
19.2 QoS Configuration	133
19.2.1 Configuring Flow Monitor	133
19.2.2 Configure Two Rate Three Color Marker	134
19.2.3 Configuring Interface Line Rate	134
19.2.4 Configuring Packet Redirection	135
19.2.5 Configuring Traffic Copy to CPU	135
19.2.6 Configuring Traffic Priority	135
19.2.7 Configuring Queue-Scheduler	136
19.2.8 Configuring Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol	136
19.2.9 Configuring Mapping Relationship between DSCP and 8 Priority in IEEE 802.1p	137
19.2.10 Configuring Flow Statistic	138
19.2.11 Configuring Flow Mirror	138
19.2.12 Displaying and Maintain QoS	139
Chapter 20	
STP Configuration	140
20.1 STP Overview	140
20.1.1 Function of STP	140
20.1.2 Protocol Packets of STP	140
20.1.3 Basic Concepts in STP	140
20.1.4 Spanning-Tree Interface States	141
20.2 How STP Works	142
20.3 Implement RSTP on Ethernet Switch	147
20.4 Configure RSTP	148
20.4.1 RSTP Configuration Task List	148
20.4.2 Enable RSTP	149
20.4.3 Configure STP Bridge Priority	149
20.4.4 Configure Time Parameter	150
20.4.5 Configure STP Path Cost	150
20.4.6 Configure STP Port Priority	151
20.4.7 Configure STP mcheck	151
20.4.8 Configure STP Point-to-Point Mode	152
20.4.9 Configure STP Portfast	152
20.4.10 Configure STP Transit Limit	152
20.4.11 Root Protection	153

20.4.12 Loop Guard	153
20.4.13 BPDU Guard	153
20.4.14 BPDU Filter	154
20.4.15 RSTP Monitor and Maintenance	154
20.4.16 STP Configuration Example	154
Chapter 21	
Configuring 802.1X	160
21.1 Brief Introduction to 802.1X Configuration	160
21.1.1 Architecture of 802.1X	160
21.1.2 Rule of 802.1x	161
21.1.3 Configuring AAA	162
21.1.4 Configuring RADIUS Server	163
21.1.5 Configuring Local User	163
21.1.6 Configuring Domain	163
21.1.7 Configuring RADIUS Features	164
21.2 Configuring 802.1X	165
21.2.1 Configuring EAP	165
21.2.2 Enable 802.1x	165
21.2.3 Configuring 802.1x Parameters for a Port	166
21.2.4 Configuring Re-Authentication	166
21.2.5 Configuring Watch Feature	166
21.2.6 Configuring User Features	167
Chapter 22	
Configuring MSTP	168
22.1 Brief Introduction to MSTP	168
22.2 BPDU	168
22.2.1 Basic Concepts in MSTP	169
22.2.2 Roles of Ports	171
22.3 Algorithm Implementation	173
22.3.1 MSTP Protocol	173
22.3.2 Determining CIST Priority Vectors	175
22.3.3 Determining the MSTI priority vectors	176
22.3.4 Determining MSTP	176
22.3.5 Active Topology	179
22.3.6 A Topology Change	180
22.3.7 MST and SST Compatibility	180
22.4 Configuring MSTP	181
22.4.1 Configuring MSTP Task	181
22.4.2 Enabling MSTP	182
22.4.3 Configuring MSTP Timer Parameter Values	182
22.4.4 Configuring MSTP Identifier	183

22.4.5 Configuring MSTP Bridge Priority	183
22.4.6 Configuring Port Boundary Port Status	184
22.4.7 Configuring Port Link Type	184
22.4.8 Configuring Path Cost	184
22.4.9 Configuring Port Priority	185
22.4.10 Configuring Root Port Protection	185
22.4.11 Configuring Digest Snooping Port	186
22.4.12 Configuring Port mcheck Function	186
22.4.13 Configuring MSTP Instance Is Enabled	187
22.4.14 Displaying and Maintain MSTP	187
 Chapter 23	
Configuring SNTP	188
23.1 Brief introduction of SNTP	188
23.1.1 SNTP Operation Mechanism	188
23.2 Configuring SNTP Client	188
23.2.1 List of SNTP Client Configuration	188
23.2.2 Enabling SNTP Client	189
23.2.3 Modifying SNTP Client Operating Mode	189
23.2.4 Configuring SNTP Sever Address	190
23.2.5 Modifying Broadcast Transfer Delay	190
23.2.6 Configuring Interval Polling	190
23.2.7 Configuring Overtime Retransmit	190
23.2.8 Configuring Client Summer Time	191
23.2.9 Configuring Valid Servers	191
23.2.10 Configuring MD5 Authentication	192
23.2.11 Displaying and Maintain SNTP Client	192
 Chapter 24	
SSH Terminal Services	193
24.1 Introduction to SSH	193
24.2 SSH Server Configuration	194
24.3 Log in Switch from SSH Client	194
24.4 SSH Server Configuration Example	195
24.4.1 Use Default Key	195
24.4.2 Use Loaded Key	196
 Chapter 25	
Configuration File Management	198
25.1 Introduction to Configuration File	198
25.2 Configuration File-Related Operations	198
 Chapter 26	
BootROM and Host Software Loading	200

26.1 Introduction to Loading Approaches	200
26.2 Local Software Loading	200
26.2.1 Loading Software Using XMODEM through Console Port	201
26.2.2 Loading Software Using TFTP through Ethernet Port	202
26.2.3 Loading Software Using FTP through Ethernet Port	204
26.3 Remote Software Loading	205
26.3.1 Remote Loading Using FTP	205
26.3.2 Remote Loading Using TFTP	205
Chapter 27	
Basic System Configuration & Debugging	206
27.1 Basic System Configuration	206
27.2 SNMP	206
27.2.1 SNMP Overview	206
27.2.2 Configuring SNMP Basic Functions	208
27.2.3 Displaying SNMP	209
27.2.4 SNMP Configuration Example	210
27.3 Network Connectivity Test	211
27.3.1 Ping	211
27.3.2 Tracert	211
27.4 Device Management	211
27.4.1 Device Management Configuration	212
27.4.2 MAC address Table management	212
27.4.3 Restarting the Ethernet Switch	217
27.5 System Maintenance	217
27.5.1 Basic Maintenance	217
27.5.2 Access-limit Management	218
27.5.3 Telnet Client	218
27.5.4 CPU-alarm	218
27.5.5 Mail-alarm	219
27.5.6 Anti-Dos Attack	219
27.5.7 Displaying System Status	220
Chapter 28	
LLDP Configuration	221
28.1 LLDP Protocol Overview	221
28.2 Configure LLDP	221
28.2.1 LLDP Configuration Task	221
28.2.2 Enable LLDP	222
28.2.3 Configure LLDP Hello-Time	222
28.2.4 Configure LLDP Hold-Time	222
28.2.5 Configure LLDP Packet Transferring and Receiving Mode on Port	222
28.2.6 LLDP Displaying and Debugging	223

28.2.7 Configuration Example	223
Chapter 29	
PPPoE Plus Configuration	225
29.1 Introduction	225
29.1.1 PPPoE packet format	225
29.1.2 PPPoE Plus	225
29.2 PPPoE Plus Configuration	226
29.2.1 Enable PPPoE Plus	226
29.2.2 Option Content Configuration	226
29.2.3 PPPoE Plus Monitor and Maintenance	227
Chapter 30	
CFM Configuration	228
30.1 Brief Introduction to CFM	228
30.1.1 CFM Concepts	228
30.1.2 CFM Main Function	229
30.2 Configuring CFM	229
30.2.1 CFM Configuration Task List	230
30.2.2 Maintain Field Configuration	230
30.2.3 Configuration and Maintenance Level Domain Name	230
30.2.4 Maintain Set Configuration	231
30.2.5 Configuration Name and Associated VLAN to Maintenance Set	231
30.2.6 Configuration MEPs	232
30.2.7 Configure Remote Maintenance Endpoint	232
30.2.8 Configuring MIPs	232
30.2.9 Configuration Continuity Detection	233
30.2.10 Configure Loopback	233
30.2.11 Configure Link Tracking	234
30.2.12 Y.1731 frame loss detection	234
30.2.13 Y.1731 frame delay detection	234
30.2.14 Display and Maintenance of CFM	235
Chapter 31	
Flex Links Configuration.....	236
31.1 Flex Links Overview	236
31.1.1 Basic Concept of Flex Links	236
31.1.2 Operating Mechanism of Flex Link	238
31.2 Flex Links Configuration	240
31.2.1 Flex Links Configuration Tasks	240
31.2.2 Configure Flex Links group	240
31.2.3 Configure Flex Links Preemption Mode	240
31.2.4 Configure Flex Links Preemption Delay	241

31.2.5 Configure Flex Links MMU	241
31.2.6 FLex Links Monitor and Maintenance	242
Chapter 32	
Monitor Link Configuration.....	243
32.1 Monitor Link Overview	243
32.1.1 Background	243
32.1.2 Benefits	244
32.2 Monitor Link Implementation	244
32.2.1 Basic Concepts in Monitor Link	244
32.3 Configuring Monitor Link	246
32.3.1 Monitor Link Configuration Tasks	246
32.3.2 Configure Monitor Links Group	246
32.3.3 Monitor Link Monitor and Maintenance	247
32.4 Monitor Link Configuration Example	247
Chapter 33	
EFM/OAM Configuration	252
33.1 Brief Introduction to EFM/OAM	252
33.1.1 EFM/OAM Main Function	252
33.1.2 EFM/OAM Protocol Packets	253
33.2 Configuration EFM/OAM	254
33.2.1 EFM/OAM Configuration Task List	254
33.2.2 EFM/OAM Basic Configuration	254
33.2.3 EFM/OAM Timer Parameter Configuration	255
33.2.4 Configuring Remote Failure Indication	256
33.2.5 Configuring Link Monitoring Capabilities	256
33.2.6 Starting Remote Access Function MIB Variable	257
33.2.7 MIB Variable Access Requests Initiated by Remote	257
33.2.8 Display and Maintenance of EFM/OAM	258
Chapter 34	
L2TP Configuration	259
34.1 L2TP Overview	259
34.2 L2TP Configuration	260
34.2.1 Configure L2-Tunnel Packet	260
34.2.2 Advanced L2TP Configuration	260
34.2.3 L2TP Monitor and Maintenance	260
Chapter 35	
QinQ Configuration	261
35.1 Introduction to QinQ	261
35.2 Implementations of QinQ	263

35.2.1 Static QinQ	263
35.2.2 Dynamic QinQ	263
35.3 Configuring QinQ	264
35.3.1 Static QinQ Configuration	264
35.3.2 Dynamic QinQ Configuration	264
Chapter 36	
Stack Configuration.....	265
36.1 Stack Overview	265
36.2 Overview for Stack Configuration	268
36.3 Stack	268
36.3.1 Stand-Alone Mode Configuration	268
36.3.2 Stack Mode Configuration	269
36.3.3 Stack Configuration Examples	269
36.3.4 LACP MAD	272
36.3.5 LACP MAD Configuration Instance	272
36.3.6 BFD MAD	274
36.3.7 BFD MAD Configuration Examples	275
Appendix A Customer Support	278
Appendix B Legal Information.....	284
Index of Commands	290

Logging in Ethernet Switch

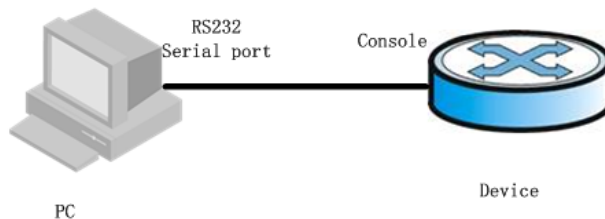
This chapter describes how to connect to the switch and do the configurations. There are ways as via console port and through telnet. It contains following sections:

- [Set up Configuration Environment via Console Port](#)
- [Set up Configuration Environment through Telnet](#)
- [Telnet Ethernet Switch through Ethernet Switch](#)

1.1 Set up Configuration Environment via Console Port

- 1 As shown in the figure below, to set up the local configuration environment, connect the serial port of a PC (or a terminal) to the Console port of the Ethernet switch with the Console cable.

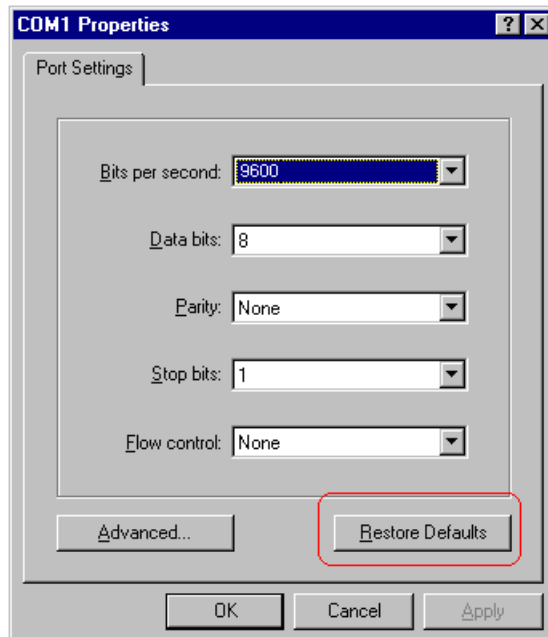
Figure 1 Set up the local configuration environment via the Console port



- 2 Run terminal emulator (such as Hyper Terminal on Windows 9X/2000/XP/Vista) on the Computer. Set the terminal communication parameters as follows: Set the baud rate to 9600, data bit to 8, parity check to none, stop bit to 1, flow control to none and select the terminal type as auto-detection.

Figure 2 Set up new connection



Figure 3 Configure the port for connection**Figure 4** Set communication parameters

- 3 The Ethernet switch is powered on. Display self-test information of the Ethernet switch and prompt you to press Enter to show the command line prompt such as `< >` after you have entered the correct username and password. The initial username is `admin` and the matched password is `1234`. It is suggested modifying the initial password after the first logging in. Please remember the modified password. If the password is forgotten, please contact us as soon as possible. Modify password refers to [Change Password](#).
- 4 Input a command to configure the Ethernet switch or Configuration Mode the operation state. Input a `?` to get an immediate help. For details of specific commands, refer to the following chapters.

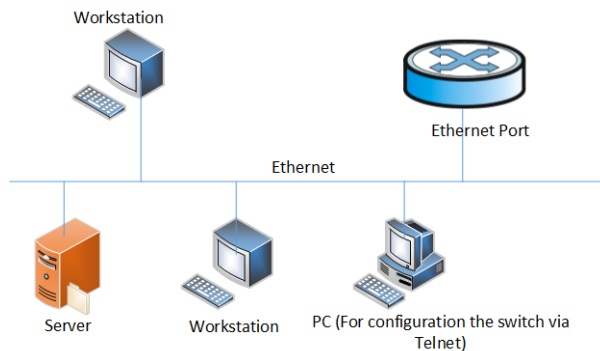
1.2 Set up Configuration Environment through Telnet

1.2.1 Connect PC to Ethernet Switch through Telnet

After you have correctly configured IP address of a VLAN interface for an Ethernet Switch via Console port (the way to configure switch via console refers to [Set up Configuration Environment via Console Port](#); the way to configure ip address of switch refers to 03 using `ip address` command in VLAN interface mode), and make sure PC can ping the switch, then you can telnet this Ethernet switch and configure it.

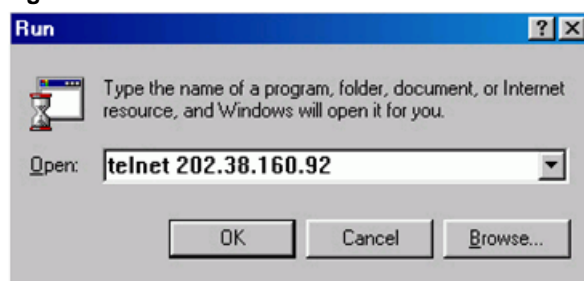
- 1 Authenticate the Telnet user via the Console port before the user logs in by Telnet.
- 2 To set up the configuration environment, connect the Ethernet port of the PC to that of the Ethernet switch via the LAN.

Figure 5 Set up configuration environment through telnet



- 3 Run Telnet on the PC and input the IP address of the VLAN connected to the PC port.

Figure 6 Run Telnet



- 4 The terminal displays "Username (1-32 chars):" and prompts the user to input the login username and password. After you input the correct username and corresponded password, it displays the command line prompt (such as < >). If the prompt "Too many users!" appears, it indicates that too many users are connected to the Ethernet through the Telnet at this moment. In this case, please reconnect later. At most 5 Telnet users are allowed to log in to the series Ethernet Switches simultaneously. Default username is `admin` and the password is `1234`. If the default password has been modified, it requires the modified password.
- 5 Use the corresponding commands to configure the Ethernet switch to monitor the running state. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.

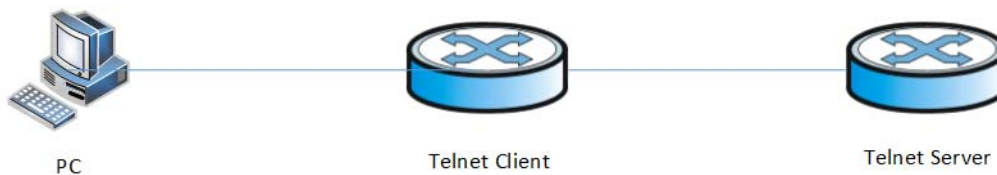
Note: When configuring the Ethernet switch via Telnet, do not modify the IP address because the modification might cut the Telnet connection.

1.2.2 Telnet Ethernet Switch through Ethernet Switch

The switch can be both the Telnet server and client. After a user has telnet to a switch from PC, he or she can configure another switch through this switch via Telnet. The local switch serves as Telnet client and the peer switch serves as Telnet server. If the ports connecting these two switches are in a same local network, their IP addresses must be configured in the same network segment. Otherwise, the two switches must establish a route that can reach each other.

As shown in the figure below, after you telnet to an Ethernet switch (that is Telnet Client in [Figure 7 on page 20](#)), you can run `telnet` command to log in and configure another Ethernet switch (that is Telnet Server in [Figure 7 on page 20](#)).

Figure 7 Provide Telnet Client service



- 1 Configure IP address for the switch (that is Telnet Client in [Figure 7 on page 20](#)). The way to configure switch via console refers to [Set up Configuration Environment via Console Port](#).
- 2 The user logs in the Telnet Client (Ethernet switch). For the login process, refer to the section describing "[Connect PC to Ethernet Switch through Telnet](#)".
- 3 Perform the following operations on the Telnet Client:
#telnet A.B.C.D (A.B.C.D is the IP address of the Telnet Server.)
- 4 Enter the preset login password and you will see the prompt such < >. If the prompt "Too many users!" appears, it indicates that too many users are connected to the Ethernet through the Telnet at this moment. In this case, please connect later.
- 5 Use the corresponding commands to configure the Ethernet switch or Configuration Mode it running state. Enter "?" to get the immediate help. For details of specific commands, refer to the following chapters.

Command Line Interface

This chapter describes command line interface (CLI) which you may use to configure your switch. It contains flowing sections:

- [Introduction of Command Line Interface](#)
- [Command Line Configuration Mode](#)
- [Feature and Functions of Command Line](#)
- [Symbols in Command](#)
- [Parameter in command](#)

2.1 Introduction of Command Line Interface

Ethernet Switches provide a series of configuration commands and command line interfaces for configuring and managing the Ethernet switch. The command line interface has the following characteristics:

- Local configuration via the Console port.
- Local or remote configuration via Telnet.
- Hierarchy command protection to avoid the unauthorized users accessing Ethernet switch.
- Enter a "?" to get immediate online help.
- Provide network testing commands, such as `Tracert` and `Ping`, to fast troubleshoot the network.
- Provide various detailed debugging information to help with network troubleshooting.
- Log in and manage other Ethernet switch directly, using the Telnet command.
- Provide FTP/TFTP/Xmodem service for the users to upload and download files.

The command line interpreter searches for target not fully matching the keywords. It is ok for you to key in the whole keyword or part of it, as long as it is unique and not ambiguous.

2.2 Command Line Configuration Mode

Ethernet Switches provide hierarchy protection for the command lines to avoid unauthorized user accessing illegally.

Commands are classified into three levels, namely visit and monitoring level, configuration level and management level. They are introduced as follows:

- **Visit and monitoring level:** Commands under this level involve network diagnosis tools (such as **ping** and **tracert**), command between different language environments of user interface (**language-mode**) **telnet** command, the **display** command and the **debugging** command, which are used for system maintenance, service fault diagnosis, etc. The operation of saving configuration file is not allowed on this level of commands.
- **Configuration level:** Service configuration commands, including routing command and commands on each network layer are used to provide direct network service to the user.
- **Management level:** They are commands that influence basis operation of the system and system support module, which plays a support role on service. Commands of this level involve file system commands, FTP commands, TFTP commands, Xmodem downloading commands, user management commands, and level setting commands.

At the same time, login users are classified into three levels that correspond to the three command levels respectively. After users of different levels logging in, they can only use commands at the levels that are equal to or lower than their own level.

In order to prevent unauthorized users from illegal intrusion, user will be identified when switching from a lower level to a higher level with `username username [privilege level] {password encryption-type password}` command. For the sake of confidentiality, on the screen the user cannot see the password that he entered. Only when correct password is input for three times, can the user switch to the higher level. Otherwise, the original user level will remain unchanged.

Different command configuration mode is implemented according to different requirements. They are related to one another. For example, after logging in the Ethernet switch, you will enter user mode, in which you can only use some basic functions such as displaying the running state and statistics information. In user mode, key in **enable** to enter privileged mode, in which you can key in different configuration commands and enter the corresponding configuration modes.

The command line provides the following configuration modes:

- User Mode
- Privileged Mode
- Global Configuration Mode
- Interface Configuration Mode
- VLAN Configuration Mode
- AAA Configuration Mode
- RADIUS Configuration Mode
- Domain Configuration Mode
- VLAN-interface Configuration Mode
- SuperVLAN-interface Configuration Mode
- RIP Configuration Mode
- OSPF Configuration Mode
- PIM Configuration Mode

The following table describes the function features of different Configuration Modes and the ways to enter or quit.

Table 1 Function feature of Command Configuration Mode

COMMAND CONFIGURATION MODE	FUNCTION	PROMPT	COMMAND TO ENTER	COMMAND TO EXIT
User Mode	Show the basic information about operation and statistics	Switch>	Enter right after connecting the switch	exit disconnects to the switch
Privileged mode	Show the basic information about operation and statistics and manage the system	Switch#	Key in enable in user mode	exit returns to user mode; quit disconnects to the switch
Global Configuration Mode	Configure system parameters	Switch(config)#	Key in configure terminal in privileged Mode	exit and end returns to privileged mode; quit disconnects to the switch
Interface Configuration Mode	Configure Interface parameters	Switch(config-if-ethernet-0/0/1)	Key in interface ethernet 0/0/1 in global Configuration Mode	exit returns to global configuration mode and end returns to privileged mode; quit disconnects to the switch
VLAN Configuration Mode	Configure VLAN parameters	Switch(config-if-Vlan)#	Key in vlan 1 in system Configuration Mode	
AAA Configuration Mode	Create domain	Switch(config-aaa)#	Key in aaa in global configuration mode	
RADIUS Configuration Mode	Configure RADIUS server parameters	Switch(config-radius-default)#	Key in radius host default in AAA configuration mode	exit returns to privileged mode and end returns to AAA configuration mode; quit disconnects to the switch
Domain Configuration Mode	Configure domain parameters	Switch(config-aaa-test.com)#	Key in domain test.com in AAA configuration mode	
VLAN interface Configuration Mode	Configure IP interface parameters for a VLAN or a VLAN aggregation	Switch(config-if-vlanInterface-22)#	Key in interface vlan-interface 22 in global configuration mode	end returns to privileged mode exit returns to global configuration mode and quit disconnects to the switch
SuperVLAN interface Configuration Mode	Configure Supervlan interface parameters	Switch(config-if-supervlanInterface-1)#	Key in interface supervlan-interface 1 in global configuration mode	
PIM Configuration Mode	Configure PIM parameters	Switch(config-router-pim)#	Key in pim in global configuration mode	
RIP Configuration Mode	Configure RIP parameters			
OSPF Configuration Mode	Configure OSPF parameters	Switch(config-router-ospf)#	Key in route ospf in global Configuration Mode	

2.3 Feature and Functions of Command Line

2.3.1 Help of Command Line

You can get the help information through the help commands, which are described as follows.

Table 2 Help commands

COMMAND	PURPOSE	EXAMPLES
Help	Obtain a brief description of the help system in any command mode.	Switch> help System mode commands: Clear clear erps-ring's statistics cls clear screen help description of the interactive help ping ping command
Abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string.	Switch(config)#interf? interface
?	List all commands available for a particular command mode.	Switch>? System mode commands: clear clear erps-ring's statistics cls clear screen help description of the interactive help ping ping command
command?	List the associated keywords for a command.	Switch(config)#spanning-tree ? forward-time config switch delaytime hello-time config switch hellotime max-age config switch max agingtime mode Set state machine mode parameter mst Multiple spanning tree configuration priority config switch priority <enter> The command end.
command keyword?	List the associated arguments for a keyword.	Switch(config)#spanning-tree forward-time ? INTEGER<4-30> switch delaytime: <4-30> (second)

Note: To switch to the Chinese display for the above information, perform the `terminal language {chinese | english}` command in privileged mode.

2.3.2 Displaying Characteristics of Command Line

Command line interface provides the following display characteristics:

For users' convenience, the instruction and help information can be displayed in both English and Chinese. For the information to be displayed exceeding one screen, pausing function is provided. In this case, users can have three choices, as shown in the table below.

Table 3 Functions of displaying

KEY OR COMMAND	FUNCTION
Press <Ctrl+C> when the display pauses	Stop displaying and executing command.
Press other key when the display pauses	Continue to display the next screen of information.
Press <Enter> when the display pauses	Continue to display the next line of information.

2.3.3 Show history Command of Command Line

Command line interface provides the function similar to that of DosKey. The commands entered by users can be automatically saved by the command line interface and you can invoke and execute them at any time later. The number of command buffer is 100 as default, that is, the command line interface can store 100 history commands for each user. The operations are shown in the table below.

Table 4 Retrieve history command

OPERATION	KEY	RESULT
Retrieve the previous history command	Up cursor key <↑> or <Ctrl+P>	Retrieve the previous history command, if there is any.
Retrieve the next history command	Down cursor key <↓> or <Ctrl+N>	Retrieve the next history command, if there is any.

Note: Cursor keys can be used to retrieve the history commands in Windows 9X/2000/XP Terminal and Telnet.

2.3.4 Common Command Line Error Messages

All the input commands by users can be correctly executed, if they have passed the grammar check. Otherwise, error messages will be reported to users. The common error messages are listed in the following table.

Table 5 Common command line error messages

ERROR MESSAGES	CAUSES
Unrecognized command	Cannot find the command.
	Cannot find the keyword.
	Wrong parameter type.
	The value of the parameter exceeds the range.
Incomplete command	The input command is incomplete.
Too many parameters	Enter too many parameters.
Ambiguous command	The parameters entered are not specific.

2.4 Symbols in Command

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([]) mean optional elements.
- Braces { } group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.
- Information you enter is in boldface screen font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

2.5 Parameter in command

There are 5 types of parameters:

- Integer

The two numbers in the angle brackets (<>), connecting by hyphen (-) mean this parameter is the integer between these two numbers.

For example: INTEGER<1-10> means user can key in any integer which can be more than or equal to 1 and less than or equal to 10, such as 8.

- IP address

A.B.C.D means an IP address.

For example: 192.168.0.100 is a valid IP address.

- MAC address

H:H:H:H:H:H means a MAC address. If a multicast MAC address is needed, there would be corresponded prompt.

For example: 01:02:03:04:05:06 is a valid MAC address.

- Interface list

Interface list is prompted as STRING<3-4>. Port parameter interface-num consists of port type and port number. Port type is Ethernet and port number is device/slot-num/port-num. Device means stack value which is 0; slot-num means slot number; port-num is the port number in the slot. Port parameter interface-list means multiple ports. Seriate interfaces with the same type can be linked by "to", but the port number behind the "to" must be larger than the one in the front, and this argument only can be repeated up to 3 times. The special declaration of interface parameter interface list will be displayed in the command.

For example: Showing spanning-tree interface ethernet 0/0/1 ethernet 0/0/3 to ethernet 0/0/5 means showing the spanning-tree information about interface ethernet 0/0/1, ethernet 0/0/2, ethernet 0/0/3, ethernet 0/0/4 and ethernet 0/0/5.

- String

The prompt STRING<1-19> means a character string which is in the length of 1 to 19. Enter "?" to see the parameter description of this command.

Manage Users

There are three kinds of users:

- Super-administrator
- Administrator
- Normal user

The normal users can only be in the user's mode after logging in the switch so they can only check the basic information about operation and statistics;

administrator can enter each configuration mode to check and manage the system; super-administrator can both manage the system and all kinds of users.

Note: Normal users cannot configure the switch and change their own password.

Administrator can manage himself; for example, change his own privilege and password. It cannot create or delete other users and change other user's password and privilege.

3.1 System Default User

There is an internal username with password called Super-administrator. It processes the superior priority in the switch to manage both the users and the switch.

The username of Super-administrator is `admin` and its initial password is `1234`. It is suggested modifying the password after the initial-logging in. This username and its administrator privilege cannot be deleted and modified.

Note: There must be only one super-administrator and all the configurations in the manual is setting super-administrator as example.

3.2 User's Account Authentication

User's authentication can be divided into local authentication and remote authentication:

- Local authentication: The users' account and password are saved in local database. All users are supported by local authentication.
- Remote authentication: The users' account and password are saved in RADIUS/TACACS+ server. Super-administrator "admin" is not supported by remote authentication.

3.3 Local Authentication Configuration

3.3.1 Add Users

At most 15 users can be added. Log in the switch first as Super-administrator and create new users as following steps:

Table 6 Add users

STEP	COMMAND	DESCRIPTION
1	Enable	Enter privileged mode
2	config terminal	Enter global configuration mode.
3	username <i>username</i> privilege <i>privilege</i> < <i>pri-value</i> > password <i>encryption-type</i> < 0 7> <i>password</i>	Adding a new user and specify the privilege, encryption-type and password.
4	show username	Check the configuration.
5	exit	Exit to user mode.
6	copy running-config startup-config	Save the configuration.

Note: *Username*: it means the name of the user to be added which must be 1 to 32 printable characters without `'',':','*','?','\','<','>','|','"`.

Level: means the priority of the user to be added which is the number between 0 and 15. 0 and 1 mean the normal user and 2 to 15 mean the administrator.

encryption-type: it can be "0" or "7", "0" means clear text and "7" means encrypted text (not supported now).

privilege: it can be 0, 1 or 2 to 15. 0 and 1 mean normal users while 2 to 15 mean administrators.

Password: the login password of new-added user which is 1 to 16 characters.

If the user's privilege level is not specified, it will default to be normal user. There is up to 8 users in the system.

Case-sensitive is for password but not username.

Example:

!Create administrator "XXXX" with its password being 1234 and privilege level is 3

```
Switch(config)#username XXXX privilege 3 password 0 1234
```

3.3.2 Change Password

In global configuration mode, Super-administrator "admin" can use following command to change the password of all users, but other administrators can only change their own password. Normal users cannot modify their own password.

Enter global configuration mode (how to enter global configuration mode refers to the first 2 steps in [Table 6 on page 29](#)) before following the below steps:

Table 7 Modify password

STEP	COMMAND	DESCRIPTION
1	username change-password	Enter the modified password following the prompt. The new password will be effective in the next log in.
2	exit	Exit to user mode.
3	copy running-config startup-config	Save the configuration.

Example:

!Change the password of user "XXXX" to be 123456

```
Switch(config)#username change-password
please input you login password : *****
please input username :XXXX
Please input user new password :*****
Please input user confirm password :*****
change user XXXX password success.
```

3.3.3 Modify User's Privilege Level

In global configuration mode, only Super-administrator "admin" can modify the privilege level of other users. Enter global configuration mode (how to enter global configuration mode refers to the first 2 steps in [Table 6 on page 29](#)) before following the below steps:

Table 8 Modify User's Privilege Level

STEP	COMMAND	DESCRIPTION
1	username <i>username</i> privilege <i>privilege <0-15></i> encryption-type <i><0/7></i> password	Modify user's privilege. Set encryption-type to 0 if you don't want to change the password.
2	show username	Check configuration.
3	Exit	Exit to user mode.
4	copy running-config startup-config	Save the configuration.

Note: *Username*: means the name of the existed user to be modified which must be 1 to 32 printable characters without '/', ':', '*', '?', '\\', '<', '>', '|', '"'. If the entered username is not existed, add it to be the new one.

Level: means the priority of the existed user (except the Super-administrator) to be modified which is the number between 0 and 15, level "0" and "1" mean the normal user and "2" to "15" mean the administrator.

Case-sensitive is for password but not username.

Example:

!Modify the privilege of the existed user "XXXX" to be 1 and its password to be 1234

```
Switch(config)#username XXXX privilege 0 password 0 1234
```

3.3.4 Delete User

Only Super-administrator "admin" can add and delete user in global configuration mode. Enter global configuration mode (how to enter global configuration mode refers to the first 2 steps in [Table 6 on page 29](#)) before following the below steps:

Table 9 Delete User

STEP	COMMAND	DESCRIPTION
1	<code>no username <i>username</i></code>	Delete user.
2	<code>show username</code>	Check configuration.
3	<code>exit</code>	Exit to user mode
4	<code>copy running-config startup-config</code>	Save the configuration

Note: *Username*: means the name of the user to be deleted.

When deleting a user which is used, it will be disconnected before delete it.

Example:

!Delete user "XXXX"

```
Switch(config)#no username XXXX
```

3.3.5 Show Users

After configuration, you can use following steps to check it. Any configuration mode is permitted.

Table 10 Show Users

STEP	COMMAND	DESCRIPTION
1	<code>show username</code>	Show specific user.
2	<code>show users</code>	Show users' log. At most 5 users are permitted on line at the same time.

3.4 Remote Authentication Configuration

3.4.1 Choose RADIUS as Remote Authentication Server

Table 11 configure RADIUS remote authentication

OPERATION	COMMAND	DESCRIPTION
Enter global configuration	<code>configure terminal</code>	-
Enable RADIUS remote authentication	<code>muser radius name {chap pap} [local]</code>	Selected If "local" is configured, it means local authentication is used if remote authentication failed. By default, it is local authentication
Enter AAA configuration mode	<code>aaa</code>	-
Create RADIUS server name and enter RADIUS configuration mode	<code>radius host name</code>	-
Configure IP of authentication/ accounting RADIUS server	<code>{primary-acct-ip primary-auth-ip } A.B.C.D { accounting port authentication port }</code>	Selected Authentication and accounting port should be the same as that of RADIUS server. Generally, they are: Accounting port:1813 Authentication port:1812
Configure shared-key of authentication/ accounting RADIUS server	<code>{acct-secret-key auth-secret-key} key</code>	Selected Shared-key should be the same as that of RADIUS server.
Show configuration	<code>show muser</code>	-

3.4.2 Choose TACACS+ Remote Authentication

Configuring user's login through TACACS+ server authentication, accounting and authorization through TACACS+ server can be chosen. When configuring TACACS+ authorization, configure corresponded priority to users first. There are 16 levels (0-16) priorities but there are only 2 levels (0-1 means normal users and 2-15 means administrators) for switches. When configuring TACACS+ un-authorization, the priority is determined by `priv_lvl` replied from remote server (no reply means administrator). Authorization failure means normal user.

When configuring TACACS+ accounting, it begins with the pass of authentication and ends with user's exit.

Table 12 Configure TACACS+ remote authentication

OPERATION	COMMAND	DESCRIPTION
Enable TACACS+ authorization/accounting	<code>muser tacacs+ {account [local] author [local] local}</code>	Selected If "local" is configured, it means local authentication is used if remote authentication failed. By default, it is local authentication
Configure IP/shared-key/TCP port/timeout of TACACS+ remote server	<code>tacacs+ { priamary secondary } server <i>ipaddress</i> [key <i>keyvalue</i>] [port <i>portnum</i>] [timeout <i>timevalue</i>]</code>	Selected By default, TCP port is 49 and timeout is 5 seconds.
Show TACACS+ configuration	<code>show tacacs+</code>	-
Show current authentication	<code>show muser</code>	-

Ethernet Port Configuration

This chapter describes the types of interfaces on switches and how to configure them.

4.1 Ethernet Port Overview

4.1.1 Link Type of Ethernet Ports

An Ethernet port can operate in one of the three link types:

- Access: An access port only belongs to one VLAN, normally used to connect user device or customer side.
- Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs and is generally used to connect another switches. The packet sent from this port can only be with tagged frames.
- Hybrid: A hybrid port can belong to multiple VLANs, can receive, or send packets for multiple VLANs, used to connect either users/customers or network devices. It allows packets of multiple VLANs to be sent with or without the tag label

4.1.2 Configuring Default VLAN ID for an Ethernet Port

Both hybrid port and trunk port can belong to more than one VLAN, but there is a default VLAN for each port. The default VLAN ID (PVID) is VLAN 1 and it can be changed if necessary (the way to change PVID refers to [Table 17 on page 36](#)).

4.1.3 Handling Packets

Different ports have different ways to handle the packet. Details are in [Table 13 on page 34](#).

Table 13 Different port handles different packet

PORT TYPE	INGRESS		EGRESS
	UNTAGGED PACKET	TAGGED PACKET	
Access port	Receive it and add a tag with VID being equal to PVID.	If VID of the packet is equal to the port permitted VID, receive it; if VID is different, discard it.	Strip the Tag and transmit the packet as the VID of the packet is equal to the port permitted VID
Hybrid port			If VID of the packet is equal to the port permitted untagged VID, remove the tag and transmit it; If VID of the packet is equal to the port permitted tagged VID, keep the tag and transmit it.
Trunk port			If VID of the packet is equal to the port permitted VID, keep the tag and transmit it.

4.2 Configure Ethernet Port

Ethernet port configuration includes:

- [Basic Ethernet Port Configuration](#)
- [Combo Port](#)
- [Enable/Disable Ingress Filtering](#)
- [Acceptable-Frame Type for Ethernet Port](#)
- [Enable/Disable Flow Control for Ethernet Port](#)
- [Display and Debug Ethernet Port](#)

4.2.1 Basic Ethernet Port Configuration

Basic Ethernet port configuration includes:

- [Enter Interface Configuration Mode](#)
- [Enter Interface Range Mode](#)
- [Configure Port Mode](#)
- [Configure Default VLAN](#)
- [Add a Port to a VLAN](#)
- [Basic Port Configuration](#)

4.2.1.1 Enter Interface Configuration Mode

Before configuring the ethernet port, you have to enter interface configuration mode first.

perform the following commands in privileged mode.

Table 14 Enter interface configuration mode

STEP	COMMAND	DESCRIPTION
1	<code>configure terminal</code>	Enter global configuration mode.
2	<code>interface ethernet { device-num/slot-num/ port-num }</code>	Enter interface configuration mode.

4.2.1.2 Enter Interface Range Mode

Sometimes we need to configure the range of ports with the same configurations. We can use interface range mode to avoid the repetition. Perform the following configuration in privileged mode.

Table 15 Enter interface range mode

STEP	COMMAND	DESCRIPTION
1	<code>configure terminal</code>	Enter global configuration mode.
2	<code>interface range interface-list</code>	Enter interface range configuration mode.

Example:

! Divide interfaces from Ethernet 0/0/1 to Ethernet 0/0/16 into an interface range.

```
Switch(config)#interface range ethernet 0/0/1 to ethernet 0/0/16
Switch(config-if-range)#
```

4.2.1.3 Configure Port Mode

Table 16 Configure port mode

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	
Enter interface configuration mode	interface ethernet <i>device-num/slot-num/port-num</i>	
Configure port mode to be Access, Hybrid or Trunk	switchport mode { <i>access hybrid trunk</i> }	
Show port mode	show interface ethernet <i>device-num/slot-num/port-num</i>	

Example:

! There is VLAN 1-20. Configure uplink port e 0/1/1 to be trunk, and it can transceive packets of VLAN1-20

```
Switch(config)#vlan 1-20
Switch(config-if-vlan)#switchport ethernet 0/1/1
Add VLAN port successfully.
Switch(config-if-vlan)#interface ethernet 0/1/1
Switch(config-if-ethernet-0/1/1)#switchport mode trunk
Switch(config-if-ethernet-0/1/1)# show interface brief ethernet 0/1/1
Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan
e0/1/1 down FALSE auto 0 1 trk 1-20
Total entries: 1 .
```

4.2.1.4 Configure Default VLAN

Table 17 Configure default VLAN

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	
Enter interface configuration mode	interface ethernet <i>device-num/slot-num/port-num</i>	
Modify port default VLAN	switchport default vlan <i>vlan_id</i>	

Example:

! The first four ports (e 0/0/1 – e0/0/4) connect to different server. These four servers should be isolated. And the servers belong to VLAN 10,VLAN 20,VLAN 30 and VLAN 40.

```
Switch(config)#vlan 10
Switch(config-if-vlan)#switchport ethernet 0/0/1
Add VLAN port successfully.
Switch(config-if-vlan)#vlan 20
Switch(config-if-vlan)#switchport ethernet 0/0/2
Add VLAN port successfully.
Switch(config-if-vlan)#vlan 30
Switch(config-if-vlan)#switchport ethernet 0/0/3
Add VLAN port successfully.
Switch(config-if-vlan)#vlan 40
Switch(config-if-vlan)#switchport ethernet 0/0/4
Add VLAN port successfully.
Switch(config-if-vlan)#interface ethernet 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport default vlan 10
Switch(config-if-ethernet-0/0/1)#interface ethernet 0/0/2
Switch(config-if-ethernet-0/0/2)#switchport default vlan 20
Switch(config-if-ethernet-0/0/2)#interface ethernet 0/0/3
Switch(config-if-ethernet-0/0/3)#switchport default vlan 30
Switch(config-if-ethernet-0/0/3)#interface ethernet 0/0/4
Switch(config-if-ethernet-0/0/4)#switchport default vlan 40
Switch(config-if-ethernet-0/0/4)#vlan 1
Switch(config-if-vlan)#no switchport ethernet 0/0/1 to ethernet 0/0/4
Switch(config-if-vlan)#show interface brief e 0/0/1 to e 0/0/4
Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan
e0/0/1 down false auto 0 10 hyb 10
e0/0/2 down false auto 0 20 hyb 20
e0/0/3 down false auto 0 30 hyb 30
e0/0/4 down false auto 0 40 hyb 40
Total entries: 4 .
```

4.2.1.5 Add a Port to a VLAN

User can add current ethernet port to a specific VLAN, thus, the ethernet port can forward packet of the VLAN.

Hybrid port and Trunk port can belong to multiple VLANs and Access port can only belong to one VLAN, which is the default VLAN. By default, all ports belong to VLAN 1.

In VLAN configuration mode, user can use switchport ethernet command to add a port to vlan, please refer to “VLAN configuration” chapter.

There is another way to add port to a VLAN, in interface configuration mode.

Table 18 Configure port mode

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	
Enter interface configuration mode	interface ethernet <i>device-num/slot-num/port-num</i>	
Add Hybrid port to specific VLAN and keep the packet VID	switchport hybrid tagged vlan <i>vlan-list</i>	
Add Hybrid port to specific VLAN and strip the packet VID	switchport hybrid untagged vlan <i>vlan-list</i>	

Table 18 Configure port mode

OPERATION	COMMAND	REMARKS
Delete Hybrid port from specific VLAN	<code>no switchport hybrid vlan <i>vlan-list</i></code>	
Add Trunk port to specific VLAN	<code>switchport trunk allowed vlan <i>vlan-list</i></code>	
Delete Trunk port from specific VLAN	<code>no switchport trunk allowed vlan <i>vlan-list</i></code>	

There are two ways to add an Access port to VLAN: one is to configure port default VLAN; the other is to add the port to another VLAN directly. Access port can only belong to one VLAN, so this port will be auto-deleted from the original VLAN.

Example:

e 0/0/1 is Hybrid. Configure this port keeping tag of VLAN 10.

```
Switch(config)#vlan 10
Switch (config-if-vlan)#interface ethernet 0/0/1
Switch (config-if-ethernet-0/0/1)#switchport hybrid tagged vlan 10
Switch (config-if-ethernet--0/0/1)#show interface brief e 0/0/1
Port Desc Link shutdn Speed Pri PVID Mode TagVlan UtVlan
e0/0/1 down false auto 0 1 hyb 10 1
Total entries: 1 .
```

4.2.1.6 Basic Port Configuration

Following basic port configurations are in the interface configuration mode.

Table 19 Basic port configuration

OPERATION	COMMAND	DESCRIPTION
Disable specific port	<code>shutdown</code>	By default, the port is enabled. If you want to re-enable the port, use <code>no shutdown</code> command.
Configure duplex of a port	<code>duplex { auto full half }</code> <code>no duplex</code>	10/100/1000BASE-T supports full duplex, half duplex and auto-negotiation; 1000BASE-X supports full duplex and auto-negotiation. By default, the working mode is auto. If duplex is auto, the speed will be auto.
Configure speed of a port	<code>speed { <i>speed-value</i> auto }</code> <code>no speed</code>	10/100/1000BASE-T supports 10Mbps, 100Mbps and 1000Mbps; 1000BASE-X supports only 1000Mbps. By default, the speed is auto. If the speed is auto, the duplex will be auto.
Configure priority of a port	<code>priority <i>priority-value</i></code> <code>no priority</code>	<i>Priority-value</i> could be 0 to 7 and the default interface priority is 0. The larger the priority value is, the higher the priority is. And the packet with the higher priority will be quickly handled.
Configure port description	<code>description <i>description-list</i></code>	The description is used to distinguish ports. By default, the description of a port is empty.

4.2.2 Combo Port

A combo port is formed by two Ethernet ports on the panel, one of which is an optical port and the other is an electrical port. For the two ports forming a combo port, only one works at a given time. They are TX-SFP multiplexed. You can specify a combo port to operate as an electrical port or an optical port as needed. That is, a combo port cannot operate as both an electrical port and an optical port simultaneously.

Generally, if both electrical port and optical port are all inserted, only electrical port can work. If the user wants to use optical port, please unplug the electrical port.

4.2.3 Enable/Disable Ingress Filtering

If ingress filtering is enabled, the received 802.1Q tagged frames will be dropped if the incoming VID don't match with the pre-joined VLAN of the interface ports. The packet will not be dropped if the function is disabled and the VLAN which the tagged frame belonged to is existed.

Perform the following configuration in interface configuration mode.

Table 20 Enable/disable ingress filtering

OPERATION	COMMAND
Enable ingress filtering	<code>ingress filtering</code>
Disable ingress filtering	<code>no ingress filtering</code>

Note: By default, ingress filtering is enabled.

Example:

! Disable VLAN ingress filtering

```
Switch(config)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#no ingress filtering
Disable ingress filtering successfully!
```

! Enable VLAN ingress filtering

```
Switch(config)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#ingress filtering
Enable ingress filtering successfully!
```

4.2.4 Acceptable-Frame Type for Ethernet Port

We can configure ingress acceptable frames type to be "all" or "tagged" only. The untagged frame will be rejected if the port is configured as "tagged" only.

Perform the following configuration in interface configuration mode.

Table 21 Configure ingress acceptable-frame

OPERATION	COMMAND
Enable ingress acceptable-frame	<code>ingress acceptable-frame { all tagged }</code>
Disable ingress acceptable-frame	<code>no ingress acceptable-frame</code>

Note: By default, ingress acceptable-frame is all.

Example:

! Configure Ethernet 0/0/5 only to receive tagged frame

```
Switch(config)#interface ethernet 0/0/5
Switch(config-if-ethernet-0/0/5)#ingress acceptable-frame tagged
Config acceptable-frame type successfully!
! Restore the default ingress acceptable-frame of Ethernet 0/0/5
Switch(config)#interface ethernet 0/0/5
Switch(config-if-ethernet-0/0/5)#no ingress acceptable-frame
Config acceptable-frame type successfully!
```

4.2.5 Enable/Disable Flow Control for Ethernet Port

After enabling flow control in both the local and the peer switch, if congestion occurs in the local switch, the switch will inform its peer to pause packet sending. Once the peer switch receives this message, it will pause packet sending, and vice versa. In this way, packet loss is reduced effectively. The flow control function of the Ethernet port can be enabled or disabled through the following command.

Perform the following configuration in interface configuration mode.

Table 22 Enable/Disable Flow Control for Ethernet Port

OPTION	COMMAND
Enable Ethernet port flow control	flow-control
Disable Ethernet port flow control	no flow-control

Note: By default, Ethernet port flow control is disabled.

Example:

! Enable flow-control on ethernet 0/0/5

```
Switch(config)#interface ethernet 0/0/5
Switch(config-if-ethernet-0/0/5)#flow-control
Setting successfully! flow-control is enable
```

! Disable flow-control on ethernet 0/0/5

```
Switch(config)#interface ethernet 0/0/5
Switch(config-if-ethernet-0/0/5)#no flow-control
Setting successfully! flow-control is disable
```

4.2.6 Display and Debug Ethernet Port

After the above configuration, execute show command in any configuration mode to display the running of the ethernet port configuration, and to verify the effect of the configuration.

Execute clear interface command in global configuration mode or interface configuration mode to clear the statistics information of the port.

Table 23 Display and debug Ethernet port

OPERATION	COMMAND	DESCRIPTION
Clear the statistics information of the port.	<code>clear interface [interface-num slot-num]</code>	The information of the interface includes: numbers of unicast, multicast and broadcast message etc.
Display interface description.	<code>show description interface [interface-list]</code>	
Display port configuration	<code>show interface [interface-num]</code>	
Display the statistic information of specified port or all ports.	<code>show statistics interface [interface-num]</code>	
Display the statistic information of all interfaces	<code>show statistic dynamic interface</code>	Statistic information refreshes automatically every 3 seconds. Press "Enter" to exit.
Display the utilization information of all ports	<code>show utilization interface</code>	The utilization information of all ports includes receiving and sending speed, bandwidth utilization rate, etc. Press "Enter" to exit.

Note: Using `clear interface` command in global mode, if the interface-num and slot-num are not assigned, the information of all interfaces is cleared. If the slot-num is assigned, the port information of the assigned slot is cleared. In interface mode, only the information of the current port can be cleared.

If port type and port number are not specified, the above command displays information about all ports. If both port type and port number are specified, the command displays information about the specified port.

Example:

! Show description of all port

```
Switch(config-if-ethernet-0/0/1)#show description interface
Port      description
e0/0/1    test
e0/0/2
e0/0/3    XXXX
e0/0/4
e0/0/5
.....
```

! Show interface Ethernet 0/0/5

```
Switch(config-if-ethernet-0/0/1)#show interface ethernet 0/0/5
Ethernet e0/0/5 is enabled, port link is down
  Hardware is Fast Ethernet, Hardware address is 00:0a:5a:11:b5:71
  SetSpeed is auto, ActualSpeed is unknown, porttype is 10/100/1000M
  Priority is 0
  Flow control is disabled
  PVID is 1
  Port mode:hybrid
    Tagged   VLAN ID :
    Untagged VLAN ID : 1
  0 packets output
    0 bytes, 0 unicasts, 0 multicasts, 0 broadcasts
  0 packets input
    0 bytes, 0 unicasts, 0 multicasts, 0 broadcasts
```

! Show statistic interface ethernet 0/0/2

```
Switch(config-if-ethernet-0/0/1)#show statistics interface ethernet 0/0/2
Port number   : e0/0/2
input rate 0 bits/sec, 0 packets/sec
output rate 0 bits/sec, 0 packets/sec
64 byte packets:0
65-127 byte packets:0
128-255 byte packets:0
256-511 byte packets:0
512-1023 byte packets:0
1024-1518 byte packets:0
0 packets input, 0 bytes , 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 input errors, 0 FCS error, 0 symbol error, 0 false carrier
0 runts, 0 giants
0 packets output, 0 bytes, 0 discarded packets
0 unicasts, 0 multicasts, 0 broadcasts
0 output errors, 0 deferred, 0 collisions
0 late collisions
Total entries: 1.
```

! Show statistic dynamic interface

```
Switch(config-if-ethernet-0/0/1)#show statistics dynamic interface
Port Statistics                               Sat Jan 1 00:39:37 2000
port  link  Tx Pkt  Tx Byte  Rx Pkt  Rx Byte  Rx      Rx
      Status Count   Count    Count   Count   Bcast   Mcast
=====
e0/0/1  down  0         0         0         0         0         0
e0/0/2  down  0         0         0         0         0         0
e0/0/3  down  0         0         0         0         0         0
e0/0/4  down  0         0         0         0         0         0
e0/0/5  down  0         0         0         0         0         0
e0/0/6  down  0         0         0         0         0         0
e0/0/7  down  0         0         0         0         0         0
e0/0/8  down  0         0         0         0         0         0
e0/0/9  down  0         0         0         0         0         0
e0/0/10 down  0         0         0         0         0         0
e0/0/11 down  0         0         0         0         0         0
e0/0/12 down  0         0         0         0         0         0
e0/0/13 down  0         0         0         0         0         0
e0/0/14 down  0         0         0         0         0         0
e0/0/15 down  0         0         0         0         0         0
e0/0/16 down  0         0         0         0         0         0
e0/0/17 down  0         0         0         0         0         0
=====0->Clear Counters  U->page up  D->page down CR->exit=====
```

! Show utilization interface

```
Switch(config-if-ethernet-0/0/1)#show utilization interface
Link Utilization Averages                     Sat Jan 1 00:43:44 2000
port  link  Receive  Peak Rx  Transmit  Peak Tx
      Status pkts/sec pkts/sec pkts/sec pkts/sec
=====
e0/0/1  down  0         0         0         0
e0/0/2  down  0         0         0         0
e0/0/3  down  0         0         0         0
e0/0/4  down  0         0         0         0
e0/0/5  down  0         0         0         0
e0/0/6  down  0         0         0         0
e0/0/7  down  0         0         0         0
e0/0/8  down  0         0         0         0
e0/0/9  down  0         0         0         0
e0/0/10 down  0         0         0         0
e0/0/11 down  0         0         0         0
e0/0/12 down  0         0         0         0
e0/0/13 down  0         0         0         0
e0/0/14 down  0         0         0         0
e0/0/15 down  0         0         0         0
e0/0/16 down  0         0         0         0
e0/0/17 down  0         0         0         0
====spacebar->toggle screen U->page up  D->page down CR->exit=====
```

! Clear interface

```
Switch(config-if-ethernet-0/0/1)#clear interface
clear current port statistics information record successfully !
```

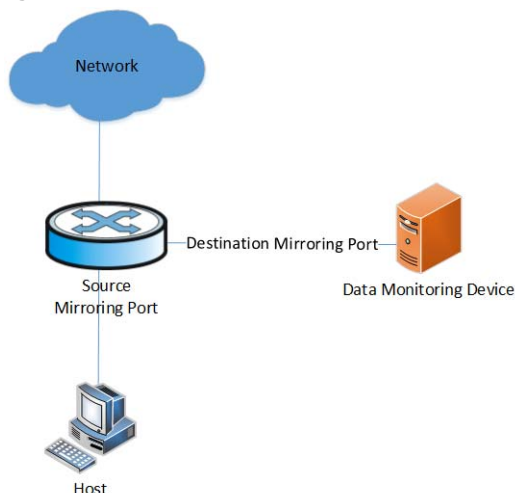
Ethernet Port Mirroring Configuration

5.1 Configure Ethernet Port Mirroring

5.1.1 Overview

Mirroring refers to the process of copying packets that meet the specified rules to a destination port. Generally, a destination port is connected to a data detect device, which users can use to analyze the mirrored packets for monitoring and troubleshooting the network.

Figure 8 mirroring



5.1.1.1 Traffic Mirroring

Traffic mirroring maps traffic flows that match specific ACLs to the specified destination port for packet analysis and monitoring. Before configuring traffic mirroring, you need to define ACLs required for flow identification.

5.1.1.2 Port Mirroring

Port mirroring refers to the process of copying the packets received or sent by the specified port to the destination port.

5.1.2 Mirroring

Switch support one-to-one and multiple-to-one mirroring.

Mirrored: mirror source can be port or packet sent or received by CPU

Mirror: mirror port can be only one. If multiple mirror port is configured, the last will be effective.

Note: Mirror port cannot be used as a normal port.

5.1.3 Configuring Port Mirroring

Table 24 Mirroring functions and related command

FUNCTION	SPECIFICATIONS	RELATED COMMAND	LINK
Mirroring	Traffic mirroring	mirrored-to no mirrored-to	QoS Configuration
	Port mirroring	mirror destination-interface mirror source-interface	Configuring Port Mirroring

5.1.4 Mirroring Configuration

For mirroring features, see [Overview](#).

5.1.4.1 Configuring Traffic Mirroring

Configuration prerequisites

- ACLs for identifying traffics have been defined. For defining ACLs, see the description on the ACL module in QoS.
- The destination port has been defined.
- The port on which to perform traffic mirroring configuration and the direction of traffic mirroring has been determined.

Configuration procedure

Perform the configuration in global configuration mode.

Table 25 Configure traffic mirroring

OPERATION	COMMAND	DESCRIPTION
Configure traffic mirroring	mirrored-to { ip-group { acl-number acl-name } [subitem subitem] link-group { acl-number acl-name } [subitem subitem] } interface ethernet interface-num	The command is for traffic mirroring on the packets which meet ACL rules (only be effective on ACL permit rules). The destination port should be specified when using this command for the first time.
Cancel traffic mirroring	no mirrored-to { ip-group { acl-number acl-name } [subitem subitem] link-group { acl-number acl-name } [subitem subitem] }	

Note: `ip-group { acl-number | acl-name } [subitem subitem]`: Specifies a basic or an advanced ACL. The *acl-number* argument ranges from 2000 to 3999; *acl-name*: Name of a string, start with letters without space and quotation mark; *subitem*: option parameter for specifying the subitem in acl-list, in the range of 0 to 127.

`link-group { acl-number | acl-name } [subitem subitem]`: Specifies a Layer 2 ACL. The *acl-number* argument ranges from 4000 to 4999; *acl-name*: Name of a string, start with letters without space and quotation mark; *subitem*: option parameter for specifying the subitem in acl-list, in the range of 0 to 127.

`interface ethernet { interface-num }`: Specifies destination port (also called monitor port) of traffic.

Configuration example

! Mirror acl-list 2000 to Ethernet 0/0/1.

```
Switch(config)#access-list 2000 permit 1.1.1.1 0
Config ACL subitem successfully.
Switch(config)#mirrored-to ip-group 2000 interface ethernet 0/0/1
Config mirrored-to successfully .
```

5.1.4.2 Configuring Port Mirroring

Configuration prerequisites

- The source port is specified and whether the packets to be mirrored are ingress or egress is specified: **ingress**: only mirrors the packets received via the port; **egress**: only mirrors the packets sent by the port; **both**: mirrors the packets received and sent by the port at the same time.
- The destination port is specified.

Configuration procedure

Perform the following configuration in global configuration mode.

Table 26 Configure port mirroring

OPERATION	COMMAND	DESCRIPTION
Configure destination port (so called monitor port)	<code>mirror destination-interface interface interface-num</code>	This command will cancel original port mirroring.
Configure source port (so called mirrored port)	<code>mirror source-interface { interface-list cpu } { both egress ingress }</code>	both means both ingress and egress; cpu means mirroring cpu packets.
Show port mirroring	<code>show mirror</code>	

Note: A port cannot be monitor and mirrored port at the same time.

Configuration example

! Mirror egress of ethernet 0/0/1 to ethernet 0/0/12 to ethernet 0/1/1

```
Switch(config)#mirror destination-interface ethernet 0/1/1
Config monitor port successfully !
Switch(config)#mirror source-interface ethernet 0/0/1 to ethernet 0/0/12 egress
Config mirrored port successfully !
```

! Mirror cpu both to ethernet 0/1/2

```
Switch(config)#mirror destination-interface ethernet 0/1/2
Config monitor port successfully !
Switch(config)#mirror source-interface cpu both
Config mirrored port successfully !
```

Configuring Port Utilization Alarm

6.1 Brief Introduction to Device Utilization Alarm

The device utilization alarm is used to monitor port bandwidth utilization, CPU loading, the purpose is to provide network utilization and running status of the network and device for administrator.

- Exceed: when port bandwidth utilization over "exceed", it triggers congestion alarm.
- Normal: when port bandwidth utilization less "exceed", it triggers recover alarm CPU utilization alarm also can set two trigger values, details as below:
- Busy: when CPU utilization over "busy", it triggers alarm of CPU busyness
- Unbusy: when CPU utilization less "busy", it triggers alarm of CPU idle Notes, all alarms will show in the list of Syslog.

6.2 Configuring Device Utilization Alarm

6.2.1 Configuring Port Utilization Alarm

Using below commands to configure port utilization. Enable port utilization in system and port mode by default. The "exceed" value equals 850M, the "normal" value equals 600M.

Table 27 configuring port utilization alarm

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable(disable)port utilization alarm with system mode	<code>(no) alarm all-packets</code>	required
Enter port configuration	<code>interface ethernet <i>interface-num</i></code>	-
Enable(disable)port utilization alarm with port mode	<code>(no) alarm all-packets</code>	Required
Configure alarm value	<code>alarm all-packets threshold {<i>exceed threshold</i> <i>normal threshold</i> }</code>	Optional

6.2.2 Configuring CPU Utilization Alarm

Using below commands to configure CPU utilization. Enable CPU utilization by default. The “busy” value equals 90%, the “unbusy” value equals 60%

Table 28 configuring CPU utilization alarm

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable(disable) CPU utilization alarm	<code>(no) alarm cpu</code>	Required
Configure congestion value	<code>alarm cpu threshold <busy unbusy> busy_threshold_value unbusy unbusy_threshold_value</code>	optional

6.2.3 Displaying and Debugging Device Utilization Alarm

After finishing above configuration, you can show configuration by below commands.

Table 29 displaying and debugging device utilization alarm

OPERATION	COMMAND	REMARKS
Display the enable status and alarm value of CPU utilization alarm	<code>show alarm cpu</code>	Perform either of the commands
Display port utilization in system mode	<code>show alarm all-packets</code>	Perform either of the commands
Display port utilization and value in port mode	<code>show alarm all-packets interface [ethernet interface-num]</code>	Perform either of the commands

Link Aggregation Configuration

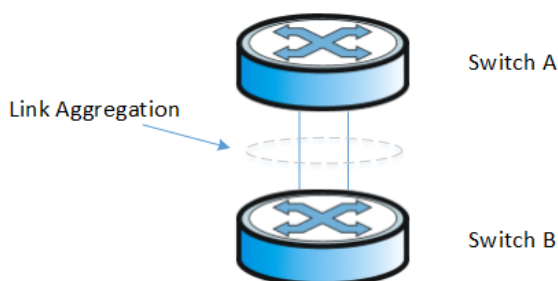
7.1 Overview

7.1.1 Introduction to Link Aggregation

Link aggregation means aggregating several ports together to form an aggregation group, the outgoing/incoming load will be shared among the member ports in the group and to enhance the connection reliability.

Depending on different aggregation modes, aggregation groups fall into two types: static LACP and dynamic LACP. Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.

Figure 9 Network diagram for link aggregation configuration



For the member ports in an aggregation group, the basic configuration must be the same. The basic configuration includes STP, QoS, VLAN, port attributes, and other associated settings.

- 1 STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, maximum transmission speed, loop prevention status.
- 2 QoS configuration, including traffic limiting, priority marking, default 802.1p priority, traffic monitor, traffic redirection, traffic statistics, and so on.
- 3 VLAN configuration, including permitted VLANs, and default VLAN ID, tag VLAN list for hybrid port and allowed VLAN list for trunk port.
- 4 Port attribute configuration, including port rate, duplex mode, and link type (Trunk, Hybrid or Access). The ports for a static aggregation group must have the same rate and link type, and the ports for a dynamic aggregation group must have the same rate, duplex mode (full duplex) and link type.

7.1.2 Introduction to LACP

The purpose of link aggregation control protocol (LACP) is to implement dynamic link aggregation. This protocol is based on IEEE802.3ad and uses LACPDUs (link aggregation control protocol data units) to implement.

After LACP is enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key (it is so called O-Key) of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated with the receiving port. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

7.1.3 Operation Key (O-Key)

An operation key of an aggregation port is generated by system depending on the configurations of the port (rate, duplex mode, other basic configuration, and administrative key) when the port is aggregated.

- 1 The ports in the same aggregation group must have the same operation key (O-Key) and administrative key (A-Key).
- 2 The administrative key (A-Key) and operation key (O-Key) of an LACP-enable aggregation port is equal to its aggregation group ID+1.
- 3 The administrative key (A-Key) and operation key (O-Key) of an LACP-enable aggregation port cannot be modified.
- 4 The operation key (O-Key) which is contained in LACPDU of an LACP-enable aggregation port is the same as its peer.

7.1.4 Static Aggregation Group

7.1.4.1 Introduction to Static Aggregation

A static aggregation group is manually created. All its member ports are manually added and can be manually removed. Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the whole aggregation group unless you remove the port.

LACP is disabled on the member ports of static aggregation groups, and enabling LACP on such a port will not take effect.

7.1.4.2 Port status of Static Aggregation Group

A port in a static aggregation group is only in one state: on, which means the port is in a static aggregation group. There can be at most 8 ports in a static aggregation group.

7.1.5 Dynamic LACP Aggregation Group

7.1.5.1 Introduction to Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed. Each dynamic aggregation group must contain at least one port. When a dynamic aggregation group contains only one port, you cannot remove the whole aggregation group unless you remove the port.

LACP is enabled on the member ports of dynamic aggregation groups, and disabling LACP on such a port will not take effect.

7.1.5.2 Mode of Dynamic Aggregation Group

The mode of dynamic aggregation group can be active or passive. It is manually set by users. The dynamic aggregation group in active mode will actively send LACPDUs; group in passive mode will only response LACPDUs passively. When interconnecting with another device, active mode can interconnect with both active and passive mode, but passive mode can only interconnect with active mode. The default mode is ACTIVE.

7.1.5.3 Port Status of Dynamic Aggregation Group

A port in a dynamic aggregation group can be in one of the three states: bundle (bndl), standby, and no-bundle (no-bndl). In dynamic aggregation group, only bundled ports can transceive LACP protocol packets; others cannot.

Note: In an aggregation group, the bundled port with the minimum port number serves as the master port of the group, and other bundled ports serve as member ports of the group.

No-bundled ports are the ports which fail to form link aggregation with other ports in the dynamic aggregation.

There is a limit on the number of bundled ports in an aggregation group. Therefore, if the number of the member ports that can be set as bundled ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

- 1 Compare device IDs (system priority and system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.
- 2 Compare port IDs (port priority and port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the bundled port and the left ports are standby ports.

7.1.5.4 Configuring System Priority

LACP determines the bundled and standby states of the dynamic aggregation group members according to the priority of the port on the end with the preferred device ID.

The device ID consists of system priority and system MAC address.

When two device IDs are compared, the system priorities are compared first, and the system MAC addresses are compared when the system priorities are the same. The device with smaller device ID will be considered as the preferred one.

Note: Changing the system priority of a device may change the preferred device between the two parties, and may further change the states (bundled or standby) of the member ports of dynamic aggregation groups.

7.1.5.5 Configuring Port Priority

LACP determines the bundled and standby states of the dynamic aggregation group members according to the port IDs on the device with the preferred device ID. When the number of members in an aggregation group exceeds the number of bundled ports supported by the device in each group, LACP determines the bundled and standby states of the ports according to the port IDs. The ports with superior port IDs will be set to bundled state and the ports with inferior port IDs will be set to standby state.

The port ID consists of port priority and port number. When two port IDs are compared, the port priorities are compared first, and the port numbers are compared if the port priorities are the same. The port with smaller port ID is considered as the preferred one.

7.2 Redundancy of Interconnected Device

LACP provides link redundancy mechanism to guarantee the redundancy conformity of the two interconnected devices and user can configure the redundant link which is realized by system and port priority. The steps are as following:

- 1 Selection reference. The two devices know the LACP sys-id and system MAC address of each other through LACPDUs exchanges. The system priorities are compared first, and then compare system MAC addresses. The device with smaller device ID will be considered as the preferred one.
- 2 Redundant link. The port priorities are compared first, and the port numbers are compared if the port priorities are the same. The port with smaller port ID is considered as the preferred one.

7.3 Load-balancing Policy

Load-balancing policy is specific physical link selection strategy to send packets, which can be source MAC, destination MAC, source and destination MAC, source IP, destination IP, and source and destination IP. The default strategy is source MAC.

7.4 Link Aggregation Configuration

Link aggregation configuration includes:

- [Configuring a Static Aggregation Group](#)
- [Configuring a Dynamic LACP Aggregation Group](#)

- [Displaying and Maintaining Link Aggregation Configuration](#)

7.4.1 Configuring a Static Aggregation Group

You can create a static aggregation group, or remove an existing static aggregation group (before that, all the member ports in the group are removed).

You can manually add/remove a port to/from a static aggregation group, and a port can only be manually added/removed to/from a static aggregation group.

Perform the configuration in global configuration mode.

Table 30 Configure a manual aggregation group

OPERATION	COMMAND	DESCRIPTION
Create a static aggregation group	<code>channel-group channel-group-number</code>	<i>channel-group-number</i> ranges from 0 to 12 If the group has already existed, turn to step 2.
Configure load-balancing policy	<code>channel-group load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}</code>	
Enter interface configuration mode	<code>interface ethernet interface_num</code>	Enter the port mode which you want to add to the aggregation group.
Enter interface range configuration mode	<code>interface range ethernet interface_list</code>	If there are multiple ports to be added, enter interface range mode.
Add a port to the aggregation group	<code>channel-group channel-group-number mode on</code>	<i>channel-group-number</i> should be existed .
Delete a port from an aggregation group	<code>no channel-group channel-group-number</code>	This command used in global configuration mode is for deleting a static aggregation group.
Back to global configuration mode	<code>exit</code>	
Delete a static aggregation group	<code>no channel-group channel-group-number</code>	This command used in interface configuration mode is for deleting a port from an aggregation group. Delete all ports from the group first before deleting the group.

7.4.2 Configuring a Dynamic LACP Aggregation Group

You can manually add/remove a port to/from a dynamic aggregation group, and a port can only be manually added/removed to/from a dynamic aggregation group.

Perform the configuration in global configuration mode.

Table 31 Configure a dynamic LACP aggregation groups

STEP	OPERATION	COMMAND	DESCRIPTION
1	Create a dynamic aggregation group	<code>channel-group channel-group-number</code>	<i>channel-group-number</i> ranges from 0 to 12 If the group has already existed, turn to step 2.
2	Configure load-balancing policy	<code>channel-group load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}</code>	The default policy is source mac.
3	Configure system priority	<code>lacp system-priority priority</code>	<i>priority</i> ranges from 1 to 65535. The default priority is 32768.
4(1)	Enter interface configuration mode	<code>interface ethernet interface_num</code>	Enter the port mode which you want to add to the aggregation group.
4(2)	Enter interface range configuration mode	<code>interface range ethernet interface_list</code>	If there are multiple ports to be added, enter interface range mode.
5	Add a port to the aggregation group	<code>channel-group channel-group-number mode {active passive}</code>	<i>channel-group-number</i> should be existed .
6	Configure port priority	<code>lacp port-priority priority</code>	<i>priority</i> ranges from 1 to 65535. The default priority is 128.
7	Delete a port from an aggregation group	<code>no channel-group channel-group-number</code>	This command used in global configuration mode is for deleting a static aggregation group.
8	Back to global configuration mode	<code>exit</code>	
9	Delete a dynamic aggregation group	<code>no channel-group channel-group-number</code>	This command used in interface configuration mode is for deleting a port from an aggregation group. Delete all ports from the group first before deleting the group.

7.4.3 Displaying and Maintaining Link Aggregation Configuration

After the above configuration, execute the show command in any mode to display the running status after the link aggregation configuration and verify your configuration.

Table 32 Display and maintain link aggregation configuration

OPERATION	COMMAND	DESCRIPTION
Show system LACP ID	<code>show lacp sys-id</code>	System LACP-ID consists of 16-bit system priority and 48-bit system MAC.
Show port member info of the aggregation group	<code>show lacp internal [channel-group-number]</code>	
Show neighbor port info of the aggregation group	<code>show lacp neighbor [channel-group-number]</code>	

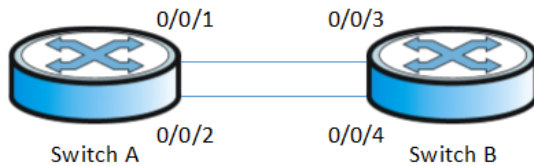
7.5 LACP Configuration Example

Network requirements

As shown in [Figure 10 on page 56](#), the link between switch-A and switch-B should be more reliable. switch-A and switch-B should realize load-balance.

Network diagram

Figure 10 LACP network diagram



Configuration procedure

1 Create channel-group

#Configure switch-A

```
switch-A#configure terminal
switch-A(config)#channel-group 1
```

#Configure switch-B

```
switch-B#configure terminal
switch-B(config)#channel-group 1
```

2 Configure channel-group load-balance

#Configure switch-A

```
switch-A(config)#channel-group load-balance src-dst-mac
```

#Configure switch-B

```
switch-B(config)#channel-group load-balance src-dst-mac
```

3 Configure LACP system and port priority

#Configure switch-A

```
switch-A(config)#lacp system-priority 1024
switch-A(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
switch-A(config-if-range)#lacp port-priority 64
switch-A(config-if-range)#exit
```


#Configure switch-B

```
switch-B(config)#lacp system-priority 2048
switch-B(config)#interface range ethernet 0/0/3 to ethernet 0/0/4
switch-B(config-if-range)#lacp port-priority 256
switch-B(config-if-range)#exit
```

4 Add port member for channel-group**4a Static****#Configure switch-A**

```
switch-A(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
switch-A(config-if-range)#channel-group 1 mode on
Remember to re-config mac-addresses associated with port e0/0/1
Remember to re-config mac-addresses associated with port e0/0/2
```

#Configure switch-B

```
switch-B(config)#interface range ethernet 0/0/3 to ethernet 0/0/4
switch-B(config-if-range)#channel-group 1 mode on
Remember to re-config mac-addresses associated with port e0/0/3
Remember to re-config mac-addresses associated with port e0/0/4
```

4b Dynamic**#Configure switch-A**

```
switch-A(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
switch-A(config-if-range)#channel-group 1 mode active
Remember to re-config mac-addresses associated with port e0/0/1
Remember to re-config mac-addresses associated with port e0/0/2
```

#Configure switch-B

```
switch-B(config)#interface range ethernet 0/0/3 to ethernet 0/0/4
switch-B(config-if-range)#channel-group 1 mode passive
Remember to re-config mac-addresses associated with port e0/0/3
Remember to re-config mac-addresses associated with port e0/0/4
```

5 Check the configuration

5a show lacp internal

```
#show lacp internal of switch-A
switch-A(config-if-range)#show lacp internal
Load balance: src-dst-mac

Channel: 1, static channel
Port      State   A-Key  O-Key  Priority  Logic-port  Actor-state
e0/0/1    bndl    -      -      -         1           -
e0/0/2    bndl    -      -      -         1           -

actor-state: activity/timeout/aggregation/synchronization
              collecting/distributing/defaulted/expired
```

#show lacp internal of switch-A

```
switch-A(config-if-range)#show lacp internal
Load balance: src-dst-mac

Channel: 1, dynamic channel
Port      State   A-Key  O-Key  Priority  Logic-port  Actor-state
e0/0/1    bndl    2      2      64        1           10111100
e0/0/2    bndl    2      2      64        1           10111100

actor-state: activity/timeout/aggregation/synchronization
              collecting/distributing/defaulted/expired
```

#show lacp internal of switch-B

```
switch-B(config-if-range)#show lacp internal
Load balance: src-dst-mac

Channel: 1, dynamic channel
Port      State   A-Key  O-Key  Priority  Logic-port  Actor-state
e0/0/3    bndl    2      2      256       3           00111100
e0/0/4    bndl    2      2      256       3           00111100

actor-state: activity/timeout/aggregation/synchronization
              collecting/distributing/defaulted/expired
```

5b Show LACP neighbor**#Show LACP neighbor of switch-A**

```
switch-A(config-if-range)#show lacp neighbor
Channel: 1
Local  Port  Key  Pri  ID              Timeout  Nei-state
e0/0/1  3      2    256  000a5a020305   82(90)  00111100
e0/0/2  4      2    256  000a5a020305   80(90)  00111100

nei-state: activity/timeout/aggregation/synchronization
              collecting/distributing/defaulted/expired
```

#Show LACP neighbor of switch-B

```
switch-B(config-if-range)#show lacp neighbor
Channel: 1
Local    Port    Key    Pri    ID                Timeout    Nei-state
e0/0/3   1        2      64     000a5a010203     71(90)    10111100
e0/0/4   2        2      64     000a5a010203     69(90)    10111100

nei-state: activity/timeout/aggregation/synchronization
           collecting/distributing/defaulted/expired
```

5c Show system ID**#Show switch-A system ID**

```
switch-A(config-if-range)#show lacp sys-id
1024,000a5a010203
```

#Show switch-B system ID

```
switch-B(config-if-range)#show lacp sys-id
2048,000a5a020305
```

6 Delete port member from channel-group**#Configure switch-A**

```
switch-A(config-if-range)#no channel-group 1
Remember to re-config mac-addresses associated with port e0/0/1
Remember to re-config mac-addresses associated with port e0/0/2
switch-A(config-if-range)#exit
```

#Configure switch-B

```
switch-B(config-if-range)#no channel-group 1
Remember to re-config mac-addresses associated with port e0/0/3
Remember to re-config mac-addresses associated with port e0/0/4
switch-B(config-if-range)#exit
```

7 Delete channel-group

```
#Configure switch-A
switch-A(config)#no channel-group 1
#Configure switch-B
switch-B(config)#no channel-group 1
```

Port Isolation Configuration

8.1 Introduction to Port Isolation

To implement Layer 2 isolation, you can add each port to different VLANs. However, this will waste the limited VLAN resource. With adding ports into the isolation group, the ports can be isolated within the same VLAN. This provides you with more free secure and flexible networking schemes.

On the current device:

- Currently, only one isolation group is supported on a device, which is created automatically by the system. The user cannot remove the isolation group or create other isolation groups.
- The maximum number of entries in an isolation group is total -1. Because isolated ports are downlink ports. There should be at least one uplink port.

Note: When a port in an aggregation group is configured as the member of isolation group, the other ports of the aggregation group will not be downlink ports.

8.2 Port Isolation Configuration

8.2.1 Port Isolation Configuration

All ports are uplink port in default. Before user want to set specific uplink port, it is necessary to delete all uplink ports.

Table 33 Configure port isolation

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port mode	<code>interface ethernet device/slot/port</code>	
Delete all uplink ports	<code>no port-isolation uplink all</code>	Required
Set specific uplink port	<code>port-isolation uplink ethernet device/slot/port</code>	Required
Show port-isolation configuration	<code>Show port-isolation</code>	On any mode

8.3 Port-isolation Configuration Example

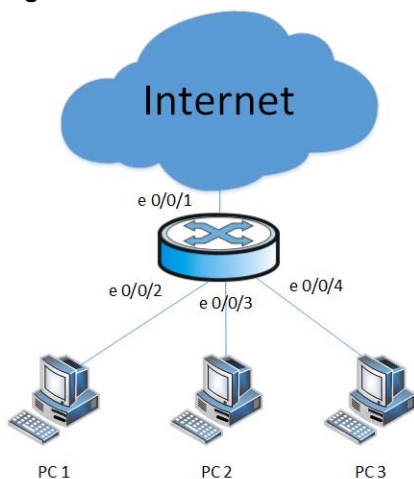
8.3.1 Port-isolation Configuration Example

Network requirements

User PC1, PC2, PC3 connect to switch e0/0/2, e0/0/3, e0/0/4. Switch connects to Internet by e0/0/1. User PC1, PC2, PC3 need independent data exchange.

Networking diagram

Figure 11



Configuration procedure

```
Switch#configure terminal
Switch(config)#isolate-port ethernet 0/0/2 to ethernet 0/0/4
Add port isolation downlink port successfully.
Switch(config)#show isolate-port
Port isolation downlink port :
e0/0/2-e0/0/4
```

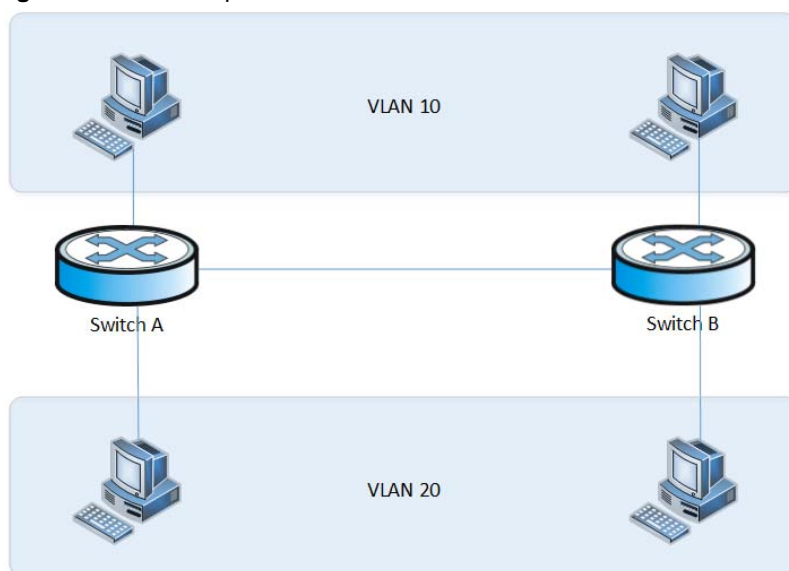
9.1 VLAN Overview

Virtual Local Area Network (VLAN) groups the devices of a LAN logically but not physically into segments to implement the virtual workgroups. IEEE issued the IEEE 802.1Q in 1999, which was intended to standardize VLAN implementation solutions.

Through VLAN technology, network managers can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demand. The workstations of a VLAN do not have to belong to the same physical LAN segment.

With VLAN technology, the broadcast and unicast traffic within a VLAN will not be forwarded to other VLAN, therefore, it is very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.

Figure 12 VLAN implementation



A VLAN can span across multiple switches, or even routers. This enables hosts in a VLAN to be dispersed in a looser way. That is, hosts in a VLAN can belong to different physical network segment.

Compared with the traditional Ethernet, VLAN has the following advantages.

- 1 Broadcasts are confined to VLAN. This decreases bandwidth utilization and improves network performance.

- 2 Network security is improved. VLAN cannot communicate with each other directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 switches are used.
- 3 Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you need not change its network configuration.

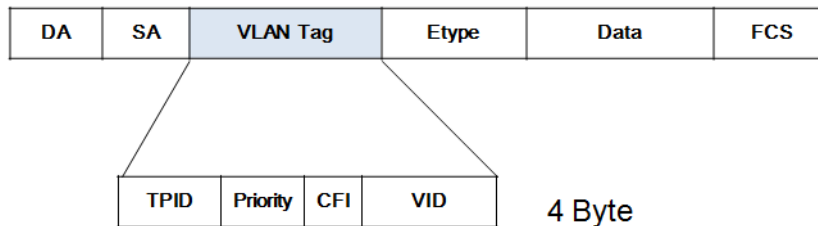
9.2 VLAN Principles

VLAN tags in the packets are necessary for the switch to identify packets of different VLAN. The switch works at Layer 2 (Layer 3 switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into only the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

Figure 13 Format of VLAN tag



As shown in [Figure 13 on page 63](#), a VLAN tag contains four fields, including TPID (Tag Protocol Identifier), priority, CFI (Canonical Format Indicator), and VID (VLAN ID).

- **TPID** is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100.
- **Priority** is a 3-bit field, referring to 802.1p priority. Refer to [Section 19.1.3 on page 129](#) for details.
- **CFI** is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.
- **VID (VLAN ID)** is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

The network devices use VLAN ID to identify VLAN which the frame belongs in. When the switch receives an un-VLAN-tagged packet, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission. For the details about setting the default VLAN of a port, refer to section "02-Port Configuration"

9.3 802.1Q VLAN

9.3.1 VLAN Link Type of Ethernet Ports

An Ethernet port can operate in one of the three link types:

- Access: An access port only belongs to one VLAN, normally used to connect user device.
- Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLAN and is generally used to connect another switch. The packet sent from this port can only be with tag label.
- Hybrid: A hybrid port can belong to multiple VLANs, can receive, or send packets for multiple VLANs, used to connect either user or network devices. It allows packets of multiple VLANs to be sent with or without the Tag label

9.3.2 Default VLAN

Details refer to 02-Port configuration.

9.3.3 Handling Packets

Different ports have different ways to handle the packet. Details are in [Table 34 on page 64](#).

Table 34 Different port handles different packet

PORT TYPE	INGRESS		EGRESS
	UNTAGGED PACKET	TAGGED PACKET	
Access port	Receive it and add a tag with VID being equal to PVID.	If VID of the packet is equal to the port permitted VID, receive it; if VID is different, discard it.	Strip the Tag and transmit the packet as the VID of the packet is equal to the port permitted VID
Hybrid port			If VID of the packet is equal to the port permitted untag VID, remove the tag and transmit it; If VID of the packet is equal to the port permitted tag VID, keep the tag and transmit it.
Trunk port			If VID of the packet is equal to the port permitted VID, keep the tag and transmit it.

9.4 VLAN Configuration

9.4.1 Default VLAN Configuration

Table 35 Default VLAN configuration

PARAMETER	DEFAULT	DESCRIPTION
Existed VLAN	VLAN 1	The vlan-id argument ranges from 1 to 4,094. VLAN 1 is the default VLAN of all ports.
VLAN description	/	VLAN description is characters ranged from 1 to 32.
Port member of VLAN	All ports are the members of VLAN 1.	

9.4.2 Create and Modify VLAN

Switch supports 4094 VLANs.

Perform following commands in privilege mode.

Table 36 Create and modify VLAN

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Create a VLAN and enter VLAN configuration mode	<code>VLAN vlan-list</code>	Required
Add port member to a VLAN	<code>switchport ethernet device /slot / port</code>	Required
Configure VLAN description	<code>description string<1-32></code>	Optional
Display the related information about VLAN	<code>show vlan vlan-id / brief</code>	Optional

9.4.3 Configure VLAN Access Port

Table 37 Configuration of VLAN Access Port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	/
Enter port configuration mode	<code>interface ethernet device/slot/port</code>	/
Set VLAN port mode	<code>switchport mode access</code>	Required, default value is hybrid
Recover VLAN port mode	<code>no switchport mode</code>	Optional
Set access port default VLAN	<code>switchport default vlan vlan-id</code>	VLAN has to be created
Recover VLAN port default VLAN	<code>no switchport default vlan</code>	Optional
Display VLAN configuration	<code>show vlan vlan-id/brief</code>	Any mode

9.4.4 Configure VLAN Trunk Port

Table 38 Configure VLAN trunk port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	/
Enter port configuration mode	<code>interface ethernet device/slot/ port</code>	/
Set VLAN port mode	<code>switchport mode trunk</code>	Required, default value is hybrid
Recover VLAN port mode	<code>no switchport mode</code>	Optional
Set access port default VLAN	<code>switchport default vlan vlan-id</code>	VLAN has to be created
Recover VLAN port default VLAN	<code>no switchport default vlan</code>	Optional
Set allowed VLAN on the trunk port	<code>switchport trunk allowed vlan { all vlan-id}</code>	Required
Delete allowed VLAN on the trunk port	<code>no switchport trunk allowed vlan { all vlan-id}</code>	Optional
Display VLAN configuration	<code>show vlan vlan-id/brief</code>	Any mode

When the VLAN ID of the frame satisfies the port's default VLAN, switch strips the VLAN tag, then transmits frame.

9.4.5 Configure VLAN Hybrid Port

Table 39 Configuration of VLAN Hybrid Port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	/
Enter port configuration mode	<code>interface ethernet device/slot/ port</code>	/
Set VLAN port mode	<code>switchport mode hybrid</code>	Required, default value is hybrid
Recover VLAN port default VLAN	<code>no switchport default vlan</code>	Optional
Set allowed VLAN on the hybrid port	<code>switchport hybrid { tagged untagged } vlan { all vlan-id }</code>	Required
Delete allowed VLAN in the hybrid port	<code>no switchport hybrid { tagged untagged } vlan { all vlan-id }</code>	Optional
Display VLAN configuration	<code>show vlan vlan-id/brief</code>	Any mode

9.4.6 Delete Port Members from a VLAN

Perform following commands in privilege mode.

Table 40 Delete port members from a VLAN

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	/
Enter VLAN configuration mode	<code>vlan vlan-list</code>	/
Delete port member from VLAN	<code>no switchport { all ethernet port_list }</code>	Required
Display the related information about VLAN	<code>show vlan vlan-id / brief</code>	Optional

Note: A port whose VLAN should not be the default VLAN.

9.4.7 Delete VLAN

Perform following commands in global configuration mode.

Table 41 Delete vlan

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Delete VLAN	<code>no vlan {vlan-list all}</code>	Required
Display the related information about VLAN	<code>show vlan vlan-id / brief</code>	optional

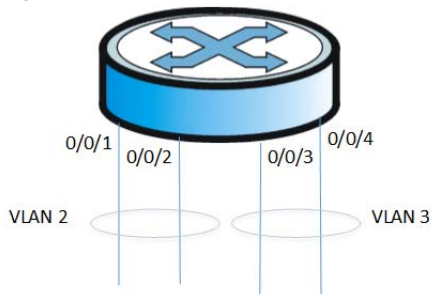
Note: After performing `no vlan all`, system will delete all vlan except VLAN 1. In other words, VLAN 1 cannot be deleted.

The VLAN to be removed cannot exist in the multicast group. So please remove the related multicast group first.

9.4.8 VLAN Configuration Example

Networking Requirements

Create VLAN2 and VLAN3. Add GigabitEthernet0/0/1 and GigabitEthernet0/0/2 to VLAN2 and add GigabitEthernet0/0/3 and GigabitEthernet0/0/4 to VLAN3. Delete GigabitEthernet0/0/1 to GigabitEthernet0/0/4 from VLAN1.

Figure 14 Networking diagram**Networking configuration**

! Create VLAN 2 and enter it.

```
Switch(config)# vlan 2
```

! Add Ethernet0/01 and Ethernet0/02 to VLAN2.

```
Switch(config-if-vlan)#switchport ethernet 0/0/1 ethernet 0/0/2
```

! Create VLAN 3 and enter it.

```
Switch(config)# vlan 3
```

! Add Ethernet0/0/3 and Ethernet0/0/4 to VLAN3.

```
Switch(config-if-vlan)#switchport ethernet 0/0/3 ethernet 0/0/4
```

! Set the default vlan of Ethernet0/0/1and Ethernet0/0/2

```
Switch(config)#interface range ethernet 0/0/1 to ethernet 0/0/2
Switch(config-if-range)# switchport default vlan 2
```

! Set the default vlan of Ethernet0/0/3 and Ethernet0/0/4

```
Switch(config)#interface range ethernet 0/0/3 to ethernet 0/0/4
Switch(config-if-range)# switchport default vlan 3
```

! Enter VLAN view and delete Ethernet0/0/1 to Ethernet0/0/4 from VLAN1.

```
Switch(config)#vlan 1
Switch(config-if-vlan)#no switchport ethernet 0/0/1 to ethernet 0/0/4
```

GVRP Configuration

10.1 Brief Introduction to GVRP

10.1.1 GARP

Generic Attribute Registration Protocol (GARP) provides a mechanism that allows participants in a GARP application to distribute, propagate and register with other participants in a bridged LAN that attributes specific to the GARP applications, such as the VLAN or multicast address attribute.

GARP itself does not exist on a device as an entity. GARP-compliant application entities are called GARP applications. It primarily applies to GVRP and GMRP. When a GARP application entity is present on a port on your device, this port is regarded as a GARP application entity.

The GARP mechanism allows the configuration of a GARP participant to propagate throughout a LAN quickly. In GARP, a GARP participant registers or deregisters its attributes with other participants by making or withdrawing declarations of attributes and at the same time, based on received declarations or withdrawals handles attributes of other participants.

GARP participants exchange attributes primarily by sending the following three types of messages: Join, Leave and LeaveAll.

- Join to announce the willingness to register some attribute with other participants.
- Leave to announce the willingness to deregister with other participants.
- LeaveAll to deregister all attributes. A LeaveAll message is sent upon expiration of a LeaveAll timer, which starts upon the startup of a GARP application entity.

Together with Join messages and Leave messages help GARP participants complete attribute registration and deregistration. All the attributes messages can forward to all switches in the same network.

GARP application entities send protocol data units (PDU) with a particular multicast MAC address as destination. Based on this address, a device can identify to which GVRP application, GVRP for example, should a GARP PDU be delivered.

GARP is described in IEEE 802.1Q.

10.1.2 GVRP

GVRP is an application of GARP. It functions based on the operating mechanism of GARP to maintain and propagate dynamic VLAN registration information for the GVRP devices on the network. It thus ensures that all GVRP participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

10.2 Configuring GVRP

10.2.1 Brief Introduction to GVRP Configuration

Table 42 GVRP configuration

CONFIGURATION		REMARK	DETAILED CONFIGURATION
Configure GVRP	Startup GVRP	required	10.2.3
	Configure VLAN under GVRP	required	10.2.4
Display and maintain GVRP		optional	10.2.5

10.2.2 Port Configuration

Table 43 port configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	required
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	required

10.2.3 Startup GVRP

Before enabling GVRP on a port, you must enable GVRP globally because it disables in default.

Notes: you need to configure the port trunk to enable GVRP.

Table 44 startup GVRP

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable GVRP in global configuration mode	<code>gvrp</code>	required
Disable GVRP in global configuration mode	<code>no gvrp</code>	required
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Enable GVRP in port configuration mode	<code>(no) gvrp</code>	required

10.2.4 Configuring VLAN Forwarded by GVRP

Obviously VLAN registration information forwarded by GVRP can be the local configuration static VLAN, or be learned by GVRP dynamic protocols. But when the administrator names, the permit VLANs can pass through the port to send GVRP packets.

Table 45 Configure VLAN forwarded by GVRP

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure VLAN forwarded by GVRP	<code>(no) garp permit vlan <i>vlan-list</i></code>	required

10.2.5 Displaying and Debugging

You can show the configuration through below commands when you finish all above configuration.

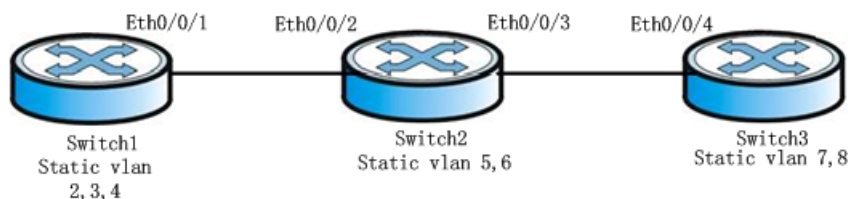
Table 46 displaying GVRP and debugging

OPERATION	COMMAND	REMARKS
Show GVRP enable globally	<code>show gvrp</code>	Perform in any configuration mode
Show port enable maintained by GVRP	<code>show gvrp interface [ethernet device/slot/port]</code>	
Show GVRP permit VLAN	<code>show garp permit vlan</code>	

10.2.6 GVRP Configuration Examples

As below, S1 and S3 forward respective static VLAN information to S2 by GVRP protocol, S2 forwards to each other with local static and learning VLAN from GVRP. At the end, S1, S2, S3 can share the dynamic VLAN information.

Figure 15 network



Configuration procedure:

!Configure S1

!Preparation before configure

```
Switch(config)#vlan 2,3,4
Switch(config-if-vlan)#switchport ethernet 0/0/1
Add VLAN port successfully.
Switch(config-if-vlan)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport mode trunk
Switch(config-if-ethernet-0/0/1)#exit
```

!Configure GVRP

```
Switch(config)#gvrp
Turn on GVRP successfully.
Switch(config)#garp permit vlan 2,3,4
Switch(config)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#gvrp
Switch(config-if-ethernet-0/0/1)#exit
```

!Verify GVRP configuration

```
Switch(config)#show gvrp
GVRP state : enable
Switch(config)#show gvrp interface ethernet 0/0/1
port      GVRP status
e0/0/1    enable
Total entries: 1.
Switch(config)#show garp permit vlan
VLAN 1 is Garp default permit VLAN
Other Garp permit VLAN : 2-4
```

!Configure S2

!Preparation before configure

```
Switch(config)#vlan 5,6
Switch(config-if-vlan)#switchport ethernet 0/0/2
Add VLAN port successfully.
Switch(config-if-vlan)#switchport ethernet 0/0/3
Add VLAN port successfully.
Switch(config-if-vlan)#exit
Switch(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)#exit
```

!Configure GVRP

```
Switch(config)#gvrp
Turn on GVRP successfully
Switch(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Switch(config-if-range)#gvrp.
Switch(config)#garp permit vlan 5,6
```


!Verify GVRP configuration

```
Switch(config)#show gvrp
GVRP state : enable
Switch(config)#show gvrp interface ethernet 0/0/2 ethernet 0/0/3
port      GVRP status
e0/0/2    enable
e0/0/3    enable
Total entries: 2.
Switch(config)#show garp permit vlan
VLAN 1 is Garp default permit VLAN
Other Garp permit VLAN : 5-6
```

!Configure S3

!Preparation before configure

```
Switch(config)#vlan 7,8
Switch(config-if-vlan)#switchport ethernet 0/0/4
Add VLAN port successfully.
Switch(config-if-vlan)#interface e 0/0/4
Switch(config-if-ethernet-0/0/4)#switchport mode trunk
```

!Configure GVRP

```
Switch(config)#gvrp
Turn on GVRP successfully.
Switch(config)#interface e 0/0/4
Switch(config-if-ethernet-0/0/4)#gvrp
Switch(config)#garp permit vlan 7,8
```

!Verify GVRP configuration

```
Switch(config)#show gvrp
GVRP state : enable

Switch(config)#show gvrp interface ethernet 0/0/4
port      GVRP status
e0/0/4    enable
Total entries: 1.

Switch(config)#show garp permit vlan
VLAN 1 is Garp default permit VLAN
Other Garp permit VLAN : 7-8
```

After finishing the configuration, you can show VLAN to check the VLAN register information learned by GVRP

!VLAN5,6,7,8 is learned by GVRP when showing S1 VLAN information

```
Switch(config)#show vlan
show VLAN information
VLAN ID          : 1
VLAN status      : static
VLAN member      : e0/0/1-e0/2/2
Static tagged ports : e0/0/1
Static untagged Ports : e0/0/2-e0/2/2
Dynamic tagged ports :
```

```
show VLAN information
VLAN ID          : 2
VLAN status      : static
VLAN member      : e0/0/1.
Static tagged ports : e0/0/1.
Static untagged Ports :
Dynamic tagged ports :
```

```
show VLAN information
VLAN ID          : 3
VLAN status      : static
VLAN member      : e0/0/1.
Static tagged ports : e0/0/1.
Static untagged Ports :
Dynamic tagged ports :
```

```
show VLAN information
VLAN ID          : 4
VLAN status      : static
VLAN member      : e0/0/1.
Static tagged ports : e0/0/1.
Static untagged Ports :
Dynamic tagged ports :
```

```
show VLAN information
VLAN ID          : 5
VLAN status      : dynamic
VLAN member      : e0/0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/0/1
```

```
show VLAN information
VLAN ID          : 6
VLAN status      : dynamic
VLAN member      : e0/0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/0/1
```

```
show VLAN information
VLAN ID          : 7
VLAN status      : dynamic
VLAN member      : e0/0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/0/1
```

```
show VLAN information
VLAN ID          : 8
VLAN status      : dynamic
VLAN member      : e0/0/1
Static tagged ports :
Static untagged Ports :
Dynamic tagged ports : e0/0/1

Total entries: 8 vlan.
```

ARP Configuration

11.1 ARP Overview

11.1.1 ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

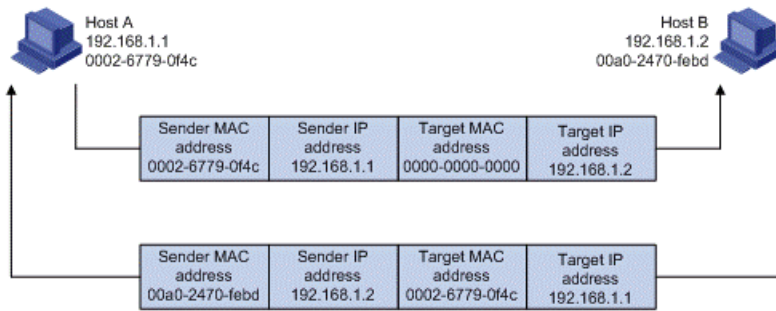
An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (such as the MAC address) of the destination host. To this end, the IP address must be resolved into the corresponding data link layer address.

Unless otherwise stated, the data link layer addresses that appear in this chapter refer to the 48-bit Ethernet MAC addresses.

ARP Address Resolution Process as below:

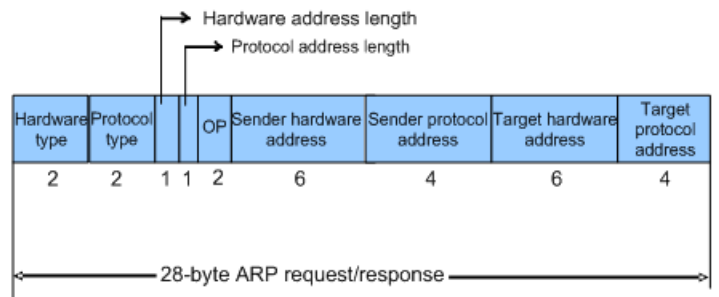
Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B, as show in [Figure 16 on page 77](#). The resolution process is as follows:

- 1 Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
- 2 If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process the request.
- 3 Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address into its ARP mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
- 4 After receiving the ARP reply, Host A adds the MAC address of Host B into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

Figure 16 ARP Address Resolution Process

When Host A and Host B are not on the same subnet, Host A first sends an ARP request to the gateway. The destination IP address in the ARP request is the IP address of the gateway. After obtaining the MAC address of the gateway from an ARP reply, Host A encapsulates the packet and sends it to the gateway. Subsequently, the gateway broadcasts the ARP request, in which the destination IP address is the one of Host B. After obtaining the MAC address of Host B from another ARP reply, the gateway sends the packet to Host B.

11.1.2 ARP Message Format

Figure 17 ARP Message Format

The following explains the fields in [Figure 17 on page 77](#).

Hardware type: This field specifies the hardware address type. The value "1" represents Ethernet.

Protocol type: This field specifies the type of the protocol address to be mapped. The hexadecimal value "0x0800" represents IP.

Hardware address length and protocol address length: They respectively specify the length of a hardware address and a protocol address, in bytes. For an Ethernet address, the value of the hardware address length field is "6". For an IPv4 address, the value of the protocol address length field is "4".

OP: Operation code. This field specifies the type of ARP message. The value "1" represents an ARP request and "2" represents an ARP reply.

Sender hardware address: This field specifies the hardware address (layer 2 MAC address) of the device sending the message.

Sender protocol address: This field specifies the protocol address (IPv4 address) of the device sending the message.

Target hardware address: This field specifies the hardware address (layer 2 MAC address) of the device the message is being sent to.

Target protocol address: This field specifies the protocol address (IPv4 address) of the device the message is being sent to.

11.2 Configuring ARP

11.2.1 Brief Configuration Guide of ARP

Table 47 Brief Configuration Guide of ARP

OPERATION	COMMAND	REMARKS
ARP table	Optional	11.2.2
ARP peer	Optional	11.2.3
ARP overwrite	Optional	11.2.4
Linkup gratuitous-arp	Optional	11.2.5
Arp-reply-repeat	Optional	11.2.6
Arp probe	Optional	11.2.7
Arp proxy	Optional	11.2.8

11.2.2 ARP Table

The device can learn and cache the IP to Media Access Control (MAC) mapping information when it receives an ARP packet or you can configure static ARP entries for IP to Media Access Control (MAC) translations. Layer 2 switches only support dynamic ARP entries; Layer 3 switches support dynamic and static ARP entries.

- 1 Dynamic ARP entries: ARP protocol learn and create IP-MAC mapping entries upon receiving ARP packets automatically, and ARP entries can be removed through ARP cache entry aging, updated upon new ARP packets, or override by a static ARP entry.
- 2 Static ARP entries: a static ARP entry is configured and maintained manually; it will never age, and will not be overwritten by dynamic ARP entries.

Static ARP entries support two types:

- Short static ARP entries.
- Long static ARP entries.

In short static ARP entry, you only need to configure the IP address and MAC address entries. Short static ARP entry cannot be directly used to forward packets. When you need to use a short static ARP entry, first send an ARP request packet, if the received response packets source IP address and source MAC address and the configured IP address and MAC address are the same, the ARP entries full complement, and then it can be used for forwarding IP data packets.

When configuring a long static ARP entry, in addition to configure the IP address and MAC address, you must also configure VLAN and output port. Long static ARP entry can be directly used to forward packets.

When manually configuring a long static ARP entry, the IP address and output VLAN port need located in the same network segment, otherwise it cannot be added successfully.

Table 48 Configure ARP Table

STEP	COMMAND	OPERATION
Enter global configuration mode	<code>configure terminal</code>	
Configure short static ARP entry	<code>arp {ipaddress mac mac }</code>	
Configure long static ARP entry	<code>arp {ipaddress mac mac vid vid port port }</code>	
Configure dynamic ARP table aging time	<code>arp aging-time aging-time</code>	The default is 20min
Bind dynamic ARP entries to static ARP entries	<code>arp bind dynamic {ipaddress all}</code>	
Remove ARP entries	<code>no arp {dynamic static all ipaddress }</code>	
Display ARP table	<code>show arp {dynamic static all}</code>	

11.2.3 ARP Peer

ARP Peer only learns the ARP packets coming from the designated ports, and the ARP packets coming from other ports will not learn.

Table 49 Configure ARP Peer

STEP	COMMAND	OPERATION
Enter global configuration mode	<code>configure terminal</code>	
Configure ARP peer port	<code>arp peer {ipaddress mac port}</code>	
Remove ARP peer table	<code>no arp peer</code>	

11.2.4 ARP Overwrite

With this command, configure the switch to handle ARP conflict situations, ARP conflict updated entry when this feature is enabled on a port, or not treated.

Table 50 Configure ARP Overwrite

STEP	COMMAND	OPERATION
Enter port configuration	<code>interface ethernet device/slot/port</code>	
Enable ARP overwrite	<code>arp overwrite</code>	The default is disabled
Disable ARP overwrite	<code>no arp overwrite</code>	

11.2.5 Linkup Gratuitous-ARP

By default, switch will not actively send gratuitous ARP packets from the port when this port linkup, in order to detect IP conflicts, it can be configured to send gratuitous ARP packets when this port linkup.

Table 51 Configure Linkup Gratuitous-ARP

STEP	COMMAND	OPERATION
Enter port configuration	<code>interface ethernet device/ slot/port</code>	
Enable linkup gratuitous-ARP	<code>linkup gratuitous-arp</code>	The default is disabled
Disable linkup gratuitous-ARP	<code>no linkup gratuitous-arp</code>	

11.2.6 ARP-Reply-Repeat

By default, the switch in response to a response packet only for each ARP request packets. You should be configured to support certain port for each ARP request packet in response to multiple ARP reply packets.

Table 52 Configure ARP-Reply-Repeat

STEP	COMMAND	OPERATION
Enter global configuration mode	<code>configure terminal</code>	
Configure ARP repeat interval and times	<code>arp-reply-repeat interval interval times times</code>	The default repeat interval is 20 ms (in milliseconds), times is 1.
Enter port configuration	<code>interface ethernet device/ slot/port</code>	
Enable ARP-replay-repeat	<code>arp-reply-repeat</code>	The default is disabled
Disable ARP-replay-repeat	<code>no arp-reply-repeat</code>	

11.2.7 ARP Probe

The principle is set the status of the ARP entry corresponds to the ARP probe IP address to ARP PROBE state, and the aging time as retransmission interval. If you receive an ARP replay, updating ARP entry aging time to normal value (20 minutes), otherwise retransmission, if the retransmission number reaches yet to receive a reply, then delete this ARP entry.

Table 53 Configure ARP Probe

STEP	COMMAND	OPERATION
Enter global configuration mode	<code>configure terminal</code>	
Configure ARP probe IP	<code>arp probe ip {ip}</code>	The up limit is 4 IPs
Remove ARP probe IP	<code>no arp probe ip {all ip}</code>	

Table 53 Configure ARP Probe

STEP	COMMAND	OPERATION
Configure ARP probe parameters	<code>arp probe [poll-timer value / retransmit {count value / interval value }]</code>	Poll-timer: 60-300s (the default value is 180s) Count: 2-5 (the default is 3) Interval: 1-3s (the default value is 3s)
Display ARP probe	<code>show arp probe</code>	

when arp-probe process is running (arp probe ip command has been configured), poll-timer is not configurable.

11.2.8 ARP Proxy

arp-proxy: because ARP request packets are broadcast packets cannot cross VLAN, if you enable the ARP proxy function, you can make ARP hosts under the same superVLAN can transmit APR packets, so that each interface under the superVLAN can communicate.

arp-proxy broadcast: allow to route ARP broadcast packets from any sub-VLAN to the other sub-VLAN.

Table 54 Configure ARP Proxy

STEP	COMMAND	OPERATION
Enter VLAN configuration mode	<code>vlan <vlanid></code>	
Enable ARP proxy	<code>arp-proxy</code>	
Disable ARP proxy	<code>no arp-proxy</code>	Optional
Enable ARP proxy broadcast	<code>arp-proxy broadcast</code>	Optional
Disable ARP proxy broadcast	<code>no arp-proxy broadcast</code>	Optional
Display ARP proxy	<code>show arp-proxy</code>	

11.3 Configuring ARP Attack Spoofing

11.3.1 Brief Introduction to ARP Spoofing

ARP provides no security mechanism and thus is prone to network attacks. An attacker can construct and send ARP packets, thus threatening network security.

A forged ARP packet has the following characteristics:

- The sender MAC address or target MAC address in the ARP message is inconsistent with the source MAC or destination MAC address in the Ethernet frame.
- The mapping between the sender IP address and the sender MAC address in the forged ARP message is not the true IP-to-MAC address binding of a valid client.

ARP attacks bring many malicious effects. Network communications become unstable, users cannot access the Internet, and serious industrial accidents may even occur. ARP attacks may also intercept accounts and passwords of services such as games, network banks, and file services.

11.3.2 ARP Anti-Spoofing Protection

ARP spoofing attacks to protection, the key is to identify and prohibit forwarding spoofed ARP packets. From the principle of ARP spoofing, we can see, to prevent ARP spoofing attack requires two ways, first to prevent the virus disguised as the gateway host, it will cause the entire segment of the user can not access; followed by preventing the virus from the host masquerade as another host, eavesdropping data or cause the same network segment can't communicate between the individual host.

MyPower S3100 series switches provide active defense ARP spoofing function, in practical applications, the network hosts the first communication, and the switch will record the ARP table entries, entries in the message of the sender IP, MAC, VID and port correspondence.

To prevent the above mentioned ARP attacks, MyPower S3100 launches a comprehensive ARP attack protection solution.

An access switch is a critical point to prevent ARP attacks, as ARP attacks generally arise from the host side. To prevent ARP attacks, the access switches must be able to

- Establish correct ARP entries, detect and filter out forged ARP packets, and ensure the validity of ARP packets it forwards
- Suppress the burst impact of ARP packets.

After configuring the access switches properly, you do not need to deploy ARP attack protection configuration on the gateway. This relieves the burden from the gateway.

If the access switches do not support ARP attack protection, or the hosts are connected to a gateway directly, the gateway must be configured to

- Create correct ARP entries and prevent them from being modified.
- Suppress the burst impact of ARP packets or the IP packets that will trigger sending of ARP requests.

The merits of configuring ARP attack protection on the gateway are that this gateway configuration hardly affects the switches and can properly support the existing network, thus effectively protecting user investment

11.3.3 Configuring Anti-Spoofing

Table 55 Configure Anti-Spoofing

STEP	COMMAND	OPERATION
step1	configure terminal	Enter global configuration mode
Step2	arp anti-spoofing	Enable ARP anti-spoofing

Table 55 Configure Anti-Spoofing

STEP	COMMAND	OPERATION
Step3	arp anti-spoofing unknown {diacard flood}	Configure the method of unknown static ARP packet
Step4	end	Return to privilege mode
Step5	copy running-config startup-config	Save modified configuration

11.3.4 Configuring ARP Packet Source MAC Address Consistency Check

This feature enables a gateway device to filter out ARP packets with a source MAC address in the Ethernet header different from the sender MAC address in the message body, so that the gateway device can learn correct ARP entries.

By default, system disables gateway spoofing.

Table 56 Configure ARP Packet Source MAC Address Consistency Check

STEP	COMMAND	OPERATION
step1	configure terminal	Enter global configuration mode
step2	arp anti-spoofing valid-check	Configure ARP packet source MAC address consistency check
step3	show arp anti-spoofing	Validation operation
step4	end	Return to privilege mode
step5	copy running-config startup-config	Save modified configuration

11.3.5 Anti-Spoofing Default Configuration Values

Table 57 Anti-Spoofing Default Configuration Values

COMMAND	DEFAULT
arp anti-spoofing	Disabled
arp anti-spoofing valid-check	Enabled
arp anti-spoofing unknown {diacard flood}	Discard

11.3.6 Displaying and Maintain Anti-Spoofing

Table 58 Display Anti-Spoofing

COMMAND	OPERATION
<code>show arp anti-spoofing</code>	Display the status of anti-spoofing
<code>show mac-address-table blackhole</code>	Display users whether add into black hole

11.4 Configuring ARP Anti-Flood

11.4.1 ARP Flood

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, switches, and servers, leading to depletion of network equipment, leaving the CPU down the network.

Flood attacks are based on the principle of the general flow of a large number of attack packets in the network equipment such as routers, switches and servers, leading to depletion of network equipment, leaving the CPU down the network.

11.4.2 ARP Anti-Flood

ARP flood attack is aimed mainly at the impact of network device's CPU, the core CPU resources leading to depletion. To defend this type of attack, the switch must determine in advance and to prohibit flood packet forwarding.

MyPower S3100's ARP anti-flood function to identify each ARP traffic, according to the ARP rate setting security thresholds to determine whether the ARP flood attack, when a host's ARP traffic exceeds a set threshold, the switch will be considered a flood attack , immediately pulled into the black host of the virus, banned from the host and all packet forwarding.

In order to facilitate the management of the network administrator to maintain, MyPower S3100, while the automatic protection will be saved in the system log related to alarms. For disabled users, administrators can set automatic or manual recovery.

In the MyPower S3100 switch on the entire process is as follows:

- Enable ARP anti-flood function will be broadcast ARP packets received on the CPU, according to an ARP packet source MAC address to identify the different streams.
- Set security ARP rate, if the rate exceeds the threshold, the switch that is ARP attack.
- If you select the above command deny-all, when an ARP traffic exceeds the threshold set, the switch will determine the source MAC address, the MAC address to the black hole list of addresses to ban this address to forward all subsequent messages.

- If you select the above command deny-arp, ARP traffic when more than a set threshold, the switch will be judged based on the source MAC address, the address against all subsequent handling of ARP packets.
- For recovery to be disabled in the user's forwarding, administrators can set up automatic or manual recovery time in two ways.

11.4.3 Configuring ARP Anti-Flood

Table 59 Configure ARP Anti-Flood

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	
Enable ARP flooding	<code>arp anti-flood</code>	Required
Configure safety trigger threshold	<code>arp anti-flood threshold threshold</code>	Optional By default, the safety trigger threshold 16PPS
Configure approach for the attacker	<code>arp anti-flood action {deny-arp deny-all} threshold threshold</code>	Optional By default, for the attacker's approach to deny ARP
Configure automatically banned user recovery time	<code>arp anti-flood recover-time time</code>	Optional Configurable time range is <0-1440> minutes, set to 0, said to be manually restored. By default, the user automatically banned recovery time of 10 minutes.
Banned user manual resume forwarding.	<code>arp anti-flood recover {H:H:H:H:H:H all}</code>	Optional

11.4.4 Displaying and Maintain ARP Anti-Flood

Table 60 Display ARP Anti-Flood

OPERATION	COMMAND	REMARKS
Display ARP anti-flood configuration and attackers list	<code>show arp anti-flood</code>	Perform either of the commands

IGMP Snooping

12.1 Brief Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a part of IP protocol which is used to support and manage the IP multicast between host and multicast router. IP multicast allows transferring IP data to a host collection formed by multicast group. The relationship of multicast group member is dynamic and host can dynamically add or exit this group to reduce network load to the minimum to realize the effective data transmission in network.

IGMP Snooping is used to monitor IGMP packet between host and routers. It can dynamically create, maintain, and delete multicast address table according to the adding and leaving of the group members. At that time, multicast frame can transfer packet according to its own multicast address table.

12.2 IGMP Snooping Configuration

12.2.1 Brief Configuration guide of IGMP Snooping

Table 61 Brief Configuration Guide of IGMP Snooping

CONFIGURATION TASK		REMARK	DETAILED CONFIGURATION
IGMP Snooping basic configuration	Enable IGMP Snooping	Required	12.2.2
Modify and optimize IGMP Snooping configuration	Configure IGMP Snooping multicast interface aging time	Optional	12.2.3
	Configure IGMP Snooping max-response-time	Optional	12.2.3
	Configure IGMP Snooping interface fast-leave	Optional	12.2.4
	Configure the number of the multicast group allowed learning	Optional	12.2.5
	Configure IGMP-Snooping multicast learning strategy	Optional	12.2.6
	Configure IGMP-Snooping CSS	Optional	12.2.7
	Configure route-port	Optional	12.2.8
	Configure IGMP Snooping multicast VLAN	Optional	12.2.9

Table 61 Brief Configuration Guide of IGMP Snooping

CONFIGURATION TASK		REMARK	DETAILED CONFIGURATION
	Configure port record host MAC	Optional	12.2.10
	Configure port whether waive research packets or not	Optional	12.2.11
	Configure port whether waive report packets or not	Optional	12.2.12
	Configure multicast preview	Optional	12.2.13
	Configure IGMP Snooping profile name list	Optional	12.2.14
Display and maintain IGMP Snooping		Optional	12.2.15

12.2.2 Enable IGMP Snooping

Table 62 Brief Configuration of IGMP Snooping

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enable IGMP Snooping	<code>igmp-snooping</code>	

12.2.3 Configuring IGMP Snooping Timer

Table 63 Configure IGMP Snooping Timer

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Configure IGMP Snooping multicast interface aging time	<code>igmp-snooping host-aging-time <i>time</i></code>	optional
		By default, dynamic interface aging time is 300S
Configure maximum leave time	<code>igmp-snooping max-response-time <i>time</i></code>	optional
		by default, maximum leave time is 10S

12.2.4 Configuring Port Fast-Leave

Under normal circumstances, IGMP-Snooping on IGMP leave message is received directly will not remove the port from the multicast group, but to wait some time before the port from the multicast group.

Enabling quickly delete function, IGMP-Snooping IGMP leave packet received, directly to the port from the multicast group. When the port is only one user, can be quickly removed to save bandwidth.

Table 64 Configure Port Fast-Leave

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration	<code>interface ethernet</code> <code>interface-num</code>	
Configure port fast-leave	<code>igmp-snooping fast-leave</code>	optional
		By default, port fast-leave disables

12.2.5 Configuring Number of Multicast Group Allowed Learning

Use `igmp-snooping group-limit` command to configure the number of the multicast group allowed learning.

Table 65 Configure the Number of the Multicast Group Allowed Learning

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration	<code>interface ethernet</code> <code>interface-num</code>	
Configure the number of the multicast group allowed learning	<code>igmp-snooping group-limit number</code>	Optional
		By default, the number of the multicast group allowed learning is NUM_MULTICAST_GROUPS

12.2.6 Configuring IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast switch is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as the IGMP Snooping querier to send IGMP queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Table 66 Configure IGMP Snooping Querier

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	

Table 66 Configure IGMP Snooping Querier

OPERATION	COMMAND	REMARKS
Configuration is not black and white list in the multicast group to learn the rules of the default	igmp-snooping {permit deny} {group all vlan vid}	Optional
		By default, not black and white list in the multicast group to learn the rules for the learning of all multicast group
Enter port configuration	interface ethernet interface-num	
Configure the port multicast black list	igmp-snooping {permit deny} group-range MAC multi-count num vlan vid	Optional
		Configure the port to learn (not learn) VID of the start of continuous num mac multicast groups
	igmp-snooping {permit deny} group MAC vlan vid	optional By default, any multicast group are not black and white list are added

12.2.7 Configuring IGMP Snooping Multicast Learning Strategy

Configured multicast learning strategies, the administrator can control the router only to learn the specific multicast group. If a multicast group is added to the blacklist, then the router will not learn the multicast group; the contrary, in the white list in the router can learn multicast group.

Table 67 Configuring IGMP Snooping Multicast Learning Strategy

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	
Open the IGMP-Snooping querier	igmp-snooping querier	
Configuring VLAN general query messages	igmp-snooping querier-vlan vid	Optional
Configured to send general query message interval	igmp-snooping query-interval interval	Optional
Configuration is generally the maximum query response time of message	igmp-snooping query-max-respond time	Optional
Configured to send general inquiries packet source IP address	igmp-snooping general-query source-ip ip	Optional

12.2.8 Configuring IGMP Snooping Router-Port

You can configure the router port will be automatically added to the dynamic IGMP Snooping Multicast learn to make routing port also has a multicast packet forwarding capability.

When the switch receives a host membership report sent packets, the port will be forwarded to the route.

Table 68 Configuring Routing Port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	
Configure hybrid routing port	igmp-snooping route-port forward	Optional

Table 68 Configuring Routing Port

OPERATION	COMMAND	REMARKS
Configure dynamic routing port aging time	<code>igmp-snooping router-port-age {on off age-time}</code>	Optional
Configure static routing port	<code>igmp-snooping route-port vlan vid interface {All ethernet interface-num}</code>	Optional

12.2.9 Configuring IGMP Snooping Port Multicast VLAN

Multicast VLAN on the port function, regardless of the port receiving the IGMP messages belong to which VLAN, the switch will be modified as a multicast VLAN.

Table 69 Configure IGMP Snooping Port Multicast VLAN

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration mode	<code>interface ethernet interface-num</code>	
Configure IGMP Snooping port multicast VLAN	<code>igmp-snooping multicast vlan vid</code>	Optional

12.2.10 Configuring Host Port Record MAC Functions

When this feature is enabled on the port, the switch will record the source packet IGMP report MAC address.

Table 70 Configure the Host Port Record MAC Functions

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration mode	<code>interface ethernet interface-num</code>	
Configure the host port record MAC	<code>igmp-snooping record-host</code>	Optional
Enter global configuration mode	<code>configure terminal</code>	

12.2.11 Configuring Port of Dropped Query Packets or Not

When this feature is enabled on a port, the switch drops the IGMP query message. Default port to receive all IGMP packets.

Table 71 Configure Port of Dropped Query Packets or Not

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration mode	<code>interface ethernet interface-num</code>	
Discard the query message to the configuration port	<code>igmp-snooping drop query</code>	Optional
Configure the port to receive the query message	<code>no igmp-snooping drop query</code>	Optional

12.2.12 Configuring Port of Discarded Packets Report or Not

When this feature is enabled on a port, the switch drops the IGMP report message. Default port to receive all IGMP packets.

Table 72 Configure Port of Discarded Packets Report or Not

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enter port configuration mode	<code>interface ethernet interface-num</code>	
Configure the port discarded packets report	<code>igmp-snooping drop report</code>	Optional
Configure the port to receive a report with	<code>no igmp-snooping drop report</code>	Optional

12.2.13 Configuring Multicast Preview

Multicast IGMP Snooping provides preview feature, users can configure the multicast channel preview, and you can configure a single multicast length preview, preview interval, duration, and reset to allow preview times.

Table 73 Configure Multicast Preview

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Configuring Multicast preview	<code>igmp-snooping preview</code>	
Configure multicast channel preview	<code>igmp-snooping preview group-ip ip vlan vid interface ethernet interface-num</code>	Optional
Configuration when the long single preview, preview interval, duration and allows preview reset the number of	<code>igmp-snooping preview {time-once time-once time-interval time-interval time-reset time-reset permit-times preview-times }</code>	Optional

12.2.14 Configuring Profile of Black and White List

IGMP Snooping provides the way black and white list feature profile, first in global configuration mode to create a number of profiles, then the port configuration mode to configure the port reference profile list. Users can configure the IGMP Snooping profile of the type and scope, which refers to the type of permit / deny, you can use the multicast IP address range or MAC address to configure. IGMP Snooping profile only the port referenced to take effect, the configuration port reference profile, the more the type of profile must be the same between that port can only refer to the same type (permit or deny) the profile. When the port is referenced permit the profile, the profile can only learn the definition of the corresponding multicast group; when the port reference deny the profile, the profile can be defined in addition to learning outside of all multicast group; when the port does not refer to any profile, in accordance with Normally learning multicast group.

Table 74 Configure Profile of Black and White List

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Create a profile, and enter profile configuration mode	<code>igmp-snooping profile profile-id</code>	
Configuration profile types	<code>profile limit {permit deny}</code>	Optional

Table 74 Configure Profile of Black and White List

OPERATION	COMMAND	REMARKS
Configuration profile IP range	<code>ip range start-ip end-ip [vlan vlan-id]</code>	Optional
Range of configuration profile mac	<code>mac range start-mac end-mac [vlan vlan-id]</code>	Optional
Enter port configuration mode	<code>interface ethernet interface-num</code>	
Reference configuration profile	<code>igmp-snooping profile refer profile-list</code>	Optional
Enter global configuration mode	<code>configure terminal</code>	

12.2.15 Displaying and Maintenance of IGMP Snooping

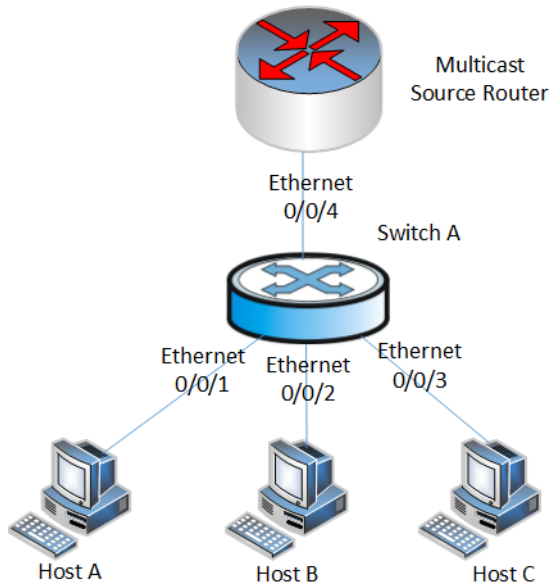
After completing the above configuration, can use the following command to view configuration.

Table 75 Configure Displaying and Maintenance of IGMP Snooping

OPERATION	COMMAND	REMARKS
See the related configuration IGMP Snooping	<code>show igmp-snooping</code>	Performs either of the commands
See dynamic routing port	<code>show igmp-snooping router-dynamic</code>	
Display static router port configuration	<code>show igmp-snooping router-static</code>	
Display Record in host MAC	<code>show igmp-snooping record-host [interface ethernet interface-num]</code>	
Display information about multicast preview	<code>show igmp-snooping preview</code>	
Display the current state of multicast channel preview	<code>show igmp-snooping preview status</code>	
Display profile configuration information	<code>show igmp-snooping profile [interface ethernet interface-num] [profile-list]</code>	
Display multicast group	<code>show multicast igmp-snooping [interface ethernet interface-num]</code>	

12.3 IGMP Snooping Configuration Examples

IGMP Snooping configuration examples as below:

Figure 18 IGMP Snooping Example

1 Network requirements

As shown in the figure 1-1, Host-A, Host-B, Host-C hosts separately belong to VLAN2, VLAN3, VLAN4. Three hosts separately receive the data of the multicast address 224.0.1.1-224.0.1.3 per configuring.

2 Configuration steps

Configuring S-switch-A

#Configure VLAN2 to 4, and add the ports separately into VLAN2,3,4 of Ethernet0/0/1, Ethernet0/0/2 and Ethernet0/0/3.

```

S-switch-A(config)#vlan 2
S-switch-A(config-if-vlan)#switchport ethernet 0/0/1
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 3
S-switch-A(config-if-vlan)#switchport ethernet 0/0/2
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/3
S-switch-A(config-if-vlan)#exit
  
```

#Enable igmp snooping

```

S-switch-A(config)#igmp-snooping
  
```

When Host-A, Host-B, Host-C forward IGMP report to S-switch-A, S-switch-A will learn corresponding multicast table entry port; When the Multicast Source Router send IGMP query time to the S-switch-A message, S-switch-A will learn the appropriate router port entry.

Show the switch learned multicast group

```
S-switch-A(config)#show multicast
show multicast table information
MAC Address      : 01:00:5e:00:01:01
VLAN ID          : 2
Static port list      :.
IGMP port list       : e0/0/1
Dynamic port list     :

MAC Address      : 01:00:5e:00:01:02
VLAN ID          : 3
Static port list      :.
IGMP port list       : e0/0/2
Dynamic port list     :

MAC Address      : 01:00:5e:00:01:03
VLAN ID          : 4
Static port list      :
IGMP port list       : e0/0/3.
Dynamic port list     :

Total entries: 3 .

S-switch-A(config)#show igmp-snooping router-dynamic
  Port      VID      Age      Type
  e0/0/4     2       284     { STATIC }
  e0/0/4     3       284     { STATIC }
  e0/0/4     4       284     { STATIC }
Total Record: 3
```

When Multicast Source Router sends 224.0.1.1-224.0.1.3 multicast serve data flow, S-switch-A will forward corresponding to Host-A, Host-B, Host-C.

Static multicast configuration examples:**Configuration steps:****Configuring S-switch-A**

#configure VLAN 2 to 4, and add the ports into VLAN2, 3, 4 of Ethernet0/0/1, Ethernet0/0/2 and Ethernet0/0/3.

```
S-switch-A(config)#vlan 2
S-switch-A(config-if-vlan)#switchport ethernet 0/0/1
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 3
S-switch-A(config-if-vlan)#switchport ethernet 0/0/2
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/3
S-switch-A(config-if-vlan)#exit
```

#Add the ports into the VLAN2 to VLAN4 of Ethernet0/0/4, configure Ethernet0/0/4 as static router port.

```
S-switch-A(config)#vlan 2-4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/4
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#igmp-snooping route-port vlan 2 interface ethernet 0/0/4
S-switch-A(config)#igmp-snooping route-port vlan 3 interface ethernet 0/0/4
S-switch-A(config)#igmp-snooping route-port vlan 4 interface ethernet 0/0/4
```

#configure static multicast group

```
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:01 vlan 2
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:01 vlan 2 interface ethernet
0/0/1
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:02 vlan 3
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:02 vlan 3 interface ethernet
0/0/2
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:03 vlan 4
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:03 vlan 4 interface ethernet
0/0/3
```

Show the switch learned multicast groups

```
S-switch-A(config)#show multicast
show multicast table information
MAC Address      : 01:00:5e:00:01:01
VLAN ID          : 2
Static port list  : .e0/0/1
IGMP port list    :
Dynamic port list :
```

```
MAC Address      : 01:00:5e:00:01:02
VLAN ID          : 3
Static port list  : e0/0/2
IGMP port list    :
Dynamic port list :
```

```
MAC Address      : 01:00:5e:00:01:03
VLAN ID          : 4
Static port list  : e0/0/3
IGMP port list    :
Dynamic port list :
```

Total entries: 3 .

```
S-switch-A(config)#show igmp-snooping router-static
Port      VID      Age      Type
e0/0/4     2      no age   { STATIC }
e0/0/4     3      no age   { STATIC }
e0/0/4     4      no age   { STATIC }
Total Record: 3
```

When Multicast Source Router sends 224.0.1.1-224.0.1.3 multicast serve data flow, S-switch-A will forward corresponding to Host-A, Host-B, Host-C.

GMRP Configuration

13.1 Brief Introduction to GMRP

GMRP (GARP Multicast Registration Protocol) is a kind of application of GARP (Generic Attribute Registration Protocol), which is based on GARP working mechanism to maintain the dynamic multicast register information in switch. All switches supported GMRP can receive multicast register information from other switches and upgrade local multicast register information dynamically and transfer it to other switches to make the consistency of multicast information of devices supported GMRP in the same switching network. Multicast register information transferred by GMRP includes local manual configuration of static multicast register information and the dynamic multicast register information of other switch.

13.2 GMRP Configuration

13.2.1 Enabling GMRP

Enable GMRP needs in both globally and port configuration. By default, GMRP disable in both globally and port configuration.

Table 76 Enable GMRP

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	
Enable GMRP in global configuration mode	<code>gmrp</code>	Required
Enter port configuration	<code>interface ethernet device/slot/ port</code>	
Enable GMRP in port configuration mode	<code>gmrp</code>	Required

13.2.2 Add Requisite Static Route Forwarded by GMRP

It forwards dynamically broadcast learning from GMRP when startup GMRP, but it is necessary for administrator to configure manually when GMRP forwards local static broadcast.

Table 77 Add Requisite Static Route Forwarded by GMRP

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	
Add requisite static route forwarded by GMRP	<code>garp permit multicast mac-address mac vlan vid</code>	Required

13.2.3 Displaying and Maintain GMRP

After finishing above configuration, you can use below commands to show GMRP client configuration.

Table 78 Display and Maintain GMRP

OPERATION	COMMAND	REMARK
Display GMRP in globally configuration mode	<code>show gmrp</code>	Perform either of the commands
Display GMRP in port configuration mode	<code>show gmrp interface [ethernet interface-num]</code>	
Display GMRP permit multicast	<code>show garp permit multicast</code>	
Display local broadcast (including static and learning broadcast by GMRP)	<code>show multicast</code>	
Enter global configuration mode	<code>configure terminal</code>	

13.2.4 GMRP Configuring Examples

As shown below, S1 and S3 by GMRP protocol packets to its own static multicast information circular to S2, S2 by GMRP packets will be learned by GMRP multicast information circular to go out in the end, making S1, S2, S3 the multicast information to be synchronized.

Figure 19 network



Configuration steps:

!Configuration on S1

!Before configuration

```

Switch(config)#vlan 111,333
Switch(config-if-vlan)#switchport ethernet 0/0/1 to ethernet 0/0/10
Add VLAN port successfully.
Switch(config)#multicast mac-address 01:00:5e:01:01:01 vlan 111
adding multicast group successfully !
Switch(config)#multicast mac-address 01:00:5e:01:01:01 vlan 111 interface ethernet
0/0/1 to ethernet 0/0/10
adding multicast group port successfully !
Switch(config-if-vlan)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#switchport mode trunk
Switch(config-if-ethernet-0/0/1)#exit
  
```

!Configure GMRP

```
Switch(config)#gvrp
Turn on GVRP successfully.
Switch(config)#gmrp
Turn on GMRP successfully.
Switch(config)#garp permit vlan 111,333
Switch(config)#garp permit multicast mac-address 01:00:5e:01:01:01 vlan 111
Switch(config)#interface e 0/0/1
Switch(config-if-ethernet-0/0/1)#gvrp
Switch(config-if-ethernet-0/0/1)#gmrp
Switch(config-if-ethernet-0/0/1)#exit
```

!GVRP configuration verification

```
Switch(config)#show gmrp
GMRP status : enable
Switch(config)#show gmrp interface ethernet 0/0/1
port      GMRP status
e0/0/1    enable
Total entries: 1.
Switch(config)#show garp permit multicast
GARP permit multicast:
  vlan 111, mac 01:00:5e:01:01:01
```

!Configuration on S2

!Before configuration

```
Switch(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
```

!Configure GMRP

```
Switch(config)#gvrp
Turn on GVRP successfully
Switch(config)#gmrp
Turn on GMRP successfully.
Switch(config)#interface range ethernet 0/0/2 to ethernet 0/0/3
Switch(config-if-range)#gvrp
Switch(config-if-range)#gmrp
Switch(config-if-range)#exit
```

!GVRP configuration verification

```
Switch(config)#show gmrp
GMRP state : enable
Switch(config)#show gmrp interface ethernet 0/0/2 ethernet 0/0/3
port      GMRP status
e0/0/2    enable
e0/0/3    enable
Total entries: 2.
```

!Configuration on S3

!Before configuration

```
Switch(config)#vlan 111,333
Switch(config-if-vlan)#switchport ethernet 0/0/1 to ethernet 0/0/10
Add VLAN port successfully.
Switch(config)#multicast mac-address 01:00:5e:03:03:03 vlan 333
adding multicast group successfully !
Switch(config)#multicast mac-address 01:00:5e:03:03:03 vlan 333 interface ethernet
0/0/1 to ethernet 0/0/10
adding multicast group port successfully !
Switch(config-if-vlan)#interface e 0/0/4
Switch(config-if-ethernet-0/0/4)#switchport mode trunk
Switch(config-if-ethernet-0/0/4)#exit
```

!Configure GMRP

```
Switch(config)#gvrp
Turn on GVRP successfully.
Switch(config)#gmrp
Turn on GMRP successfully.
Switch(config)#garp permit vlan 111,333
Switch(config)#garp permit multicast mac-address 01:00:5e:03:03:03 vlan 333
Switch(config)#interface e 0/0/4
Switch(config-if-ethernet-0/0/4)#gvrp
Switch(config-if-ethernet-0/0/4)#gmrp
Switch(config-if-ethernet-0/0/4)#exit
```

!GVRP configuration verification

```
Switch(config)#show gmrp
GMRP status : enable
Switch(config)#show gmrp interface ethernet 0/0/4
port      GMRP status
e0/0/4    enable
Total entries: 1.
Switch(config)#show garp permit multicast
GARP permit multicast:
  vlan 333, mac 01:00:5e:03:03:03
```

After configuration is complete, you can show multicast command to view the function of learning to GMRP multicast registration information.

!View the multicast information in S1 can be found, 01:00:5 e: 03:03:03 is learned by GMRP multicast.

```
Switch(config)#show multicast
show multicast table information
MAC Address      : 01:00:5e:01:01:01
VLAN ID         : 111
Static port list : e0/0/1-e0/0/10.
IGMP port list   :
Dynamic port list :

MAC Address      : 01:00:5e:03:03:03
VLAN ID         : 333
Static port list :
IGMP port list   :
Dynamic port list : e0/0/1.
```

Total entries: 2 .

! To view the multicast information on S3 can be found, 01:00:5 e: 01:01:01 and 01:00:5 e: 03:03:03 through learning to GMRP multicast.

```
Switch(config)#show multicast
show multicast table information
MAC Address      : 01:00:5e:01:01:01
VLAN ID         : 111
Static port list :
IGMP port list   :
Dynamic port list : e0/0/2.

MAC Address      : 01:00:5e:03:03:03
VLAN ID         : 333
Static port list :
IGMP port list   :
Dynamic port list : e0/0/3.
```

Total entries: 2 .

!View multicast information on S3 can be found, 01:00:5 e: 01:01:01 by GMRP multicast learn.

```
Switch(config)#show multicast
show multicast table information
MAC Address      : 01:00:5e:01:01:01
VLAN ID         : 111
Static port list :
IGMP port list   :
Dynamic port list : e0/0/4.

MAC Address      : 01:00:5e:03:03:03
VLAN ID         : 333
Static port list : e0/0/1-e0/0/10.
IGMP port list   :
Dynamic port list :

Total entries: 2 .
```

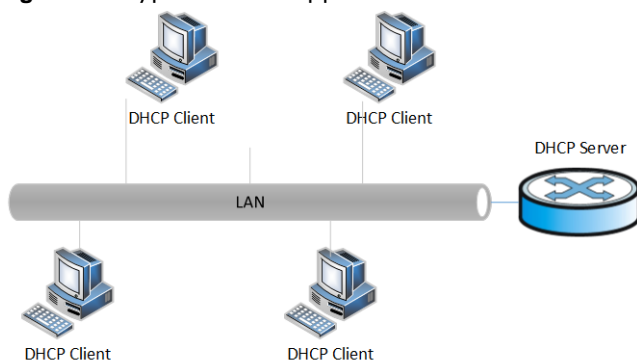
DHCP Configuration

14.1 DHCP Overview

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed in this background.

DHCP adopts a client/server model, where DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to configure IP addresses dynamically. A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in [Figure 20 on page 102](#).

Figure 20 Typical DHCP Application



14.2 DHCP IP Address Assignment

14.2.1 IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

Manual assignment: the administrator statically binds IP addresses to few clients with special uses (such as WWW server). Then the DHCP server assigns these fixed IP addresses to the clients.

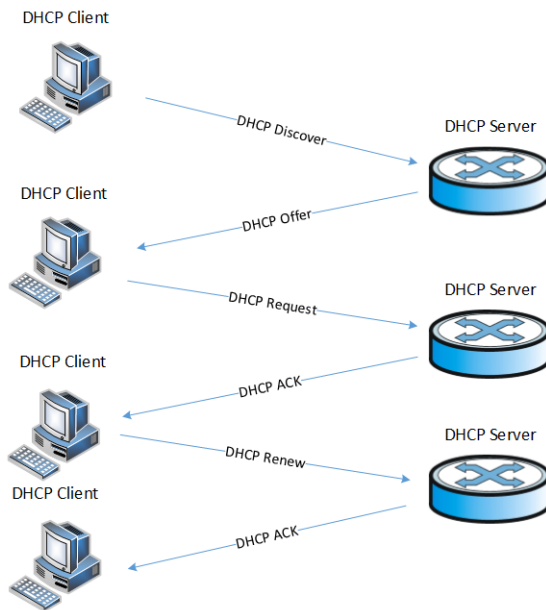
Automatic assignment: the DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.

Dynamic assignment: the DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address at the expiration of the period. This policy applies to most clients.

14.2.2 Obtaining IP Addresses Dynamically

Interaction between a DHCP client and a DHCP server is as shown in [Figure 21 on page 103](#).

Figure 21 Interaction Between a DHCP Client and a DHCP Server



There are three different modes for DHCP client to obtain IP address in different stage:

1 Initial login for DHCP client

There are four stages for the initial login of DHCP client:

- **Discover.** In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.
- **Offer.** In this phase, the DHCP server offers an IP address. Each DHCP server that receives the DHCP-DISCOVER packet chooses an unassigned IP address from the address pool based on the IP address assignment policy and then broadcasts a DHCP-OFFER packet to the DHCP client.
- **Select:** In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.
- **Acknowledge:** Upon receiving the DHCP-REQUEST packet, the DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

The IP addresses offered by other DHCP servers (if any) are not used by the DHCP client and are still available to other clients.

2 The next login for DHCP client

When DHCP client relogin, there are two types of situation:

- The last-assigned IP address is not occupied. Broadcast a DHCP-REQUEST packet containing the assigned IP address, the DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client.
- The last-assigned IP address is occupied. Broadcast a DHCP-REQUEST packet containing the assigned IP address, the DHCP server returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. The client will re-send DHCP_Discover packet to request a new IP address.

3 Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP server again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described in the previous section.

14.2.3 DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following table describes the packet format (the number in the brackets indicates the field length, in bytes):

Figure 22 DHCP Packet Format

op(1)	htype(1)	hlen(1)	hops(1)
Xid(4)			
secs(2)		flags(2)	
ciaddr(4)			
yiaddr(4)			
siaddr(4)			
chaddr(16)			
sname(64)			
file(128)			
option(variable)			

The field meanings are illustrated as follows:

op: Operation types of DHCP packets: 1 for request packets and 2 for response packets.

htype, hlen: Hardware address type and length of the DHCP client.

hops: Number of DHCP relays which a DHCP packet passes. For each DHCP relay that the DHCP request packet passes, the field value increases by 1.

xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.

secs: Elapsed time after the DHCP client initiates a DHCP request.

flags: The first bit is the broadcast response flag bit. It is used to identify that the DHCP response packet is sent in the unicast or broadcast mode. Other bits are reserved.

ciaddr: IP address of a DHCP client.

yiaddr: IP address that the DHCP server assigns to a client.

siaddr: IP address of the DHCP server.

giaddr: IP address of the first DHCP relay that the DHCP client passes after it sent the request packet.

chaddr: Hardware address of the DHCP client.

sname: Name of the DHCP server.

file: Name of the start configuration file that the DHCP server specifies for the DHCP client.

option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

14.3 DHCP Relay

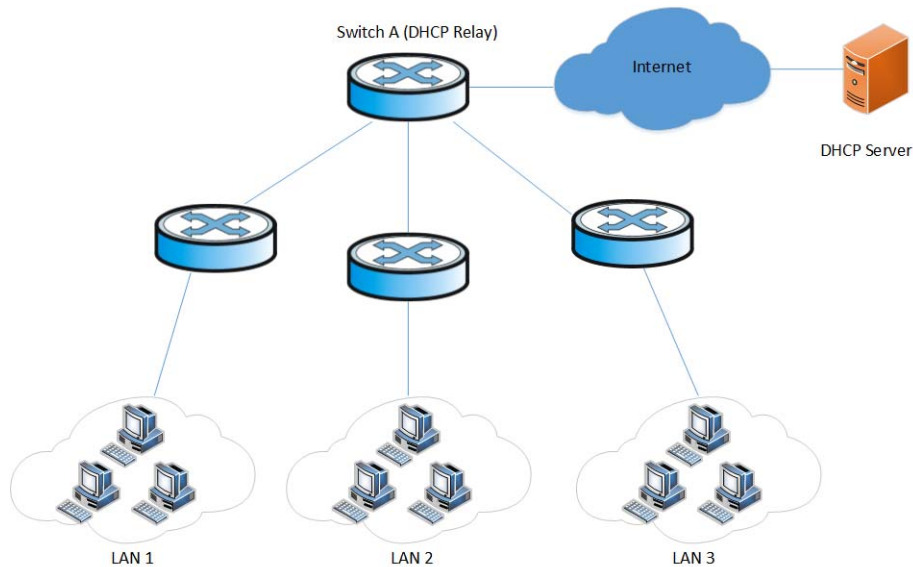
14.3.1 Usage of DHCP Relay

Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP Relay is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

14.3.2 DHCP Relay Fundamentals

Figure 23 Typical DHCP Relay Application



DHCP relays can transparently transmit broadcast packets on DHCP clients or servers to the DHCP servers or clients in other network segments.

In the process of dynamic IP address assignment through the DHCP relay, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay. The following sections only describe the forwarding process of the DHCP relay. For the interaction process of the packets, see [Obtaining IP Addresses Dynamically](#).

The DHCP client broadcasts the DHCP-DISCOVER packet.

After receiving the packets, the network device providing the DHCP relay function unicasts the packet to the designated DHCP server based on the configuration.

The DHCP server assigns IP addresses, and then broadcasts the configuration information to the client through the DHCP relay. The sending mode is determined by the flag in the DHCP-DISCOVER packets from the client. For detailed information, refer to [DHCP Packet Format](#).

14.4 DHCP Server and Relay Configuration

14.4.1 Configure DHCP Server

Table 79 Configure DHCP Server

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Configure HCP-Server IP address	<code>dhcp-server number ip <i>ipaddress</i></code>	

Table 79 Configure DHCP Server

OPERATION	COMMAND	REMARKS
Enter VLAN interface configuration mode	<code>interface vlan-interface vlan id</code>	
Enable DHCP-Server	<code>dhcp-server number</code>	Required
Enable DHCP Server trap	<code>dhcp-server traps</code>	Optional
Disable DHCP Server trap	<code>no dhcp-server traps</code>	Optional

14.4.2 Configure DHCP Address Pool

Table 80 Configure DHCP Address pool

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Create DHCP address pool	<code>ip pool name</code>	Required
Remove DHCP address pool	<code>no ip pool name</code>	Optional
Specifies the gateway of DHCP address pool	<code>gateway gateway address subnet mask</code>	Required
Specifies the range of available IP addresses	<code>section ID start ipaddress end ipaddress</code>	Required
Remove the range of available IP addresses	<code>no section ID</code>	Optional
Specifies the duration of the lease	<code>lease time</code>	Optional
Restore to the default value of lease	<code>no lease</code>	Optional
Specifies the IP address of DNS server	<code>Dns {primary-ip second-ip third-ip fourth-ip suffix} dns server address</code>	Optional
Restore the IP address of DNS server to default value	<code>no dns {primary-ip second-ip third-ip fourth-ip suffix}</code>	Optional
Configure router IP address	<code>router ipaddress</code>	Optional
Restore the router IP address to default value	<code>no router</code>	Optional
Configure wins primary IP address	<code>wins primary-ip ipaddress</code>	Optional
Configure wins secondary IP address	<code>wins second-ip ipaddress</code>	Optional
Restore the wins IP address to default value	<code>no wins {primary-ip second-ip}</code>	Optional

14.4.3 Configure DHCP Relay

Table 81 Configure DHCP Relay

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	
Enable DHCP Relay	<code>dhcp-relay</code>	Required
Configure DHCP relay hop number	<code>dhcp max-hops number <1~16></code>	Optional
Hide DHCP server IP address	<code>dhcp-relay hide server-ip</code>	Optional

14.4.4 Display DHCP Server and Relay Configuration

Table 82 Display DHCP Server and Relay Configuration

OPERATION	COMMAND	REMARKS
Display DHCP-Server configuration	<code>show dhcp-server server-id</code>	
Display the status of DHCP server interface	<code>show dhcp-server interface {vlan- interface if-id supervlan- interface if-id}</code>	
Display the information DHCP clients	<code>show dhcp-server clients</code>	
Display the status of dhcp-relay	<code>show dhcp-relay</code>	
Display the status of dhcp-relay hidden IP address	<code>show dhcp-relay hide server-ip</code>	

DHCP Snooping

15.1 Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients. Switches can track DHCP client IP addresses through the DHCP snooping function, which listens DHCP broadcast packets.

DHCP snooping listens the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

DHCP-ACK packet

DHCP-REQUEST packet

When an unauthorized DHCP server exists in the network, a DHCP client may obtain an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

Trusted ports can be used to connect DHCP servers or ports of other switches. Untrusted ports can be used to connect DHCP clients or networks.

Untrusted ports drop the DHCP-ACK and DHCP-OFFER packets received from DHCP servers. Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers.

15.2 DHCP Snooping Configuration

Perform following commands in global configuration mode.

Table 83 Configure the DHCP Snooping Function

OPERATION	COMMAND	DESCRIPTION
Enter global configuration mode	<code>configure terminal</code>	
Enable DHCP-Snooping	<code>dhcp-snooping</code>	By default, DHCP-Snooping is disabled.
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Configure port connected to DHCP server direction to be Trust	<code>dhcp-snooping trust</code>	By default, all ports are untrusted port.
Restore all ports to untrusted	<code>no dhcp-snooping trust</code>	Optional

Table 83 Configure the DHCP Snooping Function

OPERATION	COMMAND	DESCRIPTINO
Enable fast remove function when the interface is down	<code>dhcp-snooping port-down-action fast-remove</code>	By default, this function is enabled.
Disable fast remove function when the interface is link	<code>no dhcp-snooping port-down-action fast-remove</code>	Optional

15.3 DHCP-Snooping Security Configuration

15.3.1 Configure Max Clients Number

A private DHCP server on a network also answers IP address request packets and assigns IP addresses to DHCP clients. However, the IP addresses they assigned may conflict with those of other hosts. As a result, users cannot normally access networks. This kind of DHCP servers are known as private DHCP servers. Therefore, administrators can:

Restrict the DHCP-Client number connected to switch port. So only the clients connected to the same port with the attacker will suffer the attack.

Restrict the DHCP-Client number in specified VLAN. So only the clients in the same VLAN with the attacker will suffer the attack.

This function should be work with DHCP-Snooping. Perform following commands in interface configuration mode.

Table 84 Configure Max Clients Number

OPERATION	COMMAND	DESCRIPTINO
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Configure max DHCP-Client number connected to switch port	<code>dhcp-snooping max-clients <0-2048></code>	By default, the max DHCP-Client number connected to switch port is 2048.
Enter VLAN mode	<code>vlan vlan_list</code>	
Configure max DHCP-Client number in specified VLAN.	<code>dhcp-snooping max-clients <0-2048></code>	By default, the max DHCP-Client number in specified VLAN is 2048.
Restore the max DHCP-Client number to default value	<code>no dhcp-snooping max-clients</code>	This command is available under interface and VLAN configuration mode.

15.3.2 Configure IP-Source-Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. When using IP-Source-Guard, pay attention:

- DHCP-Snooping has been enabled

- Use this function in Trust port

After enabling IP-Source-Guard, all traffic with that IP source address is permitted from that trusted client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. The filtering info can be source MAC, source IP and source port number.

Perform following commands in global configuration mode:

Table 85 Configure IP-Source-Guard

OPERATION	COMMAND	DESCRIPTINO
Enter global configuration mode	<code>configure terminal</code>	
Configure IP-source-guard bind table	<code>ip-source-guard bind {ip A.B.C.D mac HH:HH:HH:HH:HH:HH interface ethernet device-num<0>/slot-num<0-2>/port-num<1-48>}</code>	
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Enable IP-Source-Guard on untrusted port	<code>ip-source-guard {ip ip-mac ip-mac-vlan}</code>	By default, ip-source-guard is disabled.
Enable VLAN IP-Source-Guard	<code>ip-source-guard vlan VLAN list</code>	By default, VLAN ip-source-guard is enabled under global configuration mode.
Disable VLAN IP-Source-Guard	<code>no ip-source-guard vlan VLAN list</code>	This command is available under global configuration mode.
Enable IGMP pass through permit function of IP-Source-Guard	<code>ip-source-guard permit igmp</code>	Optional
Disable IGMP pass through permit function of IP-Source-Guard	<code>no ip-source-guard permit igmp</code>	Optional

IP source guard filters packets based on the following types of binding entries:

Source IP

Source IP + source MAC

Source IP + source MAC + source port

15.4 Displaying and Debugging DHCP-Snooping

After the above configurations, you can verify the configurations by executing the show command in any configuration mode.

Table 86 Displaying and Debugging DHCP-Snooping

OPERATION	COMMAND	DESCRIPTINO
Display DHCP-Snooping clients	<code>show dhcp-snooping clients</code>	
Display DHCP-Snooping status in interface	<code>show dhcp-snooping interface {ethernet pon} interface-num</code>	
Display DHCP-Snooping status in VLAN	<code>show dhcp-snooping vlan</code>	
Display IP-Source-Guard status in interface	<code>show ip-source-guard</code>	
Display source IP binding table of IP-Source-Guard	<code>show ip-source-guard bind [ip A.B.C.D]</code>	
Display IGMP pass through permit status of IP-Source-Guard	<code>show ip-source-guard permit igmp</code>	
Display IP-Source-Guard status in VLAN	<code>show ip-source-guard vlan</code>	

15.5 DHCP-Snooping Configuration Example

15.5.1 Network requirements

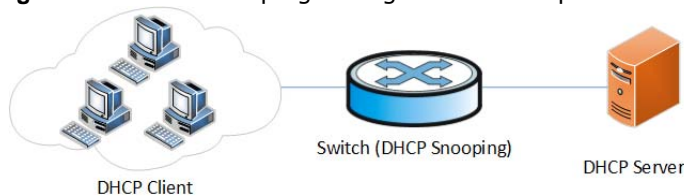
As shown in [Figure 24 on page 112](#), the GigabitEthernet0/0/1 port of Switch is connected to DHCP Server. A network segment containing some DHCP clients is connected to the Gigabit Ethernet 0/0/2 port of Switch.

The DHCP snooping function is enabled on Switch.

The GigabitEthernet1/0/1 port of Switch is a trusted port.

15.5.2 Network diagram

Figure 24 DHCP-Snooping Configuration Example



15.5.3 Configuration procedure

All following commands are performed in Switch acting as a DHCP-Snooping device.

- 1** Enter global configuration mode
`Switch#configure terminal`
`Switch(config)#`
- 2** Enable DHCP-Snooping
`Switch(config)#dhcp-snooping`
`Config DHCP Snooping successfully.`
- 3** Enter interface configuration mode of Ethernet0/0/1
`Switch(config)#interface ethernet 0/0/1`
- 4** Set Ethernet0/0/1 to be Trust
`Switch(config-if-ethernet-0/0/1)#dhcp-snooping trust`
`Config DHCP Snooping mode of port successfully.`

DHCP Option 82

16.1 Introduction to option 82 supporting

Option: A length-variable field in DHCP packets, carrying information such as part of the lease information and packet type. It includes at least one option and at most 255 options.

Option 82: Also known as relay agent information option. This option is a part of the Option field in DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 includes at least one sub-option and at most 255 sub-options. Currently, the commonly used sub-options in option 82 are sub-option 1 and sub-option 2.

Sub-option 1: A sub-option of option 82. Sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the port number and VLAN-ID of the switch port connected to the DHCP client, and is usually configured on the DHCP relay. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

Sub-option 2: A sub-option of option 82. Sub-option 2 represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay, and is usually configured on the DHCP relay. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

16.2 DHCP Option82 Configuration

16.2.1 Enable DHCP Option82

To enable option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay.

If the packet contains option 82, the DHCP relay processes the packet depending on the configured policy:

- **Drop:** Specifies to discard the DHCP request packets that carry option 82.
- **Keep:** Specifies to remain the DHCP request packets that carry option 82 unchanged.
- **Replace:** Specifies to replace the option 82 carried by a DHCP request packet with that of the DHCP relay.

Perform following commands in global configuration mode:

Table 87 Enable DHCP Option82

OPERATION	COMMAND	DESCRIPTION
Enter global configuration mode	<code>configure terminal</code>	
Enable DHCP Option82	<code>dhcp option82</code>	By default, DHCP Option82 is disabled.
Configure the format of DHCP option82	<code>dhcp option82 format {henan normal verbose}</code>	By default, the format of DHCP Option82 is normal.
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Configure the strategy for the DHCP relay to process request packets containing option 82	<code>dhcp option82 strategy {drop keep replace}</code>	By default, the DHCP relay replaces the option 82 carried by a DHCP request packet with its own option 82.
Configure the circuit-id of DHCP option82	<code>dhcp option82 circuit-id {string user-defined}</code>	Optional
Restore the circuit-id of DHCP option82 to default	<code>no dhcp option82 circuit-id {string user-defined}</code>	Optional
Configure the remote-id of DHCP option82	<code>dhcp option82 remote-id {string user-defined}</code>	Optional
Restore the remote-id of DHCP option82 to default	<code>no dhcp option82 remote-id {string user-defined}</code>	Optional

16.2.2 Displaying and Debugging DHCP Option82

Table 88 Displaying and Debugging DHCP Option82

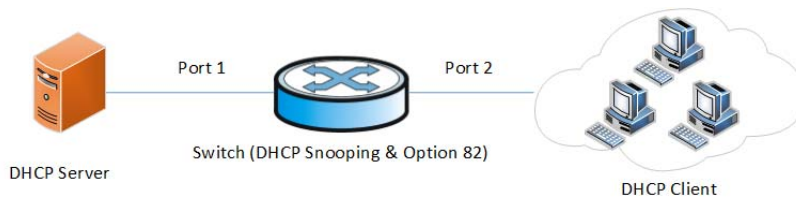
OPERATION	COMMAND	DESCRIPTION
Display DHCP option82 status	<code>show dhcp option82</code>	

16.3 DHCP Option82 Configuration Example

Network requirements

When you enable the DHCP snooping information option 82 on the switch, the switch forwards the DHCP request that includes the option-82 field to the DHCP server.

Figure 25 DHCP Option82 Configuration Example



Configuration procedure

Switch port 1 is connected to DHCP Server and port 2 is connected to DHCP client; Enable DHCP-Snooping function and dhcp-option 82 function on switch, and set switch port 1 as a trusted port.

All following commands are performed in Switch acting as a DHCP-Snooping device.

```
Switch#configure terminal
Switch (config)#dhcp-snooping
Config DHCP Snooping successfully.           //Enable DHCP-Snooping function
Switch (config)#dhcp option82                //Enable DHCP option82 function
Switch(config)#interface ethernet 0/0/1
Switch (config-if-ethernet-0/0/1)#dhcp-snooping trust //Set switch port 1 as a
trusted port.
Config DHCP Snooping mode of port successfully.
```

Result:

You can capture DHCP packets that include the dhcp-option82 field on port 1.

ACL Configuring

17.1 Brief Introduction to ACL

As network scale and network traffic are increasingly growing, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal users from accessing networks and to control network traffic and save network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

ACLs are sets of rules (or sets of permit or deny statements) that decide what packets can be passed and what should be rejected based on matching criteria such as source MAC address, destination MAC address, source IP address, destination IP address, and port number.

When an ACL is assigned to a piece of hardware and referenced by a QoS policy for traffic classification, the switch does not take action according to the traffic behavior definition on a packet that does not match the ACL.

ACL according to application identified by ACL numbers, fall into three categories,

- Basic ACL: Source IP address
- Extended ACL: Source IP address, destination IP address, protocol carried on IP, and other Layer 3 or Layer 4 protocol header information
- Layer 2 ACL: Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority, and link layer protocol type

17.1.1 Matching Order

An ACL consists of multiple rules, each of which has different matching criteria. These criteria may have overlapping or conflicting parts. This is where the order in which a packet is matched against the rules comes to rescue.

Two match orders are available for ACLs:

- config: where packets are compared against ACL rules in the order in which they are configured.
- auto: where depth-first match is performed. The term depth-first match has different meanings for different types of ACLs. Depth-first match for a basic ACL

For example, now configuring 2 types of ACL as below:

```
Switch(config)#access-list 2000 deny any
Config ACL subitem successfully.
Switch(config)#access-list 2000 permit 1.1.1.1 0
Config ACL subitem successfully.
```

- If it is the configuration mode, sub-item 0 is the first command. You can see as below configuration:

```
Switch(config)#show access-list config 1
Standard IP Access List 1, match-order is config, 2 rule:
deny    any
permit  1.1.1.1  0.0.0.0
```

- If it is the auto mode, sub-item 0 is the longest ACL match rule. You can see as below configuration:

```
Switch(config)#show access-list config 1
Standard IP Access List 1, match-order is auto, 2 rule:
0 permit 1.1.1.1 0.0.0.0
1 deny   any
```

Notes, ACL must enable. Switches must obey "first enable then active. Please refer to [Section 17.5 on page 125](#) for detailed configuration.

17.1.2 Switch Support ACL

Switch support ACL as below:

- Basic ACL
- Extended ACL
- Layer 2 AC

17.2 Configuring Time Range

There are two kinds of configuration: configure absolute time range and periodic time range. Configuring absolute is in the form of year, month, date, hour and minute. Configuring periodic time range is in the form of day of week, hour and minute.

17.2.1 Configuration Procedure

Table 89 Configuration procedure

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
new build time range and enter time range mode	time-range name	-
Configure absolute start	absolute start <i>HH:MM:SS YYYY/MM/DD</i> [end <i>HH:MM:SS YYYY/MM/DD</i>]	required
Configure periodic start	periodic <i>days-of-the-week hh:mm:ss</i> to [<i>day-of-the-week</i>] <i>hh:mm:ss</i>	

Note that:

Periodic time range created using the `time-range time-name start-time to end-time days` command. A time range thus created recurs periodically on the day or days of the week.

Absolute time range created using the `time-range time-name {from time1 date1 [to time2 date2] | to time2 date2 }` command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the `time-range test from 00:00 01/01/2004 to 23:59 12/31/2004` command.

Compound time range created using the `time-range time-name start-time to end-time days { from time1 date1 [to time2 date2] | to time2 date2 }` command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the `time-range test 12:00 to 14:00 Wednesday from 00:00 01/01/2004 to 23:59 12/31/2004` command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

With no start time specified, the time range is from the earliest time that the system can express (that is, 00:00 01/01/1970) to the end time. With no end time specified, the time range is from the time the configuration takes effect to the latest time that the system can express (that is, 24:00 12/31/2100).

Up to 256 time ranges can be defined.

17.2.2 Configuration Examples

- Create an absolute time range from 16:00, Jan 3, 2009 to 16:00, Jan 5, 2009

```
Switch#configure terminal
Switch(config)#time-range b
Config time range successfully.
Switch(config-timerange-b)#absolute start 16:00:00 2009/1/3 end 16:00:00 2009/1/5
Config absolute range successfully .
Switch(config-timerange-b)#show time-range name b
Current time is: 02:46:43    2009/01/31    Saturday
```

```
time-range: b ( Inactive )
absolute:  start 16:00:00 2009/01/03 end 16:00:00 2009/01/05
```

- Create a periodic time range that is active from 8:00 to 18:00 every working day.

```
Switch#configure terminal
Switch(config)#time-range b
Config time range successfully.
Switch(config-timerange-b)#periodic weekdays 8:00:00 to 18:00:00
Config periodic range successfully .
Switch(config-timerange-b)#show time-range name b
Current time is: 02:47:56    2009/01/31    Saturday
```

```
time-range: b ( Inactive )
periodic:  weekdays 08:00 to          18:00
```

17.2.3 Configuring a Basic ACL

Basic ACLs filter packets based on source IP address. They are numbered in the range 1 to 99. At most 99 ACL with number mark and at most 1000 ACL with name mark. At most 128 rules for each ACL at the same time. If you want to reference a time range to a rule, define it with the time-range command first.

17.2.4 Configuration Procedure

Follow these steps to configure a basic ACL

Table 90 Configure basic ACL based on digital identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Define sub-item match rule	access-list num match-order { config auto }	optional
		by default ,system is config
Define basic ACL	access-list num { permit deny } { source-IPv4/v6 source-wildcard any ipv6any } [time-range name]	required

Table 91 Configure basic ACL based on name identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Define sub-item match rule	access-list standard name match-order { config auto }	optional
		by default ,system is config
Define basic ACL and enter configuration mode	access-list standard name	required
Configure ACL rule	{ permit deny } { source-IPv4/v6 source-wildcard any ipv6any } [time-range name]	required

17.2.5 Configuration Examples

!Define a basic ACL with number mark to deny packet with source IP 10.0.0.1

```
Switch#configure terminal
Switch(config)#access-list 1 deny 10.0.0.1 0
```


!Define a basic ACL with name mark to deny packet with source IP 10.0.0.2

```
Switch#configure terminal
Switch(config)#access-list standard stdacl
Switch(config-std-nacl-stdacl)#deny 10.0.0.2 0
```

17.3 Define Extended ACL

Switch can define at most 100 extended ACL with the number ID (the number is in the range of 100 to 199), at most 1000 extended ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID).

17.3.1 Configuration Procedure

Follow these steps to configure an extended ACL:

Table 92 Configure extended ACL based on digital identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Define sub-item match rule	access-list num match-order { config auto }	optional by default ,system is config
Define extended ACL	access-list num { permit deny } [protocol] [established] { source-IPv4/v6 source-wildcard any ipv6any } [port [portmask]] { dest- IPv4/v6 dest-wildcard any ipv6any } [port [portmask]] { [precedence precedence] [tos tos] [dscp dscp] } [time-range name]	required
Delete ACL	no access-list { num / all }	

Table 93 Configure extended ACL based on name identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Define subitem match rule	access-list extended name match-order { config auto }	optional by default ,system is config
Define extended ACL and enter configuration mode	access-list extended name	required

Table 93 Configure extended ACL based on name identification

OPERATION	COMMAND	REMARK
Configure ACL rule	{ permit deny } [protocol] [established] { source-IPv4/v6 source-wildcard any ipv6any } [source-port wildcard] { dest-IPv4/v6 dest-wildcard any ipv6any } [dest-port wildcard] [icmp-type icmp-code] [igmp-type] [traffic-class traffic-class] [[precedence precedence] [tos tos] [dscp dscp]] [fragments] [time-range name]	required
Delete ACL	no access-list { name all }	

Detailed parameters of extended ACL as below [Table 94 on page 122](#):

Table 94 Detailed parameters of extended ACL

PARAMETERS	FUNCTION	REMARK
protocol	IP protocol type carried	A number in the range of 1 to 255 Represented by name, you can select GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP
source-IPv4/v6	ACL rules specified the source address information	sour-address sour-wildcard used to determine the packet's source IP address. Dotted decimal notation;
sour-wildcard		sour-wildcard of 0 means that the host address
any ipv6any		any source address.
dest-IPv4/v6	The purpose of ACL rules specified address information	dest-addr dest-wildcard used to determine the packet destination address, in dotted decimal notation;
dest-wildcard		dest-wildcard is 0, the host address
any ipv6any		Any is any destination address.
source-port/ dest-port wildcard	TCP / UDP port number	—
icmp-type icmp-code	ICMP	Protocol should be icmp/icmpv6
igmp-type	IGMP	Protocol should be IGMP
precedence precedence	priority precedence message	IP precedence values range from 0 to 7
tos tos	tos priority packets	ToS priority ranges from 0 to 15
dscp dscp	DSCP priority Level ranges from 0 to 63	Rule applies only to non-first fragment packet effective

Table 94 Detailed parameters of extended ACL

PARAMETERS	FUNCTION	REMARK
time-range <i>name</i>	Create a time range	—
fragments	fragment fragmentation information	

17.3.2 Configuration Procedure

!Create extended ACL based on digital identification to deny the FTP packets with source address 10.0.0.1 .

```
Switch#configure terminal
Switch(config)#access-list 100 deny tcp 10.0.0.1 0 ftp any
```

!Create extended ACL based on name identification to deny the FTP packets with source address 10.0.0.1.

```
Switch#configure terminal
Switch (config)#access-list extended extacl
Switch(config-ext-nacl-extacl)#deny tcp 10.0.0.2 0 ftp any
```

17.4 Define Layer 2 ACL

Switch can define at most 100 layer 2 ACL with the number ID (the number is in the range of 200 to 299), at most 1000 layer 2 ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Layer 2 ACL only classifies data packet according to the source MAC address, source VLAN ID, layer protocol type, layer packet received and retransmission interface and destination MAC address of layer 2 frame head of data packet and analyze the matching data packet.

17.4.1 Configuring Layer 2 ACL

Follow these steps to configure a Layer 2 ACL rule.

Table 95 Configure Layer 2 ACL based on digital identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Configure sub-item match rule	access-list <i>num</i> match-order { config auto }	optional by default ,system is config

Table 95 Configure Layer 2 ACL based on digital identification

OPERATION	COMMAND	REMARK
Configure Layer 2 ACL	<code>access-list num { permit deny } [protocol] [cos vlan-pri] ingress { { [source-vlan-id] [source-mac-addr source-mac-wildcard] [interface interface-num] } any } egress { { [dest-mac-addr dest-mac-wildcard] [interface interface-num cpu] } any } [time-range name]</code>	required
Delete ACL rules	<code>no access-list [num all]</code>	

Table 96 Configure Layer 2 ACL based on name identification

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Define sub-item match rule	<code>access-list link name match-order { config auto }</code>	optional by default ,system is config
Define Layer 2 ACL and enter configuration mode	<code>access-list link name</code>	required
Configure ACL rule	<code>{ permit deny } [protocol] [cos vlan-pri] ingress { { [source-vlan-id] [source-mac-addr source-mac-wildcard] [interface interface-num] } any } egress { { [dest-mac-addr dest-mac-wildcard] [interface interface-num cpu] } any } [time-range name]</code>	required

17.4.2 Configuration Examples

!Create Layer 2 ACL based on digital identification to deny the MAC with ARP address 00:00:00:00:00:01.

```
Switch#configure terminal
Switch(config)#access-list 200 deny arp ingress 00:00:00:00:00:01 0 egress any
```

!Create Layer 2 ACL based on name identification to deny the MAC with ARP address 00:00:00:00:00:02.

```
Switch#configure terminal
Switch(config)#access-list link lnkacl
Switch (config-link-nacl-lnkacl)#deny arp ingress 00:00:00:00:00:02 0 egress any
```

17.5 Activate ACL

The priority of ACL rules is based on the rule activated order.

Table 97 Activate ACL

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Active ACL	access-group [ip-group <i>name num</i>] [subitem <i>num</i>] [link-group <i>name num</i>] [subitem <i>num</i>]	required
Disable Specified ACL	access-group [ip-group <i>name num</i>] [subitem <i>num</i>] [link-group <i>name num</i>] [subitem <i>num</i>]	
Disable All ACL	no access-group all	

17.5.1 Configuration Examples

Switches only permit with source IP address 1.1.1.1

!Before configuration

```
Switch(config)#show access-list config 2000
Standard IP Access List 2000, match-order is config, 2 rule:
0 deny any
1 permit 1.1.1.1 0.0.0.0
```

!Configuration steps

```
Switch(config)#access-group ip-group 2000
Activate ACL successfully .
```

!Before configuration

```
Switch(config)#show access-list config 2000
Standard IP Access List 1, match-order is auto, 2 rule:
0 permit 1.1.1.1 0.0.0.0
1 deny any
```

!Configuration steps

```
Switch(config)#access-group ip-group 1 subitem 1
Activate ACL successfully .
Switch(config)#access-group ip-group 1 subitem 0
Activate ACL successfully .
```

17.5.2 Activate ACL successfully .Active ACL Binding

IP+MAC+Port binds through ACL binding active.

!Configuration request

MAC is 00:00:00:00:00:01, IP address of 1.1.1.1 the user can only enter from e0/0/1 mouth.

!Configuration steps

```
Switch(config)#access-list 2000 permit 1.1.1.1 0
Switch(config)#access-list 4000 permit ingress 00:00:00:00:00:01 0 interface
ethernet 0/0/1 egress any
Switch(config)#access-group ip-group 2000 link-group 4000
```

17.6 Displaying and Debugging ACL

After finishing above configuration, you can see configuration as below commands.

Table 98 Display and debug ACL

OPERATION	COMMAND	REMARK
Display ACL statistics	show access-list config statistic	perform either of the commands
Display ACL configuration	show access-list config {all num name name}	
Display ACL	show access-list runtime {all num name name}	

Storm-control Configuration

18.1 Storm-control Overview

When there is loop or malicious attacker in the network, there will be plenty of packets, which occupy the bandwidth and even affect the network. Storm-control will avoid too much packets appear in the network. Restrict the speed rate of port receiving broadcast/multicast/ unknown unicast packets and unknown unicast packets received by all ports.

18.2 Storm-Control Configuration

18.2.1 Configure Storm-Control

Storm-Control configuration is configured in global configuration mode and enable/disable in interface configuration mode, that is, administrator can enable it per port.

Table 99 Configure Storm-control

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure storm-control type and rate	<code>Storm-control type {broadcast multicast unicast } rate <64-32000000></code>	Required
Enter interface configuration mode	<code>interface ethernet device/slot/port</code>	-

18.2.2 Storm-control Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 100 Storm-control monitor and maintenance

OPERATION	COMMAND	REMARKS
Show interface	<code>show storm-control interface ethernet slot/port</code>	On any configuration mode

Note: If there is no configuration for storm-control, there will be no info show for that.

QoS Configuration

19.1 Brief Introduction to QoS

In traditional IP networks, every packet is treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order of packets arriving. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

With the fast development of computer networks, more and more networks are connected into Internet. Users hope to get better services, such as dedicated bandwidth, transfer delay, jitter voice, image, important data which enrich network service resources and always face network congestion. Internet users bring forward higher requirements for QoS. Ethernet technology is the widest network technology in the world recently. Now, Ethernet becomes the leading technology in every independent LAN, and many LAN in the form of Ethernet have become a part of internet. With the development of Ethernet technology, Ethernet connecting will become one of main connecting for internet users. To execute end-to-end QoS solution has to consider the service guarantee of Ethernet QoS, which needs Ethernet device applies to Ethernet technology to provide different levels of QoS guarantee for different types of service flow, especially the service flow highly requiring delay and jitter.

19.1.1 Traffic

Traffic means all packets through switch.

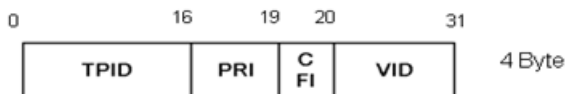
19.1.2 Traffic Classification

Traffic classification is to identify packets conforming to certain characters according to certain rules. It is the basis and prerequisite for proving differentiated services. A traffic classification rule can use the precedence bits in the type of service (ToS) field of the IP packet header to identify traffic with different precedence characteristics. A traffic classification rule can also classify traffic according to the traffic classification policy set by the network administrator, such as the combination of source address, destination address, MAC address, IP protocol, or the port numbers of the application. Traffic classification is generally based on the information in the packet header and rarely based on the content of the packet.

19.1.3 Priority

- 1 802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2. As shown in the chapter of VLAN configuration. Each host supported 802.1Q protocol forwards packets which are from Ethernet frame source address add a 4-byte tag header. See [Figure 26 on page 129](#).

Figure 26 802.1Q tag



As shown in the figure above, PRI segment is 802.1p priority. It consists of 3 bits whose range is from 0 to 7. The three bits point the frame priority. The tag including 8 formats gives the precedence to forward the packets.

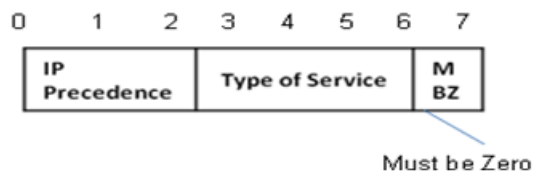
Table 101 Description on 802.1Q values

COS (DECIMAL)	COS (BINARY)	DESCRIPTION
0	000	spare
1	001	background
2	010	best-effort
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

- 2 IP precedence, TOS precedence, and DSCP values

The TOS field in the IP header contains eight bits: the first three bits represent IP precedence; the subsequent four bits represent a ToS value and 1 bit with currently unused defaults 0. The four bits of TOS packets are grouped into four classes: the smallest time delay, maximum rate, highly reliability, minimum cost. Only 1 bit can be set, if the DSCP values equal 0, that means normal service.

Figure 27 IP precedence and TOS precedence



IP precedence contains 8 formats.

Table 102 Description on IP Precedence

IP PRECEDENCE (DECIMAL)	IP PRECEDENCE (BINARY)	DESCRIPTION
0	000	routine
1	001	priority

Table 102 Description on IP Precedence

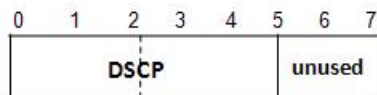
IP PRECEDENCE (DECIMAL)	IP PRECEDENCE (BINARY)	DESCRIPTION
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

TOS precedence contains 5 formats.

Table 103 Description on TOS Precedence

TOS (DECIMAL)	TOS (BINARY)	DESCRIPTION
0	0000	normal
1	0001	min-monetary-cost
2	0010	max-reliability
4	0100	max-throughput
8	1000	min-delay

According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and ranges from 0 to 63. The remaining two bits (6 and 7) are reserved.

Figure 28 DSCP values

In a network in the Diff-Serve model, traffic is grouped into the following classes, and packets are processed according to their DSCP values

- Expedited forwarding (EF) class: In this class, packets are forwarded regardless of link share of other traffic. The class is suitable for preferential services requiring low delay, low packet loss, low jitter, and high bandwidth.
- Assured forwarding (AF) class: This class is divided into four subclasses (AF 1 to AF 4), each containing three drop priorities for more granular classification. The QoS level of the AF class is lower than that of the EF class.
- Class selector (CS) class: This class is derived from the IP ToS field and includes eight subclasses.
- Best effort (BE) class: This class is a special CS class that does not provide any assurance. AF traffic exceeding the limit is degraded to the BE class. All IP network traffic belongs to this class by default.

Table 104 Description on DSCP values

DSCP (DECIMAL)	DSCP (BINARY)	KEYS
0	000000	be
46	101110	ef
10	001010	af1

Table 104 Description on DSCP values

DSCP (DECIMAL)	DSCP (BINARY)	KEYS
18	010010	af2
26	011010	af3
34	100010	af4
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7

19.1.4 Access Control List

To classify flow is to provide service distinctively which must be connected resource distributing. To adopt which kind of flow control is related to the stage it is in and the current load of the network. For example: monitor packet according to the promised average speed rate when the packet is in the network and queue scheduling manage the packet before it is out of the node.

19.1.5 Packet Filtration

Packet filtration is to filtrate service flow, such as deny, that is, deny the service flow which is matching the traffic classification, and permit other flows to pass. System adopts complicated flow classification to filtrate all kinds of information of service layer 2 packets to deny useless, unreliable, and doubtable service flow to strengthen network security.

Two key points of realizing packet filtration:

- 1 Classify ingress flows according to some regulation;
- 2 Filtrate distinct flow by denying. Deny is default accessing control.

19.1.6 Flow Monitor

In order to serve customers better with the limited network resources, QoS can monitor service flow of specified user in ingress interface, which can adapt to the distributed network resources.

19.1.7 Interface Speed Limitation

Interface speed limitation is the speed limit based on interface which limits the total speed rate of interface outputting packet.

19.1.8 Redirection

User can re-specify the packet transmission interface based on the need of its own QoS strategies.

19.1.9 Priority Mark

Ethernet switch can provide priority mark service for specified packet, which includes: TOS, DSCP, 802.1p. These priority marks can adapt different QoS model and can be defined in these different models.

19.1.10 Choose Interface Outputting Queue for Packet

Ethernet switch can choose corresponding outputting queue for specified packets.

19.1.11 Queue Scheduler

It adopts queue scheduler to solve the problem of resource contention of many packets when network congestion. There are three queue scheduler matchings: Strict-Priority Queue (PQ), Weighted Round Robin (WRR) and WRR with maximum delay.

1 PQ

PQ (Priority Queuing) is designed for key service application. Key service possesses an important feature, that is, require the precedent service to reduce the response delay when network congestion. Priority queue divides all packets into 4 levels, that is, superior priority, middle priority, normal priority and inferior priority (3, 2, 1, 0), and their priority levels reduce in turn.

When queue scheduler, PQ precedently transmits the packets in superior priority according to the priority level. Transmit packet in inferior priority when the superior one is empty. Put the key service in the superior one, and non-key service (such as email) in inferior one to guarantee the packets in superior group can be first transmitted and non-key service can be transmitted in the spare time.

The shortage of PQ is: when there is network congestion, there are more packets in superior group for a long time, the packets in inferior priority will wait longer.

2 WRR

WRR queue scheduler divides a port into 4 or 8 outputting queues (S2926V-O has 4 queues, that is, 3, 2, 1, 0) and each scheduler is in turn to guarantee the service time for each queue. WRR can configure a weighted value (that is, w3, w2, w1, w0 in turn) which means the percentage of obtaining the resources. For example: There is a port of 100M. Configure its WRR queue scheduler value to be 50, 30, 10, 10 (corresponding w3, w2, w1, w0 in turn) to guarantee the inferior priority queue to gain at least 10Mbit/s bandwidth, to avoid the shortage of PQ queue scheduler in which packets may not gain the service.

WRR possesses another advantage. The scheduler of many queues is in turn, but the time for service is not fixed-if some queue is free, it will change to the next queue scheduler to make full use of bandwidth resources.

3 SP+ WRR

Superior priority or less priority use SP algorithm, others use WRR algorithm.

19.1.12 Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol

System will map between 802.1p protocol priority of packet and hardware queue priority. For each packet, system will map it to specified hardware queue priority according to 802.1p protocol priority of packet.

19.1.13 Flow Mirror

Flow mirror means coping specified data packet to monitor interface to detect network and exclude failure.

19.1.14 Statistics Based on Flow

Statistics based on flow can statistic and analyze the packets customer interested in.

19.1.15 Copy Packet to CPU

User can copy specified packet to CPU according to the need of its QoS strategies.

System realizes QoS function according to accessing control list, which includes: flow monitor, interface speed limit, packet redirection, priority mark, queue scheduler, flow mirror, flow statistics, and coping packet to CPU.

19.2 QoS Configuration

19.2.1 Configuring Flow Monitor

Flow monitor is restriction to flow rate which can monitor the speed of a flow entering switch. If the flow is beyond specified specification, it will take actions, such as dropping packet or reconfigure their priority.

Table 105 Configure flow rate

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Configure flow rate	<code>rate-limit { input output } { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } target-rate</code>	

19.2.2 Configure Two Rate Three Color Marker

Two Rate Three Color Marker is defined in RFC 2698. There is 4 parameter for it: CIR, CBS, PIR and PBS.

Table 106 Configure Two Rate Three Color Marker

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Configure Two Rate Three Color Marker	<code>two-rate-policer { [mode {color-aware color-bind} [set-pre-color dscp-value {green red yellow}]] }</code>	optional
Configure Two Rate Three Color Marker	<code>rate-limit { input output } { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } two-rate-policer policer-id</code>	optional

19.2.3 Configuring Interface Line Rate

Line-limit is the speed limit based on interface which restricts the total speed of packet outputting.

Table 107 Configure interface line rate

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet device/slot/port</code>	-
Configure egress rate	<code>bandwidth egress target-rate</code>	optional <i>target-rate</i> should be a multiple of 64Kbps.
Configure ingress rate	<code>bandwidth ingress target-rate</code>	optional <i>target-rate</i> should be a multiple of 64Kbps.

19.2.4 Configuring Packet Redirection

Packet redirection configuration is redirecting packet to be transmitted to some egress.

Table 108 Configure packet redirection

OPERATION	COMMAND	REMARK
Enter globally configuration mode	configure terminal	-
Configure packet redirection	traffic-redirect { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } { [interface interface-num cpu] }	optional

19.2.5 Configuring Traffic Copy to CPU

Switch automatically copies to CPU after configuring traffic copy to CPU.

Table 109 Configure traffic copy to CPU

OPERATION	COMMAND	REMARK
Enter globally configuration mode	configure terminal	-
Configure traffic copy to CPU	traffic-copy-to-cpu { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] }	optional

19.2.6 Configuring Traffic Priority

Traffic priority configuration is the strategy of remark priority for matching packet in ACL, and the marked priority can be filled in the domain which reflects priority in packet head.

Table 110 Configure traffic priority

OPERATION	COMMAND	REMARK
Enter globally configuration mode	configure terminal	-
Configure traffic priority	traffic-priority { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } { [dscp dscp-value] [cos { pre-value from-ipprec }] [local-precedence pre-value] }	optional
Enter global configuration mode	configure terminal	

19.2.7 Configuring Queue-Scheduler

When network congestion, it must use queue-scheduler to solve the problem of resource competition. System supports 3 kinds of queue-scheduler, that is SP, WRR and full SP+WRR. By default is SP in system.

Table 111 Configure queue-scheduler

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Configure SP	<code>queue-scheduler strict-priority</code>	optional
Configure WRR	<code>queue-scheduler wrr queue1-weight queue2-weight queue3-weight queue4- weight</code>	optional
Configure SR+WRR	<code>queue-scheduler sp-wrr queue1-weight queue2-weight queue3-weight</code>	optional

19.2.8 Configuring Cos-map Relationship of Hardware Priority Queue and Priority of IEEE802.1p Protocol

The cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol is one - to - one correspondence. Administrators change the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol timely when the one-to-one correspondence shifting.

By default, the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol as below:

Table 112 802.1p and he cos-map relationship of hardware priority queue

802.1P	HARDWARE PRIORITY QUEUE
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Administrators also change the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol according to the actual network.

Table 113 Modifying 802.1p and he cos-map relationship of hardware priority queue

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Modify 802.1p and he cos-map relationship of hardware priority queue	<code>queue-scheduler cos-map queue- number packed-priority</code>	optional

19.2.9 Configuring Mapping Relationship between DSCP and 8 Priority in IEEE 802.1p

The same situation as 1.2.7, by default, the relation between DSCP and 8 priority in IEEE 802.1p as below;

Table 114 Relation between DSCP and 8 priority in IEEE 802.1p

SCP	HARDWARE PRIORITY QUEUE	DSCP	HARDWARE PRIORITY QUEUE	DSCP	HARDWARE PRIORITY QUEUE	DSCP	HARDWARE PRIORITY QUEUE
0	0	16	1	32	2	48	3
1	0	17	1	33	2	49	3
2	0	18	1	34	2	50	3
3	0	19	1	35	2	51	3
4	0	20	1	36	2	52	3
5	0	21	1	37	2	53	3
6	0	22	1	38	2	54	3
7	0	23	1	39	2	55	3
8	0	24	1	40	2	56	3
9	0	25	1	41	2	57	3
10	0	26	1	42	2	58	3
11	0	27	1	43	2	59	3
12	0	28	1	44	2	60	3
13	0	29	1	45	2	61	3
14	0	30	1	46	2	62	3
15	0	31	1	47	2	63	3

Administrators also change the mapping relationship between DSCP and 8 priority in IEEE 802.1p according to the actual network.

Table 115 Configuring the relation between DSCP and 8 priority in IEEE 802.1p

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Startup the relation between DSCP and 8 priority in IEEE 802.1p	<code>queue-scheduler dscp-map</code>	required
		by default, it is disable.
Modify the relation between DSCP and 8 priority in IEEE 802.1p	<code>queue-scheduler dscp-map</code> <code>dscp-value 802.1p-priority</code>	optional

19.2.10 Configuring Flow Statistic

Flow statistic configuration is used to statistic specified service flow packet. The statistic is accumulated value and reset to zero when re-configuring.

Table 116 Configure flow statistic

OPERATION	COMMAND	REMARK
Enter globally configuration mode	<code>configure terminal</code>	-
Configure flow statistic	<code>traffic-statistic { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] }</code>	optional
reset to Zero	<code>clear traffic-statistic { [all [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]]] }</code>	optional

19.2.11 Configuring Flow Mirror

Flow mirror is copying the service flow which matches ACL rules to specified monitor interface to analyze and monitor packet.

19.2.12 Displaying and Maintain QoS

After finishing above configuration, please use below commands to show the configuration.

Table 117 Display and maintain QoS

OPERATION	COMMAND	REMARK
Display all the informaion of QoS	<code>show qos-info all</code>	perform either of the commands
Display QoS statistic	<code>show qos-info statistic</code>	
Display queue-scheduler mode and parameters	<code>show queueY-scheduler</code>	
Display the cos-map relationship of hardware priority queue and priority of IEEE802.1p protocol	<code>show queue-scheduler cos-map</code>	
Display the dscp-map relationship of hardware priority queue and priority of IEEE802.1p protocol	<code>show queue-scheduler dscp-map</code>	
Display all QoS port configuration	<code>show qos-interface all</code>	
Display rate-limit parameters	<code>show qos-interface [interface-num] rate-limit</code>	
Display interface line rate parameters	<code>show bandwidth-control interface Ethernet [interface-num]</code>	
Display QoS interface statistic parameters	<code>show qos-interface statistic</code>	
Display traffic-priority parameters	<code>show qos-info traffic-priority</code>	
Display traffic-redirect parameters	<code>show qos-info traffic-redirect</code>	
Display packet redirection	<code>show qos-info traffic-statistic</code>	
Display information of traffic copy to CPU	<code>show qos-info traffic-copy-to-cpu</code>	

STP Configuration

20.1 STP Overview

20.1.1 Function of STP

Spanning Tree Protocol (STP) is applied in loop network to block some undesirable redundant paths with certain algorithms and prune the network into a loop-free tree, thereby avoiding the proliferation and infinite cycling of the packet in the loop network.

20.1.2 Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP-compliant network devices. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used for calculating spanning trees and maintaining the spanning tree topology.
- Topology change notification (TCN) BPDUs, used for notifying concerned devices of network topology changes, if any.

20.1.3 Basic Concepts in STP

1 Root Bridge

A tree network must have a root; hence the concept of “root bridge” has been introduced in STP.

There is one and only one root bridge in the entire network, and the root bridge can change alone with changes of the network topology. Therefore, the root bridge is not fixed.

Upon network convergence, the root bridge generates and sends out configuration BPDUs at a certain interval, and other devices just forward the BPDUs. This mechanism ensures topological stability.

2 Root Port

On a non-root bridge device, the root port is the port nearest to the root bridge. The root port is responsible for communication with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

3 Designated Bridge

For a device, Designated Bridge is the device directly connected with this device and responsible for forwarding BPDUs; For a LAN, Designated Bridge is the device responsible for forwarding BPDUs to this LAN segment.

4 Designated Port

For a device, Designated Port is the port through which the designated bridge forwards BPDUs to this device; For a LAN, Designated Port is the port through which the designated bridge forwards BPDUs to this LAN segment.

5 Path cost

Path cost is a reference value used for link selection in STP. By calculating the path cost, STP selects relatively "robust" links and blocks redundant links, and finally prunes the network into loop-free tree structure.

20.1.4 Spanning-Tree Interface States

Each Layer 2 interface on a switch using spanning tree exists in one of these states:

- **Disabled**

The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

- **Blocking**

The interface does not participate in frame forwarding.

- **Listening**

The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.

- **Learning**

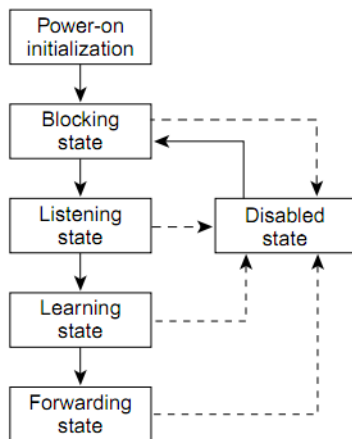
The interface prepares to participate in frame forwarding.

- **Forwarding**

The interface forwards frames.

An interface moves through these states:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled

Figure 29 Spanning-Tree Interface States

When you power up the switch, spanning tree is enabled by default, and every interface in the switch, VLAN, or network goes through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking states.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

- 1 The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
- 2 While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
- 3 In the learning state, the interface continues to block frame forwarding as the switch learns end-station location information for the forwarding database.
- 4 When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

20.2 How STP Works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID: consisting of root bridge priority and MAC address.
- Root path cost: the cost of the shortest path to the root bridge.
- Designated bridge ID: designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port name.
- Message age: age of the configuration BPDU while it propagates in the network.
- Max age: maximum age of the configuration BPDU maintained in the device.
- Hello time: configuration BPDU interval.
- Forward delay: forward delay of the port.

Note: For the convenience of description, the description and examples below involve only four parts of a configuration BPDU:

- Root bridge ID (in the form of device priority)
- Root path cost
- Designated bridge ID (in the form of device priority)
- Designated port ID (in the form of port name)

1 Specific calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each port generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Table 118 Selection of the optimum configuration BPDU

STEP	DESCRIPTION
1	<p>Upon receiving a configuration BPDU on a port, the device performs the following processing:</p> <ul style="list-style-type: none"> • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

Note: Principle for configuration BPDU comparison:

The configuration BPDU that has the lowest root bridge ID has the highest priority.

If all configuration BPDUs have the same root bridge ID, they will be compared for their root path costs. If the root path cost in a configuration BPDU plus the path cost corresponding to this port is S , the configuration BPDU with the smallest S value has the highest priority.

If all configuration BPDUs have the same root path cost, they will be compared for their designated bridge IDs, then their designated port IDs, and then the IDs of the ports on which they are received. The smaller the ID, the higher message priority.

- Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the devices compare one another's root bridge ID. The device with the smallest root bridge ID is elected as the root bridge.

- Selection of the root port and designated ports

The process of selecting the root port and designated ports is as follows:

Table 119 Selection of the root port and designated ports

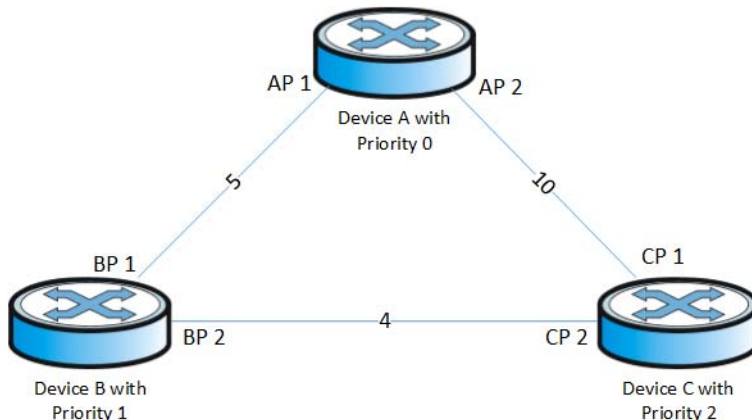
STEP	DESCRIPTION
1	A non-root-ridge device regards the port on which it received the optimum configuration BPDU as the root port.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. <ul style="list-style-type: none"> • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port of which the port role is to be defined, and does different things according to the comparison result: <ul style="list-style-type: none"> • If the calculated configuration BPDU is superior, the device will consider this port as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. • If the configuration BPDU on the port is superior, the device will block this port without updating its configuration BPDU, so that the port will only receive BPDUs, but not send any, and will not forward data.

Note: When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state- they only receive STP packets but do not forward user traffic.

Once the root bridge, the root port on each non-root bridge and designated ports have been unsuccessfully elected, the entire tree-shaped topology has been constructed.

The following is an example of how the STP algorithm works. The specific network diagram is shown in [Figure 30 on page 144](#). In the feature, the priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

Figure 30 Network diagram for the STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 120 Initial state of each device

DEVICE	PORT NAME	BPDU OF PORT
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

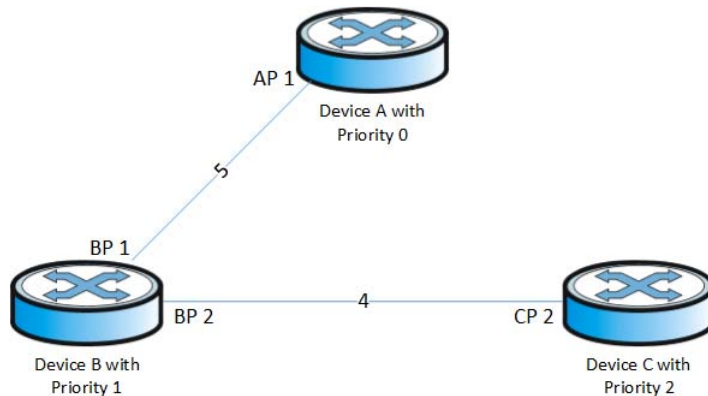
Table 121 Comparison process and result on each device

DEVICE	COMPARISON PROCESS	BPDU OF PORT AFTER COMPARISON
Device A	<ul style="list-style-type: none"> • Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the configuration received message, and discards the received configuration BPDU. • Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. • Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are Device A itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically. 	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	<ul style="list-style-type: none"> • Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1. • Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. 	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	<ul style="list-style-type: none"> • Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. • Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. • Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically. 	Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}

Table 121 Comparison process and result on each device

DEVICE	COMPARISON PROCESS	BPDU OF PORT AFTER COMPARISON
Device C	<ul style="list-style-type: none"> Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and updates the configuration BPDU of CP2. 	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	By comparison: <ul style="list-style-type: none"> The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU. 	Root port CP1: {0, 0, 0, AP2} Designated port CP2: {0, 10, 2, CP2}
	Next, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process. At the same time, port CP1 receives configuration BPDUs periodically from Device A. Device C does not launch an update process after comparison.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	By comparison: <ul style="list-style-type: none"> Because the root path cost of CP2 (9) (root path cost of the BPDU (5) plus path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down. 	Blocked port CP2: {0, 0, 0, AP2} Root port CP2: {0, 5, 1, BP2}

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in [Figure 31 on page 146](#).

Figure 31 The final calculated spanning tree

Note: To facilitate description, the spanning tree calculation process in this example is simplified, while the actual process is more complicated.

2 The BPDU forwarding mechanism in STP

- Upon network initiation, every switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.
- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.
- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately send out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device will generate a configuration BPDU with itself as the root and sends out the BPDU. This triggers a new spanning tree calculation process so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

3 STP timers

STP calculations need three important timing parameters: forward delay, hello time, and max age.

- Forward delay is the delay time for device state transition. A path failure will cause re-calculation of the spanning tree, and the spanning tree structure will change accordingly. However, the new configuration BPDU as the calculation result cannot be propagated throughout the network immediately. If the newly elected root port and designated ports start to forward data right away, a temporary loop is likely to occur. For this reason, as a mechanism for state transition in STP, a newly elected root port or designated port requires twice the forward delay time before transitioning to the forwarding state, when the new configuration BPDU has been propagated throughout the network.
- Hello time is the time interval at which a device sends hello packets to the surrounding devices to ensure that the paths are fault-free.
- Max age is a parameter used to determine whether a configuration BPDU held by the device has expired. A configuration BPDU beyond the max age will be discarded.

20.3 Implement RSTP on Ethernet Switch

The Ethernet Switch implements the Rapid Spanning Tree Protocol (RSTP), i.e., the enhancement of STP. The Forward Delay for the root ports and designated ports to enter forwarding state is greatly reduced in certain conditions, thereby shortening the time period for stabilizing the network topology.

To achieve the rapid transition of the root port state, the following requirement should be met: The old root port on this switch has stopped data forwarding and the designated port in the upstream has begun forwarding data.

The conditions for rapid state transition of the designated port are:

- The port is an Edge port that does not connect with any switch directly or indirectly. If the designated port is an edge port, it can switch to forwarding state directly without immediately forwarding data.
- The port is connected with the point-to-point link, that is, it is the master port in aggregation ports or full duplex port. It is feasible to configure a point-to-point connection. However, errors may occur and therefore this configuration is not recommended. If the designated port is connected with the point-to-point link, it can enter the forwarding state right after handshaking with the downstream switch and receiving the response.

The switch that uses RSTP is compatible with the one using STP. Both protocol packets can be identified by the switch running RSTP and used in spanning tree calculation.

Note: RSTP is the protocol of single spanning tree. A switching network only has one spanning tree. To guarantee the normal communication inside a VLAN, the devices of a VLAN shall have routes to one another on the Spanning Tree, otherwise, the communication inside the VLAN will be affected if some links inside a VLAN are blocked.

For some VLAN that cannot be arranged along the spanning tree paths for some special requirements, you have to disable RSTP on the switch port corresponding to the VLAN.

20.4 Configure RSTP

20.4.1 RSTP Configuration Task List

Table 122 RSTP Configuration Task List

CONFIGURATION TASK LIST		REMARKS	
RSTP basic configuration	Enable STP	Required	20.4.2
	Select the working mode	Required	20.4.2

Table 122 RSTP Configuration Task List

CONFIGURATION TASK LIST		REMARKS	
Configure RSTP	Configure STP bridge priority	Optional	20.4.3
	Configure Hello-packet sending interval	Optional	20.4.4
	Configure STP forward-delay	Optional	20.4.4
	Configure STP max-age	Optional	20.4.4
	Configure STP path cost	Optional	20.4.5
	Configure STP port priority	Optional	20.4.6
	Configure STP mcheck	Optional	20.4.7
	Configure STP point-to-point mode	Optional	20.4.8
	Configure STP portfast	Optional	20.4.9
	Configure STP transit limit	Optional	20.4.10
	Configure STP Root Protection	Optional	20.4.11
	Configure STP Loop Guard	Optional	20.4.12
	Configure STP BPDU Guard	Optional	20.4.13
	Configure STP BPDU Filter	Optional	20.4.14
Show RSTP		Optional	20.4.15

20.4.2 Enable RSTP

After enabling STP globally, all ports will be defaulted to join the STP topology calculating by default. If some port is not allowed to take part in the STP calculation, administrator can use `interface ethernet` command to enter interface configuration mode and then use `no spanning-tree` command to disable STP on this port.

Table 123 Enable STP

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable STP globally	<code>spanning-tree</code>	Required
Select STP mode	<code>spanning-tree mode stp</code>	Optional
Enter interface configuration mode	<code>interface ethernet device/slot/port</code>	-
Enable/disable STP on port	<code>(no) spanning-tree</code>	Optional

Note: When enable STP globally, the system is working under RSTP mode.

20.4.3 Configure STP Bridge Priority

The priority of bridge determines this switch can be root or not. If this switch is needed to be the root, the priority can be configured inferior.

By default, the switch bridge priority is 32768.

Table 124 Configure STP priority

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure STP priority	<code>spanning-tree priority <i>bridge priority</i></code>	Optional

20.4.4 Configure Time Parameter

There are three time parameters: Forward Delay, Hello Time and Max Age.

User can configure these three parameters for RSTP calculation.

Table 125 Configure the time parameter

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure Hello-packet sending interval	<code>spanning-tree hello-time <i>seconds</i></code>	Optional
Configure STP forward-delay	<code>spanning-tree forward-time <i>seconds</i></code>	Optional
Configure STP max-age	<code>spanning-tree max-age <i>seconds</i></code>	Optional

Note:

- Too long Hello Time may cause link failure thought by network bridge for losing packets of the link to restart accounting STP; too smaller Hello Time may cause network bridge frequently to send configuration packet to strengthen the load of network and CPU. Hello Time ranges from 1 to 10 seconds. It is suggested to use the default time of 2 seconds. $\text{Hello Time} \leq \text{Forward Delay} - 2$.
- If Forward Delay is configured too small, temporary redundancy will be caused; if Forward Delay is configured too large, network will not be restored linking for a long time. Forward Delay ranges from 4 to 30 seconds. The default forward delay time, 15 seconds is suggested to use. $\text{Forward Delay} \geq \text{Hello Time} + 2$.
- Max Age is used to configure the longest aging interval of STP. Lose packet when over-timing. The STP will be frequently accounts and take crowded network to be link fault, if the value is too small. If the value is too large, the link fault cannot be known timely. Max Age is determined by diameter of network, and the default time of 20 seconds is suggested. $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$ When enable STP globally, the system is working under RSTP mode.

20.4.5 Configure STP Path Cost

Configure interface STP path cost and choose the path with the smallest path cost to be the effective path.

The path cost is related to the link speed rate. The larger the speed rate is, the less the cost is. STP can auto-detect the link speed rate of current interface and converse it to be the cost.

Configure port path cost will make STP re-calculating. The value of the path cost is 1-65535. It is suggested using the default value, which makes the STP to calculate the current port cost by itself. By default, the path cost is determined by the current port speed.

When the port is 10M, the default cost is 200,000; when the port is 100M, the default cost is 20,000; 1000M, 2,000.

Table 126 Configure STP path cost

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	Optional
Configure STP path cost	<code>spanning-tree cost <i>path-cost</i></code>	Optional

If the port aggregation is enabled, the cost could be configured by the following command.

Table 127 Configure STP path cost

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure STP path cost for aggregation ID	<code>channel-group <i>id</i> spanning-tree cost <i>path-cost</i></code>	Optional

20.4.6 Configure STP Port Priority

Specify specified port in STP by configuring port priority. Generally, the smaller the value is, the superior the priority is, and the port will be more possible to be included in STP. If the priorities are the same, the port number is considered.

The smaller the value is, the superior the priority is, and the port is easier to be the root interface. Change the port priority may cause the re-calculating of the STP. The port priority ranges from 0 to 240 and the value should be divided by 16. The default port priority is 128.

Table 128 Configure STP port priority

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure STP port priority	<code>spanning-tree port-priority <i>priority</i></code>	Optional

20.4.7 Configure STP mcheck

Switch working under RSTP mode can be connected to switch with STP. But when the neighbor is working under RSTP, the two connected ports are still work under STP mode. The mcheck function is for force port sending RSTP packet to make sure the two neighbor ports can be working under RSTP. If yes, the working mode will turn to be RSTP.

Table 129 Configure STP mcheck

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure STP mcheck	<code>spanning-tree mcheck</code>	Optional

20.4.8 Configure STP Point-to-Point Mode

In RSTP, the requirement of interface quickly in transmission status is that the interface must be point to point link, not media sharing link. It can be specified interface link mode manually and can also judge it by network bridge.

If the configuration of point-to-point mode is *auto*, the port in full-duplex is point-to-point link type and the port in half-duplex is not point-to-point link type.

If the configuration of point-to-point mode is *forcetrue*, the port is point-to-point link type.

If the configuration of point-to-point mode is *forcefalse*, the port is not point-to-point link type.

Table 130 Configure STP point-to-point mode

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet interface-num</code>	-
Configure switch auto-check the point-to-point	<code>spanning-tree point-to-point auto</code>	Optional
Configure STP point-to-point mode forcetrue	<code>spanning-tree point-to-point forcetrue</code>	Optional
Configure STP point-to-point mode forcefalse	<code>spanning-tree point-to-point forcefalse</code>	Optional

20.4.9 Configure STP Portfast

Edge port is the port connecting to the host which can be in transmission status in very short time after linkup, but once the port receiving STP packet, it will shift to be non-edge port. The portfast configuration only works in RSTP.

Table 131 Configure STP portfast

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet interface-num</code>	-
Configure STP portfast	<code>spanning-tree portfast</code>	Optional

20.4.10 Configure STP Transit Limit

Restrict STP occupying bandwidth by restricting the speed of sending BPDU packet. The speed is determined by the number of BPDU sent in each hello time.

By default, port will send 3 BPDU packets in every Hello time interval.

Table 132 Configure STP transit limit

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet interface-num</code>	-
Configure STP transit limit	<code>spanning-tree transit-limit transit-limit</code>	Optional

20.4.11 Root Protection

Due to the wrong configuration or attacking, the root bridge could receive supervisor BPDUs and it will cause the topology changed. The root protection feature can avoid this case.

There are two actions in root protection is enabled when switch receives a supervisor BPDUs.

block-port: discard the BPDU and block this port.

drop-packets: only discard the BPDUs.

Table 133 Configure STP root protection

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure the action of root protection	<code>spanning-tree root-guard action {block-port drop-packets}</code>	-
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Enable root protection on this port	<code>spanning-tree root-guard</code>	
Disable root protection on this port	<code>no spanning-tree root-guard</code>	

20.4.12 Loop Guard

When the function is active, the port will keep in block state even it cannot receive any configuration BPDUs.

Table 134 Configure loop guard

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet interface-num</code>	
Enable loop guard on this port	<code>spanning-tree loop-guard</code>	
Disable loop guard on this port	<code>no spanning-tree loop-guard</code>	

20.4.13 BPDU Guard

The device on access layer are directly connect to user terminals, such as PC or NB and the port on the device will be configured as an edge port. If the edge port receives configuration BPDUs, the edge port will be reconfigured and the spanning tree will be calculated. The BPDU guard can prevent this cases.

When the edge port receives configuration BPDUs, the switch will shut down this port and send syslog message to syslog server.

Table 135 Configure BPDU Guard

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable BPDU Guard Feature on this device	<code>spanning-tree bpdu-guard</code>	
Disable BPDU Guard Feature on this device	<code>no spanning-tree bpdu-guard</code>	

Table 135 Configure BPDU Guard

OPERATION	COMMAND	REMARKS
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	
Enable BPDU Guard on this port	<code>spanning-tree bpdu-guard</code>	
Disable BPDU Guard on this port	<code>no spanning-tree bpdu-guard</code>	

20.4.14 BPDU Filter

The edge port with activate BPDU filter will drop any configuration BPDUs, and this port do not send any BPDUs.

Table 136 Configure BPDU Filter

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable BPDU Filter Feature on this device	<code>spanning-tree bpdu-filter</code>	
Disable BPDU Filter Feature on this device	<code>no spanning-tree bpdu-filter</code>	
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	
Enable BPDU Filter on this port	<code>spanning-tree bpdu-filter</code>	
Disable BPDU Filter on this port	<code>no spanning-tree bpdu-filter</code>	

20.4.15 RSTP Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 137 RSTP monitor and maintenance

OPERATION	COMMAND	REMARKS
Show STP interface	<code>show spanning-tree interface [brief [ethernet <i>device/slot/port</i>]]</code>	On any configuration mode

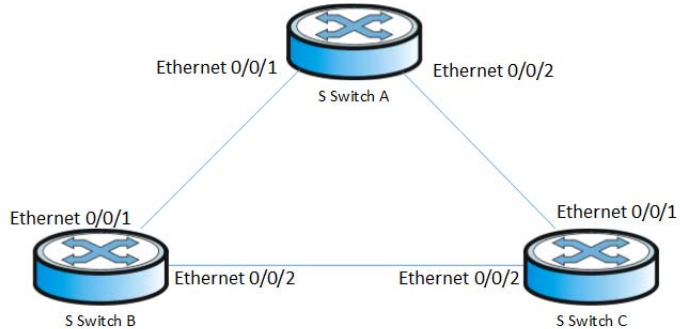
20.4.16 STP Configuration Example

Network requirements

As shown in following figure, S-switch-A is core switch as the root and S-switch-B is the bridge. The link between S-switch-A and S-switch-B is backup link. When there is failure between S-switch-B and S-switch-C, the link between S-switch-A and S-switch-B can work normally.

Network diagram

Figure 32 STP network example



Configuration procedure

The default STP mode is RSTP. Enable global RSTP and use its default time parameter.

Configure Switch A

Here are commands in S-switch-A

```
#configure Ethernet0/0/1 and Ethernet0/0/2 to be trunk, and enable root-guard

S-switch-A(config)#interface range ethernet 0/0/1 ethernet 0/0/2
S-switch-A(config-if-range)#switchport mode trunk
S-switch-A(config-if-range)#spanning-tree root-guard
S-switch-A(config-if-range)#exit

# configure S-switch-A priority to be 0 to make sure S-switch-A is root

S-switch-A(config)#spanning-tree priority 0

# Enable global RSTP
S-switch-A(config)#spanning-tree
```

Configure Switch B

Here are commands in S-switch-B

```
#configure Ethernet0/0/1 and Ethernet0/0/2 to be trunk

S-switch-B(config)#interface range ethernet 0/0/1 ethernet 0/0/2
S-switch-B(config-if-range)#switchport mode trunk
S-switch-B(config-if-range)#exit

# configure S-switch-B priority to be 4096 to make sure S-switch-B is bridge. Configure
cost of Ethernet0/0/1 and Ethernet0/0/2 to be 10

S-switch-B(config)#spanning-tree priority 4096
S-switch-B(config)#interface range ethernet 0/0/1 ethernet 0/0/2
S-switch-B(config-if-range)#spanning-tree cost 10
S-switch-B(config-if-range)#exit

# Enable global RSTP

S-switch-B(config)#spanning-tree
```

Configure Switch C

Here are commands in S-switch-C

```
#configure Ethernet0/0/1 and Ethernet0/0/2 to be trunk

S-switch-C(config)#interface range ethernet 0/0/1 ethernet 0/0/2
S-switch-C(config-if-range)#switchport mode trunk
S-switch-C(config-if-range)#exit

#Configure cost of Ethernet0/0/1 and Ethernet0/0/2 to be 10 to make sure link
between S-switch-B and S-switch-C to be main link

S-switch-C(config)#interface range ethernet 0/0/1 ethernet 0/0/2
S-switch-C(config-if-range)#spanning-tree cost 10
S-switch-C(config-if-range)#exit

# Enable global RSTP

S-switch-C(config)#spanning-tree
```

Check the configuration

S-switch-A

Use `show spanning-tree interface` command to check configuration.

```
S-switch-A(config)#show spanning-tree interface ethernet 0/0/1 ethernet 0/
0/2
The bridge is executing the IEEE Rapid Spanning Tree protocol
The bridge has priority 0, MAC address: 000a.5a13.b13d
Configured Hello Time 2 second(s), Max Age 20 second(s),
Forward Delay 15 second(s)
Root Bridge has priority 0, MAC address 000a.5a13.b13d
Path cost to root bridge is 0
Stp top change 3 times

Port e0/0/1 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a DesignatedPort
Port path cost 200000
Port priority 128
root guard enabled and port is not in root-inconsistent state
Designated bridge has priority 0, MAC address 000a.5a13.b13d
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 0
sent BPDU: 54
TCN: 0, RST: 54, Config BPDU: 0
received BPDU: 10
TCN: 0, RST: 10, Config BPDU: 0

Port e0/0/2 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a DesignatedPort
Port path cost 200000
Port priority 128
root guard enabled and port is not in root-inconsistent state
Designated bridge has priority 0, MAC address 000a.5a13.b13d
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
Times: Hello Time 2 second(s), Max Age 20 second(s)
Forward Delay 15 second(s), Message Age 0
sent BPDU: 16
TCN: 0, RST: 17, Config BPDU: 0
received BPDU: 3
TCN: 0, RST: 3, Config BPDU: 0
```

S-switch-B

Use `show spanning-tree interface` command to check configuration.

```
S-switch-B(config)#show spanning-tree interface ethernet 0/0/1 ethernet 0/0/2
The bridge is executing the IEEE Rapid Spanning Tree protocol
The bridge has priority 4096, MAC address: 0000.0077.8899
Configured Hello Time 2 second(s), Max Age 20 second(s),
Forward Delay 15 second(s)
Root Bridge has priority 0, MAC address 000a.5a13.b13d
Path cost to root bridge is 10
Stp top change 3 times

Port e0/0/1 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a RootPort
Port path cost 10
Port priority 128
root guard disabled and port is not in root-inconsistent state
Designated bridge has priority 0, MAC address 000a.5a13.b13d
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
  Times: Hello Time 2 second(s), Max Age 20 second(s)
        Forward Delay 15 second(s), Message Age 0
  sent BPDUs:      21
        TCN: 0, RST: 12, Config BPDU: 9
  received BPDU: 204
        TCN: 0, RST: 202, Config BPDU: 2

Port e0/0/2 of bridge is Forwarding
Spanning tree protocol is enabled
remote loop detect is disabled
The port is a DesignatedPort
Port path cost 10
Port priority 128
root guard disabled and port is not in root-inconsistent state
Designated bridge has priority 4096, MAC address 0000.0077.8899
The Port is a non-edge port
Connected to a point-to-point LAN segment
Maximum transmission limit is 3 BPDUs per hello time
  Times: Hello Time 2 second(s), Max Age 20 second(s)
        Forward Delay 15 second(s), Message Age 1
  sent BPDUs:      191
        TCN: 0, RST: 188, Config BPDU: 3
  received BPDU: 13
        TCN: 0, RST: 5, Config BPDU: 8
```

S-switch-C

Use `show spanning-tree interface` command to check configuration.

```
S-switch-C(config)#show spanning-tree interface ethernet 0/0/1 ethernet 0/0/2
The bridge is executing the IEEE Rapid Spanning Tree protocol
  The bridge has priority 32768, MAC address: 000a.5a13.f48e
  Configured Hello Time 2 second(s), Max Age 20 second(s),
  Forward Delay 15 second(s)
  Root Bridge has priority 0, MAC address 000a.5a13.b13d
  Path cost to root bridge is 20
  Stp top change 3 times

Port e0/0/1 of bridge is Discarding
  Spanning tree protocol is enabled
  remote loop detect is disabled
  The port is a AlternatePort
  Port path cost 200000
  Port priority 128
  root guard disabled and port is not in root-inconsistent state
  Designated bridge has priority 0, MAC address 000a.5a13.b13d
  The Port is a non-edge port
  Connected to a point-to-point LAN segment
  Maximum transmission limit is 3 BPDUs per hello time
  Times: Hello Time 2 second(s), Max Age 20 second(s)
        Forward Delay 15 second(s), Message Age 0
  sent BPDUs:      3
        TCN: 0, RST: 3, Config BPDUs: 0
  received BPDUs: 396
        TCN: 0, RST: 396, Config BPDUs: 0

Port e0/0/2 of bridge is Forwarding
  Spanning tree protocol is enabled
  remote loop detect is disabled
  The port is a RootPort
  Port path cost 10
  Port priority 128
  root guard disabled and port is not in root-inconsistent state
  Designated bridge has priority 4096, MAC address 0000.0077.8899
  The Port is a non-edge port
  Connected to a point-to-point LAN segment
  Maximum transmission limit is 3 BPDUs per hello time
  Times: Hello Time 2 second(s), Max Age 20 second(s)
        Forward Delay 15 second(s), Message Age 1
  sent BPDUs:      8
        TCN: 0, RST: 8, Config BPDUs: 0
  received BPDUs: 418
        TCN: 0, RST: 418, Config BPDUs: 0
```

Configuring 802.1X

21.1 Brief Introduction to 802.1X Configuration

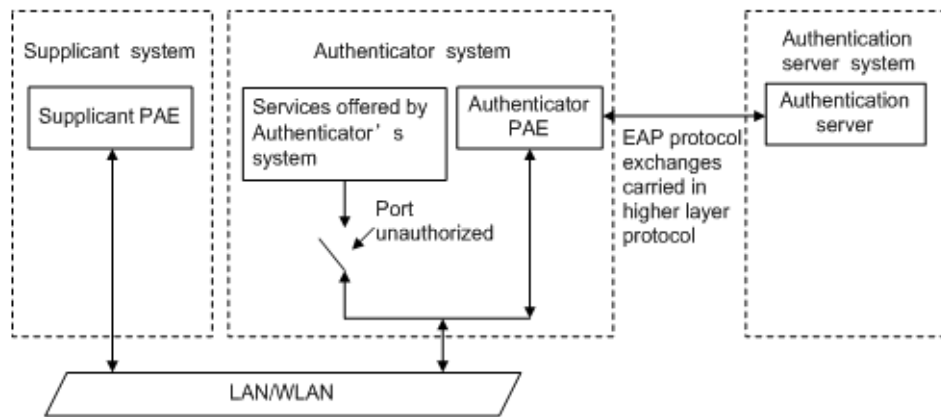
IEEE 802.1X is the accessing management protocol standard based on interface accessing control passed in June, 2001. Traditional LAN does not provide accessing authentication. Users access the devices and resources in LAN when connecting to the LAN, which is a security hidden trouble. For application of motional office and CPN, device provider hopes to control and configure user's connecting. There is also the need for accounting.

IEEE 802.1X is a network accessing control technology based on interface which is the accessing devices authentication and control by physical accessing level of LAN devices. Physical accessing level here means the interface of LAN Switch devices. When getting authentication, switch is the in-between (agency) of client and authentication server. It obtains user's identity from client of accessing switch and verifies the information through authentication server. If the authentication passes, this user is allowed to access LAN resources or it will be refused.

21.1.1 Architecture of 802.1X

802.1X operates in the typical client/server model and defines three entities: supplicant system, authenticator system, and authentication server system, as shown in [Figure 33 on page 161](#).

- Supplicant system: A system at one end of the LAN segment, which is authenticated by the authenticator system at the other end. A supplicant system is usually a user-end device and initiates 802.1x authentication through 802.1x client software supporting the EAP over LANs (EAPOL) protocol.
- Authenticator system: A system at the other end of the LAN segment, which authenticates the connected supplicant system. An authenticator system is usually an 802.1x-enabled network device and provides ports (physical or logical) for supplicants to access the LAN.
- Authentication server system: The system providing authentication, authorization, and accounting services for the authenticator system. The authentication server, usually a Remote Authentication Dial-in User Service (RADIUS) server, maintains user information like username, password, VLAN that the user belongs to, committed access rate (CAR) parameters, priority, and ACLs.

Figure 33 Architecture of 802.1x

The above systems involve three basic concepts: PAE, controlled port, control direction.

1 PAE

Port access entity (PAE) refers to the entity that performs the 802.1x algorithm and protocol operations.

- The authenticator PAE uses the authentication server to authenticate a supplicant trying to access the LAN and controls the status of the controlled port according to the authentication result, putting the controlled port in the authorized or unauthorized state. In authorized state, the port allows user data to pass, enabling the supplicant(s) to access the network resources; while in unauthorized state, the port denies all data of the supplicant(s).
- The supplicant PAE responds to the authentication request of the authenticator PAE and provides authentication information. The supplicant PAE can also send authentication requests and logoff requests to the authenticator.

2 Controlled port and uncontrolled port

An authenticator provides ports for supplicants to access the LAN. Each of the ports can be regarded as two logical ports: a controlled port and an uncontrolled port.

- The uncontrolled port is always open in both the inbound and outbound directions to allow EAPOL protocol frames to pass, guaranteeing that the supplicant can always send and receive authentication frames.
- The controlled port is open to allow normal traffic to pass only when it is in the authorized state.
- The controlled port and uncontrolled port are two parts of the same port. Any frames arriving at the port are visible to both of them.

3 Control direction

In the unauthorized state, the controlled port can be set to deny traffic to and from the supplicant or just the traffic from the supplicant.

21.1.2 Rule of 802.1x

The 802.1x authentication system employs the Extensible Authentication Protocol (EAP) to exchange authentication information between the supplicant PAE, authenticator PAE, and authentication server.

At present, the EAP relay mode supports four authentication methods: EAP-MD5, EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol).

- 1 When a user launches the 802.1x client software and enters the registered username and password, the 802.1x client software generates an EAPOL-Start frame and sends it to the authenticator to initiate an authentication process.
- 2 Upon receiving the EAPOL-Start frame, the authenticator responds with an EAP-Request/Identity packet for the username of the supplicant.
- 3 When the supplicant receives the EAP-Request/Identity packet, it encapsulates the username in an EAP-Response/Identity packet and sends the packet to the authenticator.
- 4 Upon receiving the EAP-Response/Identity packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.
- 5 When receiving the RADIUS Access-Request packet, the RADIUS server compares the identify information against its user information table to obtain the corresponding password information. Then, it encrypts the password information using a randomly generated challenge, and sends the challenge information through a RADIUS Access-Challenge packet to the authenticator.
- 6 After receiving the RADIUS Access-Challenge packet, the authenticator relays the contained EAP-Request/MD5 Challenge packet to the supplicant.
- 7 When receiving the EAP-Request/MD5 Challenge packet, the supplicant uses the offered challenge to encrypt the password part (this process is not reversible), creates an EAP-Response/MD5 Challenge packet, and then sends the packet to the authenticator.
- 8 After receiving the EAP-Response/MD5 Challenge packet, the authenticator relays the packet in a RADIUS Access-Request packet to the authentication server.
- 9 When receiving the RADIUS Access-Request packet, the RADIUS server compares the password information encapsulated in the packet with that generated by itself. If the two are identical, the authentication server considers the user valid and sends to the authenticator a RADIUS Access-Accept packet.
- 10 Upon receiving the RADIUS Access-Accept packet, the authenticator opens the port to grant the access request of the supplicant. After the supplicant gets online, the authenticator periodically sends handshake requests to the supplicant to check whether the supplicant is still online. By default, if two consecutive handshake attempts end up with failure, the authenticator concludes that the supplicant has gone offline and performs the necessary operations, guaranteeing that the authenticator always knows when a supplicant goes offline.
- 11 The supplicant can also send an EAPOL-Logoff frame to the authenticator to go offline unsolicitedly. In this case, the authenticator changes the status of the port from authorized to unauthorized and sends an EAP-Failure frame to the supplicant.

21.1.3 Configuring AAA

Finish necessary configuration of domain and RDIUS project of 802.1X authentication.

21.1.4 Configuring RADIUS Server

RADIUS server saves valid user's identity. When authentication, system transfers user's identity to RADIUS server and transfer the validation to user. User accessing to system can access LAN resources after authentication of RADIUS server.

Table 138 Configure RADIUS server

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter AAA mode	<code>aaa</code>	required
Enter RADIUS configuration	<code>radius host name</code>	required
Configure primary RADIUS	<code>primary-auth-ip ipaddr port</code>	required
Configure second RADIUS	<code>second-auth-ip ipaddr port</code>	optional
Configure key string of primary RADIUS	<code>auth-secret-key keystring</code>	required
Configure key string of second RADIUS	<code>acct -secret-key keystring</code>	optional
Configure NAS-RADIUS address	<code>nas-ipaddress ipaddr</code>	optional
Setup the username format	<code>username-format { with-domain without-domain }</code>	optional
Configure accounting	<code>realtime-account</code>	optional
Configure the times of accounting	<code>realtime-account interval <time></code>	optional

21.1.5 Configuring Local User

Client need configure local user name and password.

Table 139 Configure local user

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter AAA mode	<code>aaa</code>	required
Configure local user	<code>local-user username name password pwd [vlan vid]</code>	required

21.1.6 Configuring Domain

Client need provide username and password when authentication. Username contains user's ISP information, domain and ISP corresponded. The main information of domain is the RADIUS server authentication and accounting the user should be.

Table 140 Configure Domain

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter AAA mode	<code>aaa</code>	required
Configure default Domain	<code>default domain-name domain-name</code>	required
setup Domain	<code>domain name</code>	required
Configure default Domain scheme	<code>scheme { local radius [local] }</code>	required

Table 140 Configure Domain

OPERATION	COMMAND	REMARKS
choice RADIUS name	radius host binding <i>radius-name</i>	optional
configure access limit users	access-limit { enable <i>number</i> disable }	optional
active the state	state { active block }	required

21.1.7 Configuring RADIUS Features

Configuring RADIUS some compatible or special features as below:

Table 141 Configure RADIUS features

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	-
Enter AAA mode	aaa	required
Enable user re-authentication, when it executives, the device restarts after a user authentication to the RADIUS server sends Accounting-On message, notify the RADIUS server to force the device goes offline.	accounting-on { enable <i>sen-num</i> disable }	optional
H3C Cams compatible under this feature can uprate-value / dnrte-value to configure the upstream bandwidth / downstream bandwidth of the Vendor Specific attribute name of the attribute number.	h3c-cams { enable disable }	optional
This feature can be under the RADIUS attribute client-version to the version of configuration information to send the client to the RADIUS server.		
accounting function	radius accounting	optional
Accounting packets without response need cut off users	radius server-disconnect drop 1x	optional
port priority	radius 8021p enable	optional
This feature is turned on, if the user authentication passes, it will be modified by the user where the priority of the port.		
This feature is by default the property name in the Vendor Specific attribute number to 77, with radius config-attribute you can modify the properties of numbers.		
Port PVID	radius vlan enable	optional
This feature is turned on, if the user authentication passes , it will be modified by the user where port PVID is		
This function is fixed by the Tunnel-Pvt-Group-ID attribute names, which requires a string of the property value, this string for the VLAN by name descriptor matches the VLAN value.		

Table 141 Configure RADIUS features

OPERATION	COMMAND	REMARKS
Limit port of MAC address numbers	radius mac-address-number enable	optional
This feature is turned on, if the user authentication passes, the user will modify the port about the limiting number of MAC address learning.		
This feature is by default the property name in the Vendor Specific attribute number to 50, with radius config-attribute you can modify the properties of numbers.		
Limit port bandwidth	radius bandwidth-limit enable	optional
This feature is turned on, if the user authentication passes, the user will modify the port bandwidth limitation. Upstream bandwidth control carries out per attribute number 75 in Vendor specific attribution and be modified attribution by using radius config-attribute. Downstream bandwidth control carries out per attribute number 76 in Vendor specific attribution and be modified attribution by using radius config-attribute.		
By default unit is kbps, can be modified through radius config-attribute access-bandwidth unit.		

21.2 Configuring 802.1X

21.2.1 Configuring EAP

The 802.1X authentication can be initiated by either a supplicant or the authenticator system. A supplicant can initiate authentication by launching the 802.1x client software to send an EAPOL-Start frame to the authenticator system, while an authenticator system can initiate authentication by unsolicitedly sending an EAP-Request/Identity packet to an unauthenticated supplicant.

Table 142 Configure EAP

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	-
set the protocol type between system and RADIUS	dot1x eap-finish eap-transfer	optional

21.2.2 Enable 802.1x

802.1x provides a user identity authentication scheme. However, 802.1x cannot implement the authentication scheme solely by itself. RADIUS or local authentication must be configured to work with 802.1x

Enabling 802.1S authentication, users connected to the system can access to LAN per passing the authentication.

Table 143 Enable 802.1x

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable 802.1x	<code>dot1x method { macbased portbased }</code>	required

21.2.3 Configuring 802.1x Parameters for a Port

The 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Table 144 Configure 802.1x parameters for a port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure 802.1x parameters for a port	<code>dot1x port-control { auto forceauthorized forceunauthorized } [interface-list]</code>	required

21.2.4 Configuring Re-Authentication

In EAP-FINISH way, the port supports re-authentication. After the user is authenticated, the port can be configured to immediately re-certification, or periodic re-certification.

Table 145 Configure re-authentication

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Immediately re-certification	<code>dot1x re-authenticate [interface-list]</code>	Optional
Periodic re-authentication enabled on a port	<code>dot1x re-authentication [interface-list]</code>	Optional
Periodic re-authentication time configuration port	<code>dot1x timeout re-authperiod time [interface-list]</code>	Optional

21.2.5 Configuring Watch Feature

Opening function, the port without the user's circumstances, will watch regularly sends a 1x packet, triggering the following 802.1x user authentication.

Table 146 Configure watch feature

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Open the watch function	<code>dot1x daemon [interface-list]</code>	Optional
Configuration time between sending packets Watch	<code>dot1x daemon time time [interface-list]</code>	Optional

21.2.6 Configuring User Features

The operations mainly conclude of the number of users for port configuration, user and delete users, and heartbeat detection operations.

Table 147 Configure user feature

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configuration allows the maximum number of users through the authentication	<code>dot1x max-user [interface-list]</code>	Optional
Deletes the specified users online	<code>dot1x user cut {username name mac-address mac [vlan vid]}</code>	Optional
Open heartbeat detection	<code>dot1x detect [interface-list]</code>	Optional
Heartbeat detection time configuration	<code>dot1x detect interval time</code>	Optional

Configuring MSTP

22.1 Brief Introduction to MSTP

The Spanning Tree Protocol (STP) was established based on the 802.1d standard of IEEE to eliminate physical loops at the data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging information with one another and eliminate loops by selectively blocking certain ports until the loop structure is pruned into a loop-free network structure. This avoids proliferation and infinite recycling of packets that would occur in a loop network and prevents deterioration of the packet processing capability of network devices caused by duplicate packets received.

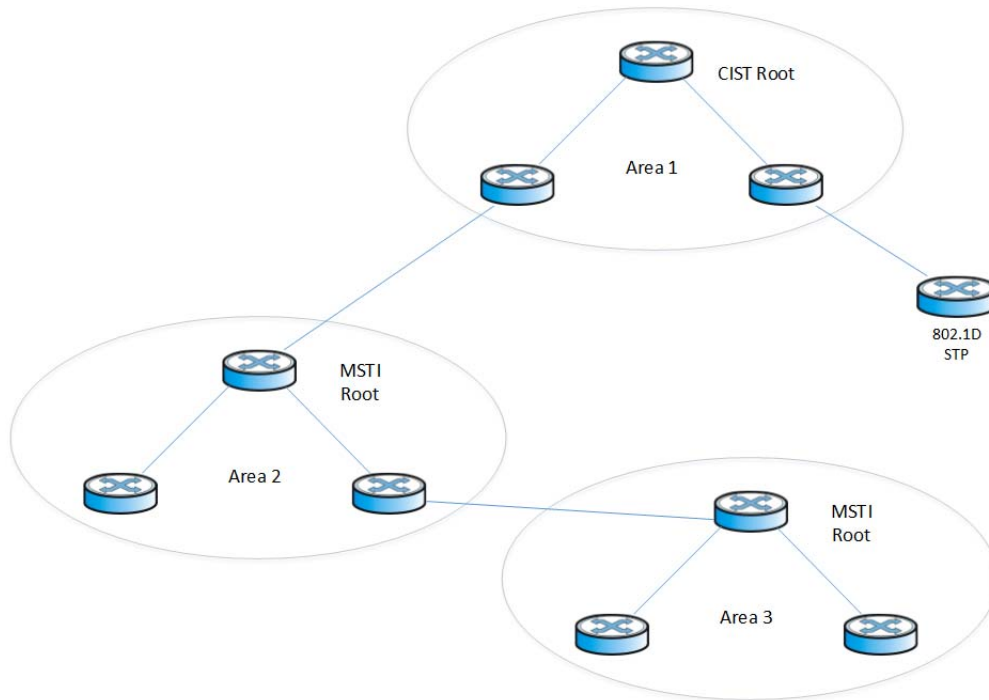
The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links. For description about VLANs, refer to VLAN.

22.2 BPDU

MSTP uses BPDU algorithm the same as STP, RSTP. Meanwhile, BPDU in MSTP also exist MSTP configuration information in the switch.

22.2.1 Basic Concepts in MSTP

Figure 34 MSTP topology example



As shown in [Figure 34 on page 169](#) is the MSTP network. MSTP is composed of three spanning tree areas and a running 802.1D STP protocol switch.

1 MST region

A multiple spanning tree region (MST region) is composed of multiple devices in a switched network and network segments among them. These devices have the following characteristics:

- All are MSTP-enabled.
- They have the same region name.
- They have the same VLAN-to-instance mapping configuration,.
- They have the same MSTP revision level configuration.
- They are physically linked with one another.

Multiple MST regions can exist in a switched network. You can use an MSTP command to group multiple devices to the same MST region.

2 CIST

Jointly constituted by ISTs and the CST, the CIST is a single spanning tree that connects all devices in a switched network.

In [Figure 34 on page 169](#), for example, the ISTs in all MST regions plus the inter-region CST constitute the CIST of the entire network.

3 CST

The CST is a single spanning tree that connects all MST regions in a switched network. If you regard each MST region as a “device”, the CST is a spanning tree calculated by these devices through STP or RSTP. For example, as show in [Figure 34 on page 169](#), CST is composed of Area 1, 2, 3 and STP switch.

4 IST

Internal spanning tree (IST) is a spanning tree that runs in an MST region.

ISTs in all MST regions and the common spanning tree (CST) jointly constitute the common and internal spanning tree (CIST) of the entire network. An IST is a section of the CIST in the given MST region.

5 MSTI

Multiple spanning trees can be generated in an MST region through MSTP, one spanning tree being independent of another. Each spanning tree is referred to as a multiple spanning tree instance (MSTI).

6 CIST root bridge

CIST root, the root bridge of the IST or an MSTI within an MST region is the regional root bridge of the MST or that MSTI. Based on the topology, different spanning trees in an MST region may have different regional roots.

7 CIST External root path cost

External root path cost refers to the cost of the shortest path for a packet to travel to the common root bridge.

8 CIST Internal root path cost

CIST Internal root path cost refers to the cost of the shortest path for a packet to travel to the CIST regional root bridge.

9 CIST designated bridge

CIST designated bridge is the STP appointed bridge

10 MSTI regional root,

The root bridge of the IST or an MSTI within an MST region is the regional root bridge of the IST or the MSTI. Based on the topology, different spanning trees in an MST region may have different regional roots.

11 MSTI internal root path cost

MSTI Internal root path cost refers to the cost of the shortest path for a packet to travel to the MSTI regional root bridge.

12 MSTI Designated bridge

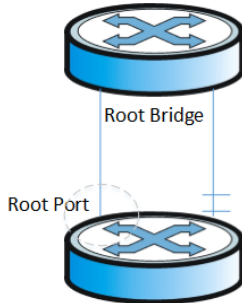
MSTI designated bridge is the STP appointed bridge.

22.2.2 Roles of Ports

In the MSTP calculation process, port roles include root port, designated port, master port, alternate port, backup port, and so on.

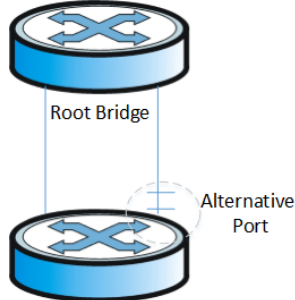
- 1 Root port: a port responsible for forwarding data to the root bridge.

Figure 35 Root port



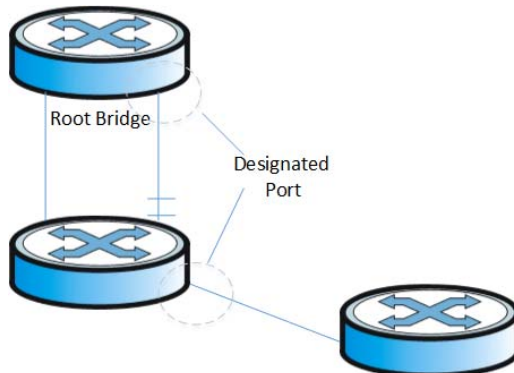
- 2 Alternate port: The standby port for the root port or master port. When the root port or master port is blocked, the alternate port becomes the new root port or master port.

Figure 36 Alternate port

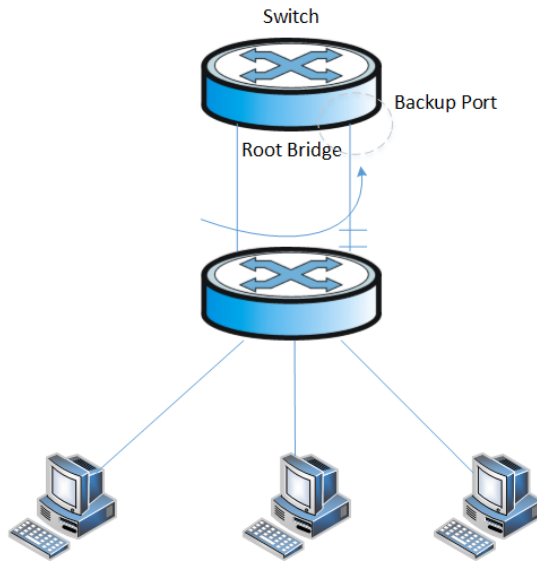


- 3 Designated port: a port responsible for forwarding data to the downstream network segment or device.

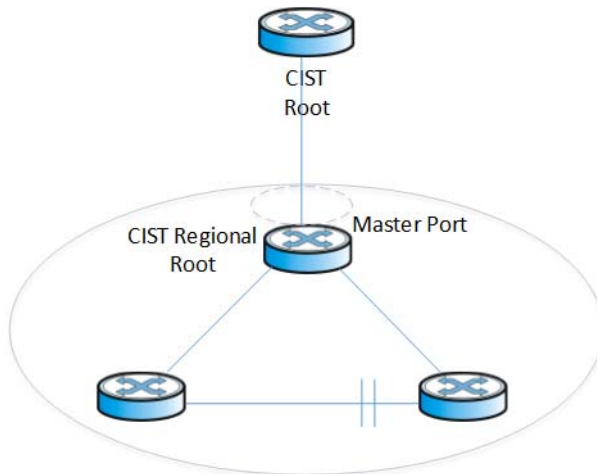
Figure 37 Designated port



- 4 Backup port: The backup port of designated ports. When a designated port is blocked, the backup port becomes a new designated port and starts forwarding data without delay. When a loop occurs while two ports of the same MSTP device are interconnected, the device will block either of the two ports, and the backup port is that port to be blocked.

Figure 38 Backup port

- 5 A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root. In the CST, the master port is the root port of the region, which is considered as a node. The master port is a special boundary port. It is a root port in the IST/CIST while a master port in the other MSTIs

Figure 39 master port

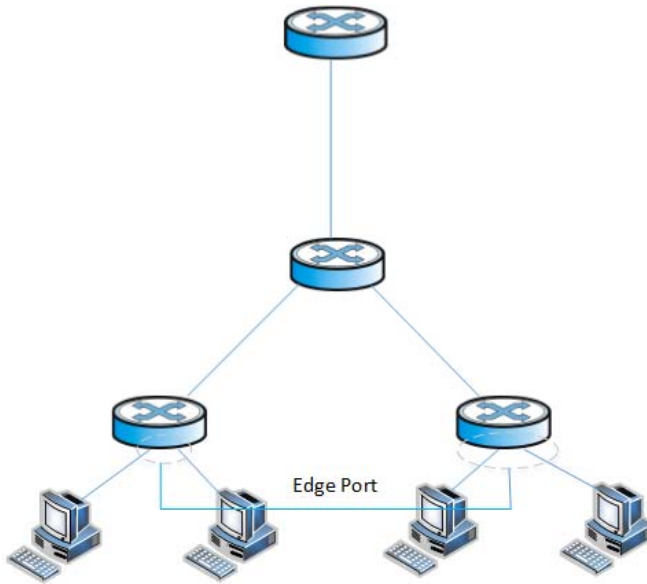
6 Boundary Port

A boundary port is a port that connects an MST region to another MST configuration, or to a single spanning-tree region running STP, or to a single spanning-tree region running RSTP.

During MSTP calculation, a boundary port assumes the same role on the CIST and on MST instances. Namely, if a boundary port is the master port on the CIST, it is also the master port on all MST instances within this region.

7 Edge Port

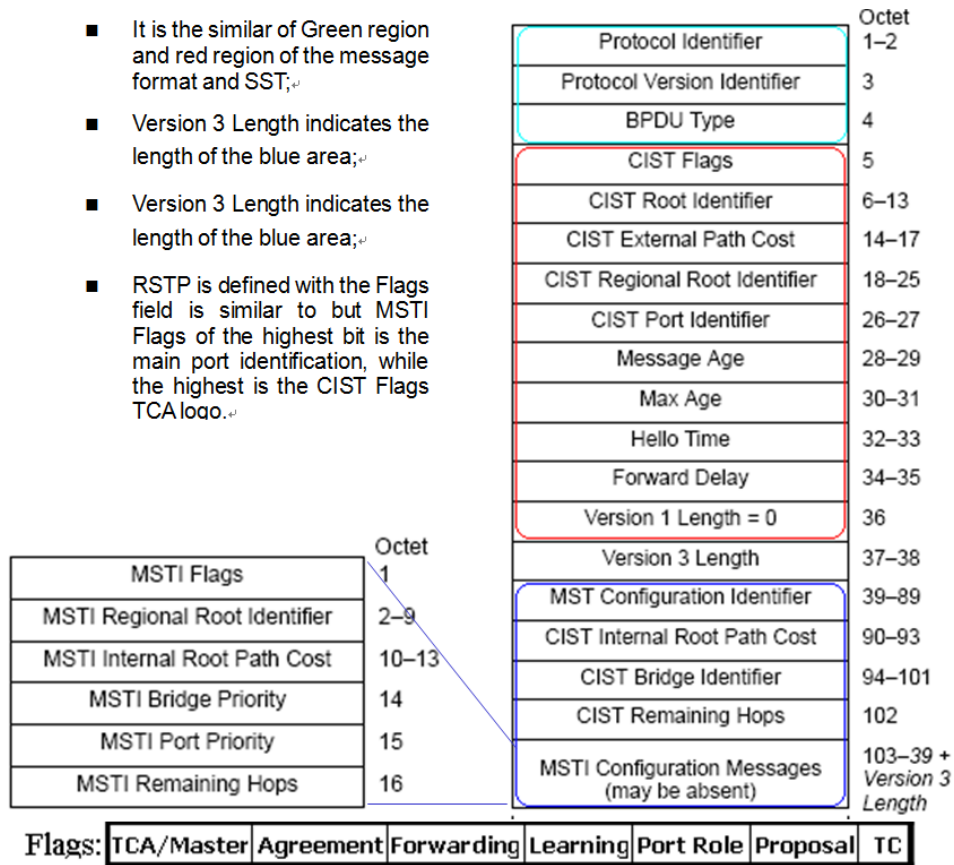
In RSTP and MSTP protocols, edge port means that connect to host port in the network, these ports can be in a forwarding status and not be a loopback without waiting.

Figure 40 Edge Port

22.3 Algorithm Implementation

22.3.1 MSTP Protocol

MST BPDU packet format as below:

Figure 41 MSTP PDU protocol packet

Protocol Identifier: is 0x0000, identifies the Spanning Tree Protocol (2 bytes).

Protocol Version Identifier: as the 0x03, identifies the protocol version (1 byte).

BPDU Type: for the 0x02, that RST BPDU (1 byte).

- CIST Flags: identify the CIST topology change confirmation, consent, forwarding, learning, port role, suggested that the topology change state (1 byte).
- CIST Root Identifier: CIST root bridge's unique identifier, by the CIST root bridge of the CIST root bridge priority and MAC address (8 bytes).
- CIST External Root Path Cost: CIST external root path cost, when only cross-domain changes in the propagation constant region (4 bytes).
- CIST Regional Root Identifier: CIST regional root bridge's unique identifier, the CIST regional root bridge priority and the CIST regional root bridge MAC address, when only cross-domain change in the spread within a fixed time (8 bytes).
- CIST Port Identifier: MST BPDU packets to send the port identified by the port priority and port ID component (2 bytes).
- Message Age: CIST root bridge is from this MST BPDU packets generated since the time when the only cross-domain change in the propagation constant region (2 bytes).
- Max Age: MST BPDU message valid time, this parameter is set by the CIST root bridge (2 bytes).
- Hello Time: CIST root bridge generates MST BPDU packet interval, this parameter is set by the CIST root bridge (2 bytes).

- Forward Delay: forwarding delay, this parameter is set by the CIST root bridge (2 bytes). Its role is twofold:

To be as a port state transition (from Discarding to Learning, from Learning to Forwarding) protocol timer time; in the network topology changes, be as the dynamic filtering database entry aging time.

- Version 1 Length: additional information, is fixed at 0 (1 byte).
- Version 3 Length: instructions from the MST BPDU configuration identification to the end of length of the packet (2 bytes);
- MST Configuration Identifier: MST configuration identification, configuration selected by the device, the configuration name, revision level and configuration summary form only when the cross-domain changes in the propagation constant region (51 bytes).
- CIST Internal Root Path Cost: CIST internal root path cost, effective only in the Ministry of MST region (4 bytes).
- CIST Bridge Identifier: sending MST BPDU packet bridge identified by the bridge priority and MAC address of the bridge (8 bytes).
- CIST Remaining Hops: MST BPDU packets remaining in the CIST in the number of hops (1 byte).
- MSTI Flags: identification of MSTI's main port, agreed to, forward, learning, port role, suggested that the topology change state (1 byte).
- MSTI Regional Root Identifier: MSTI regional root bridge's unique identifier, the MSTI regional root bridge priority, MSTID and MSTI regional root bridge MAC address, its domain for different MSTI root bridge may be different (8 bytes).
- MSTI Internal Root Path Cost: MSTI internal root path cost, effective only in the Ministry of MST region (4 bytes).
- MSTI Bridge Priority: MSTI bridge priority, and the CIST Bridge Identifier of the MAC address of the MSTI configuration information with the composition of the sending bridge (1 byte).
- MSTI Port Priority: MSTI port priority, and the CIST Port Identifier of the port ID with the composition of MSTI send port configuration information (1 byte).
- MSTI Remaining Hops: MST BPDU packets remaining in the MSTI in hops (1 byte).

22.3.2 Determining CIST Priority Vectors

The MSTP role of each bridge is calculated based on the information carried in BPDUs. The most important information carried in BPDUs is the spanning tree priority vector. The following part introduces how to calculate the CIST priority vectors and MSTI priority vectors.

The CIST priority vector consists of common root bridge, external root path cost, regional root, internal root path cost, designated bridge ID, designated port ID, and the BPDU-receiving port ID.

Detailed as below:

- 1 CIST root id
- 2 CIST external root path cost
- 3 CIST regional root id
- 4 CIST internal root path cost
- 5 CIST designated bridge id

- 6 CIST designated port id
- 7 CIST receiving port id

These parameters exist prior, the superior the more precedence.

22.3.3 Determining the MSTI priority vectors

The MSTI priority vector consists of common root bridge, external root path cost, regional root, internal root path cost, designated bridge ID, designated port ID, and the BPDU-receiving port ID.

Detailed as below:

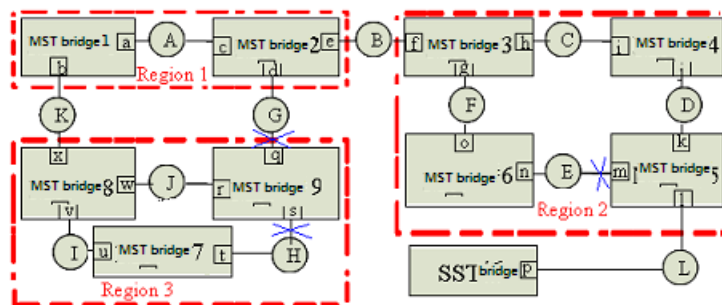
- 1 MSTI regional root id
- 2 MSTI internal root path cost
- 3 MSTI designated bridge
- 4 MSTI designated port
- 5 MSTI receiving port

These parameters exist prior, the superior the more precedence.

22.3.4 Determining MSTP

Determining MSTP divide into two parts, first starts CIST priority vectors, then MSTI priority vectors.

Figure 42



As [Figure 42 on page 176](#), suppose all the cost of the ports in the whole bridge is equal, “MST brige-1”—“MST brige-9”the identify increase by step, “SST bridge” is the most one.

1.3.4.1 Determining CIST Priority Vectors

- 1 The election of CIST root bridge, CIST root port

Throughout the bridged LAN, MST bridge 1 bridge priority of the highest identity, was selected as the CIST root bridge. Assuming Region 2, Region 3 to the CIST root bridge of the external root path cost is 1. Therefore, the bridge 8 MST CIST bridge priority vector update (MST bridge 1,1, MST

Bridge 8,0, MST Bridge 8), MST bridge 8 port x is the CIST root port; MST CIST bridge priority bridge 9 level vector update (MST bridge 1,1, MST Bridge 9,0, MST Bridge 9). Similarly, MST bridge port 3 f is the CIST root port.

2 The election of each domain CIST regional root bridge (IST root bridge), CIST root port CIST

CIST root bridge was elected, they begin to select the various regions of the CIST regional root bridge. To Region 3 as an example:

MST Bridge 7 Port u receive MST CIST bridge 8 priority vector (MST Bridge 1,1, MST Bridge 8,0, MST bridge 8, v), with its own port u (MST Bridge 7,0, MST Bridge 7, 0, MST bridge 7, u) compared to that of MST Bridge 8 better, so the information is updated to the port u (MST bridge 1,1, MST Bridge 8,0, MST bridge 8, v); Similarly, t update the port information (MST bridge 1,1, MST Bridge 9,0, MST Bridge 9, s), then the port 7 MST bridge then u and t CIST priority vector, we found that the port u better information, so the election for the Region 3 8 MST bridge the CIST regional root bridge, MST bridge 7, u is the CIST root port the port. Assuming MST Bridge 7 CIST internal root path cost is 1, then the information will update t port (MST bridge 1,1, MST Bridge 8,1, MST bridge 7, t).

Bridge 8 port w MST received the CIST bridge priority vector 9 (MST Bridge 1,1, MST Bridge 9,0, MST Bridge 9, r), with its own port w (MST Bridge 1,1, MST Bridge 8, 0, MST bridge 8, w) compared to find themselves better, do not update the port information of w; Similarly, port v of the information received MST bridge over the CIST priority vector 7 (MST Bridge 7,0, MST Bridge 7,0, MST bridge 7, u) better, do not update the port v information. Then MST bridge 8 port w and v for CIST priority vector comparison, the election for the Region 3 MST bridge 8 the CIST regional root bridge.

MST Bridge Port 9 r received MST CIST bridge 8 priority vector (MST Bridge 1,1, MST Bridge 8,0, MST bridge 8, w), r with the port itself (MST Bridge 1,1, MST Bridge 9, 0, MST Bridge 9, r) compared to that of MST Bridge 8 better, it will update the port information of r (MST bridge 1,1, MST Bridge 8,0, MST bridge 8, w); port s information than the MST received the CIST bridge priority vector 7 (MST Bridge 7,0, MST Bridge 7,0, MST bridge 7, u) better, do not update the port s of information. Then MST Bridge 9 r and s, with CIST port priority vector comparison, the election for the Region 3 MST bridge 8 the CIST regional root bridge, MST Bridge 9 port r is the CIST root port. Assuming MST Bridge 9 CIST internal root path cost is 1, then the information will be updated to the port s (MST bridge 1,1, MST Bridge 8,1, MST Bridge 9, s).

Similarly, MST bridge 3 was selected as the CIST regional root Region 2 bridge, MST bridge 4 port i is the CIST root port, MST Bridge 5 port k is the CIST root port, MST Bridge 6 o is the CIST root port the port.

As the MST CIST root bridge 1 bridge, so bridge a MST Region 1 is the CIST regional root bridge, MST bridge port 2 c is the CIST root port.

3 All elections within the specified bridge IST, CIST specified port

CIST regional root bridge elected after the Region 3, for example:

MST CIST regional root bridge 8 for the bridge, the port w and v are specified port is the LAN I, J of the designated bridge.

MST Bridge 9 s in the port receiving the message priority vector (MST Bridge 1,1, MST Bridge 8,1, MST bridge 7, t) 9 own bridge than the MST port priority vector (MST Bridge 1,1, MST Bridge 8,1, MST Bridge 9, s) excellent, that is to receive the CIST root bridge, CIST external root path cost, CIST regional root bridge and the CIST internal root path costs are equal, but CIST logo smaller than their designated bridge, so choose MST bridges to LAN 7 H, CIST designated bridge, MST bridge 7 of the CIST port t becomes the designated port, MST Bridge 9 port s port on the

replacement, is set to the Discarding state. Similarly, MST Bridge 2 port d to specify the port, MST Bridge 2 is the designated bridge of G LAN, MST Bridge Port 9 q is replaced by the port, is set to the Discarding state.

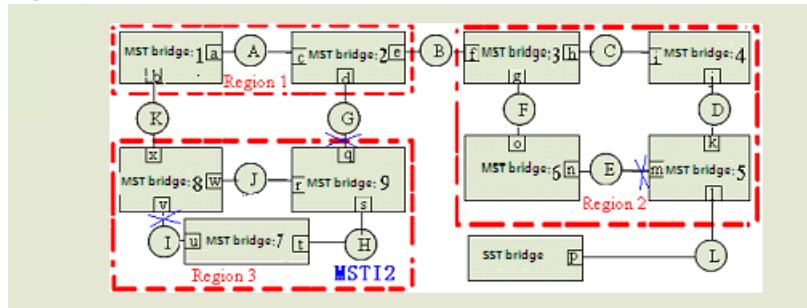
Similarly, in Region 2 in, MST bridge 4 port j for the CIST port specified, MST bridge 4 on the designated bridge for LAN D; MST Bridge 6, n is the CIST port specify a port, MST bridge on the LAN E, 6 designated bridge.

In Region 1 in, MST CIST regional root bridge 1 bridge, so the port a and port b is the designated port is the LAN A designated bridge; MST Bridge 2 port e to the specified port, MST bridge B is designated for the LAN 2 bridge.

1.3.4.2 Determining MSTI Priority Vectors

MSTI elections and the electoral process similar to the single spanning tree, MSTI priority vector is used to compare the election.

Figure 43



To Region 3 as an example MSTI1 formation, as shown in [Figure 43 on page 178](#):

Assuming the bridge priority: MST bridge 9 < MST bridge 8 < MST bridge 7, The path cost of all ports is 1.

1 MSTP domain root bridge election

MST Bridge 7 Bridge highest priority, was selected MSTI regional root bridge.

2 Election of the non-root bridge MSTI root port

MST Bridge 8: Select the port v is the MSTI root port, MSTI internal root path cost is 1.

MST Bridge 9: Select the port s is the MSTI root port, MSTI internal root path cost is 1.

3 Election of the designated bridge of the MSTI port

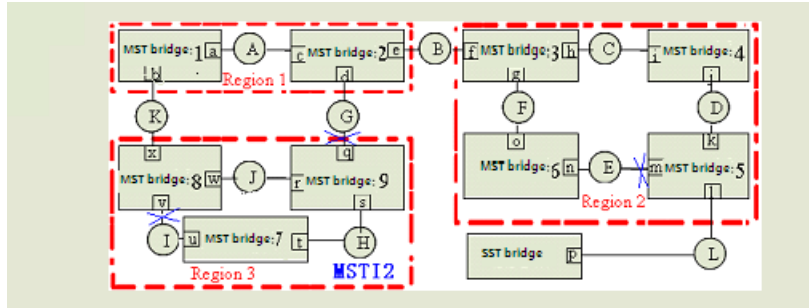
MST Bridge 7: H was selected as the designated regional networks and bridges, ports, u and t as specified MSTI port.

MST Bridge 8: J was selected as the designated bridge the LAN port w is specified MSTI port; port x is Region 3 and the upstream communications port, and is designated as the main port MSTI1 of MSTI.

MST Bridge 9: port s, r is replaced by MSTI port; port q is replaced Region 3 of the CIST port while designated as MSTI1 replace the MSTI port.

LAN J Select MSTI port designated bridge and designated MSTI process: MST Bridge 9 r in the port receiving the message priority vector (MST Bridge 7,1, MST bridge 8, w) 9 own bridge than the MST port priority vector (MST Bridge 7,1, MST Bridge 9, r) excellent, that is to receive the MSTI regional root bridge and MSTI internal root path costs are equal, but MSTI logo smaller than their designated bridge, so choose the LAN MST Bridge J, MSTI 8 designated bridge, LAN port w J, MSTI has become the designated port, the port was set to r Discarding state.

Figure 44



To Region 3 as an example MSTI2 formation, as shown in [Figure 44 on page 179](#):

Assuming the bridge priority: MST bridge 8 < MST bridge 7 < MST bridge 9, The path cost of all ports is 1.

- 1 MST Bridge 9 Bridge highest priority, was selected MSTI regional root bridge.
- 2 MST bridge 7 and 8 of the MSTI internal root path cost is 1, port t and w are MSTI root port.
- 3 MST was selected as the LAN Bridge 9 J and H, designated bridges, ports r and s is the specified MSTI port; MST Bridge 7 was selected as the designated bridge LAN I, u is the MSTI port specified port; MST Bridge Port v 8 was selected as the MSTI port w replace port
- 4 Port x is Region 3 and the upstream communications port, and is designated as the primary port MSTI2 the MSTI; port q is replaced Region 3 of the CIST port while designated as MSTI2 replace the MSTI port.

It can be seen from: MSTI in a Region border port in the CIST role is limited, role for the CIST port if the CIST root port (IST root bridge root port), it is the main port of all MSTI; if the CIST Port Role replace the main port of the CIST port, it is the replacement of all MSTI port. The same port for different MSTI, the port state may be different (such as port v in MSTI1 for forwarding state, and in MSTI2 for discarding state).

In addition, the bridge priority and port priority and port path cost settings for different MSTI unrelated (such as MSTI1 and MSTI2 can configure their parameter values, respectively).

22.3.5 Active Topology

According running MSTP switch receives a BPDU perform calculations and comparison, and ultimately allows the network to reach steady state as follows:

- 1 CIST Root :A switch was selected as the CIST root the entire network;
- 2 Each switch will determine the LAN segment and to the CIST root of the path with minimum cost, to ensure the integrity of the connection and prevent loops;

- 3 Within each region will elect a switch as the CIST regional root (CIST Regional Root), the CIST root switch has reached the minimum cost path;
- 4 Each MSTI will be an independent choice of a switch as the MSTI regional root;
- 5 Each switch within the region and will determine the LAN segment where the MSTI root to reach the path of least cost;
- 6 CIST Root Port provided through the CIST regional root (if not the CIST regional root switch) to reach the CIST root (if not the CIST root switch) with minimum cost path;
- 7 Alternate and Backup ports in the switch, port or LAN connection fails or is removed to provide;
- 8 MSTI root port (Root Port) providing reach the MSTI regional root of the minimum cost path (if the switch is not MSTI regional root bridge);
- 9 A main port (Master Port) to provide regional and regional CIST root bridge outside the connections. Within the region, CIST regional root bridge of the CIST root port as the area of all MSTI master ports.

22.3.6 A Topology Change

MSTP and RSTP topology change in a similar spread.

In MSTP, only one is considered a topology change occurs, that is, when a port changes from an inactive port to port activities that occur when the topology changes, the role of the port is replaced by the port or backup port to switch to the root port, specify the port or the main port.

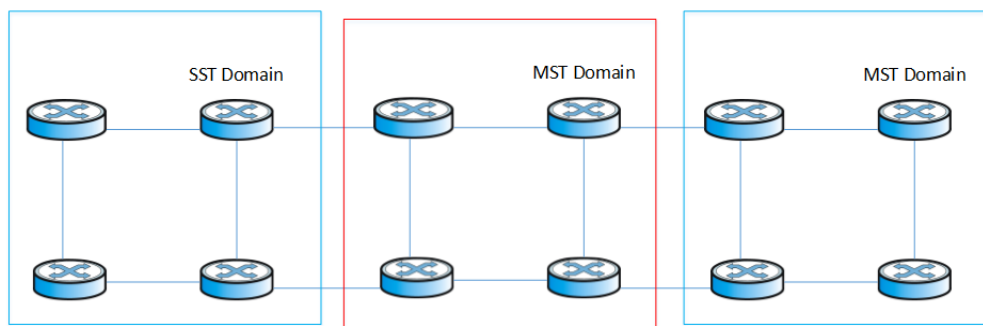
In addition, MSTP and RSTP is also supported as a "proposal / consent" mechanism and point to point link type, used to quickly convert the port state to Forwarding state.

22.3.7 MST and SST Compatibility

MSTP protocol and the MSTP-enabled switch does not support the MSTP switch is divided into different regions, respectively, called the MST region and SST fields, the Ministry of the MST region to run multiple instances of spanning tree, the edge in an MST region to run RSTP compatible protocol.

Diagram below shows MSTP works:

Figure 45



The middle of the red MST region use MSTP BPDUs exchange between the switch topology information, the blue region of the switch use the SST STP / RSTP BPDUs exchange topology information.

MST region and SST fields between the edge of the port on the MSTP processing is slightly more complicated:

When the edge of the other switch port receives STP BPDUs sent by the time the port will enter the STP-compliant state, sending STP BPDUs;

When the edge of the port when the received RSTP BPDUs, the port will enter the RSTP-compatible state, but still send MSTP BPDUs. Because RSTP to consider when designing the expansion, so the equipment side of the RSTP MSTP packets can be understood as the right RSTP packets.

22.4 Configuring MSTP

22.4.1 Configuring MSTP Task

Table 148 Configuring MSTP task

CONFIGURING MSTP TASK		REMARK	DETAILED CONFIGURATION
MSTP basic configuration	Choose STP mode	required	22.4.2
	Enable STP	required	22.4.2
Adjust and optimize the MSTP configuration	Configure bridge forward delay	optional	22.4.3
	Configure bridge hello time	optional	22.4.3
	Configure bridge max aging time	optional	22.4.3
	Configure bridge max hops	optional	22.4.3
	Configure MSTP identifier	optional	22.4.4
	Configure MSTP identifier revision	optional	22.4.4
	Configure MSTP instance configuration and VLAN identifier mapping	optional	22.4.4
	Configure MSTP bridge priority	optional	22.4.5
	Configure the boundary port status	optional	22.4.6
	Configure the port link type	optional	22.4.7
	Configure port internal path cost	optional	22.4.8
	Configure port external path cost	optional	22.4.8
	Configure port priority	optional	22.4.9
	Configure port protection	optional	22.4.10
	Configure port digest Snooping	optional	22.4.11
	Configure port mCheck	optional	22.4.12
	Configure MSTP instance is enabled	optional	22.4.13
Display and maintain MSTP		optional	22.4.14

22.4.2 Enabling MSTP

After the tree starts to give birth to a global default for all ports will participate in the spanning tree topology is calculated, if an administrator wants some of the port does not participate in the calculation of the production tree, or go to the specified port configuration mode, use the no spanning-tree to disable the port Spanning Tree function.

Table 149 Enable MSTP

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Choose STP mode	<code>spanning-tree mode mstp</code>	required
Enable STP	<code>spanning-tree</code>	required
Disable STP	<code>no spanning-tree</code>	
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Enable(disable) port STP	<code>(no) spanning-tree</code>	optional

22.4.3 Configuring MSTP Timer Parameter Values

MSTP timers include: forwarding delay, contracting cycle hello time, maximum aging time, and the maximum hops. Users can configure these three parameters on the switch for MSTP spanning tree.

Table 150 Configure MSTP timer parameter values

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure bridge forward delay	<code>spanning-tree mst forward-time <i>forward-time</i></code>	optional
Configure bridge hello time	<code>spanning-tree mst hello-time <i>hello-time</i></code>	optional
Configure bridge max aging time	<code>spanning-tree mst max-age <i>max-age</i></code>	optional
Configure bridge max hops	<code>spanning-tree mst max-hops <i>max-hops</i></code>	optional

Notes:

- The Hello Time value is too long will lead to packet loss due to leaving the bridge that links the link failure, began to re-calculate the spanning tree; too short can cause the bridge Hello Time value configured to send messages frequently to increase the network and CPU burden. Hello Time value range is 1 to 10 seconds, recommended default value of 2 seconds. Hello Time must be less than equal to the Forward Delay 2.
- If the Forward Delay configuration is too small, may introduce temporary redundant paths; if the Forward Delay configuration is too large, the network may not be a long time to restore connectivity. Forward Delay value range is 4 to 30 seconds, it is recommended to use the default value of 15 seconds. Forward Delay time must be greater than equal to the Hello Time + 2.

- Max Age is used to set the MSTP protocol packet aging longest interval, if the timeout, it discards the packet. If this value is too small, spanning tree will be more frequent, there may be network congestion mistaken link failure; If this value is too large, is not conducive to timely detection of link failures. Max Age of the range is 6 to 40 seconds. Max Age time value and the exchange of the network diameter. Recommended default value of 20 seconds. Max Age time must be greater than equal to $2 * (\text{Hello Time} + 1)$, less than or equal $2 * (\text{Forward Delay} - 1)$.

22.4.4 Configuring MSTP Identifier

MSTP configuration identifiers include: MSTP configuration name, MSTP revision level, and the MSTP instance and VLAN mapping, MSTP will have the same configuration identifier and the bridge connected to each other logically be treated as a virtual bridge.

Table 151 Configure MSTP identifier

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Configure MSTP identifier name	<code>spanning-tree mst name <i>name</i></code>	optional
Configure MSTP identifiers revision	<code>spanning-tree mst revision <i>revision-level</i></code>	optional
Configure MSTP instance configuration and VLAN identifier mapping	<code>spanning-tree mst instance <i>instance-num</i> vlan <i>vlan-list</i></code>	optional
Delete MSTP instance configuration and VLAN identifier mapping	<code>no spanning-tree mst instance <i>instance-num</i> vlan <i>vlan-list</i></code>	

22.4.5 Configuring MSTP Bridge Priority

In MSTP, the bridge priority is based on the parameters of MSTI, the bridge priority together with port priority and port path cost determines the topology of each spanning tree instance, constitute the basis for link load balancing.

Switch bridge priority determines the size of this switch is able to be selected as the spanning tree root bridge. By configuring the bridge priority of the smaller, you can specify a switch to become the spanning tree root bridge purposes.

By default, the switch bridge priority is 32768.

Table 152 Configure MSTP bridge priority

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure MSTP instance priority	<code>spanning-tree mst instance <i>instance-num</i> priority <i>priority</i></code>	optional

22.4.6 Configuring Port Boundary Port Status

Border and port means connected to the host ports that can linkup within a very short time after entering the forwarding state, but once these ports receive spanning tree packets will automatically switch to non-border ports.

Table 153 Configure the port boundary port status

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>Interface ethernet <i>interface-num</i></code>	-
Configure the port boundary port status	<code>(no) spanning-tree mst portfast</code>	optional

22.4.7 Configuring Port Link Type

Port link type is divided into two kinds: First, the type of shared media links (links through the hub, etc.), another type of point to point link. Link type is mainly used in the rapid conversion of the proposed port state - agreed mechanism, only the port link type as point to point only to allow the port state of rapid transformation.

In MSTP, the port state requires quick access to the port forwarding to point to point link, not a shared media link, you can manually specify the port link type, then can determine the port by the bridge current link type.

Table 154 Configure the port link type

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure the switch automatically detects whether the port is point to point link	<code>spanning-tree mst link-type point-to-point auto</code>	Optional
Configure the port connected to the link point to point link	<code>spanning-tree mst link-type point-to-point forcetrue</code>	Optional
Configure the port connected to link non-point link	<code>spanning-tree mst link-type point-to-point forcefalse</code>	Optional

22.4.8 Configuring Path Cost

Port path cost is divided into internal and external costs to spend, the former is based on the configuration parameters for each instance of MSTP, each MSTP region to determine the topology of different instances, which is unrelated to an instance of the parameters used to determine each region of the topology composed of CST.

Cost path through the configuration port, you can make the port more likely to be the root port or designated port.

Port path cost and the link rate on the port, the larger the link rate, the smaller should be the parameter configuration. MSTP protocol can automatically detect the current port link rate, and converted into the corresponding path cost.

Configuring the Ethernet port will cause the spanning tree path cost to recalculate. Port path cost in the range 1 to 65535. Recommended default values, so that their MSTP protocol to calculate the path of the current port cost. By default, the port was based on the rate to determine the path cost.

Port path cost default value is determined according to the port speed, port speed 10M when the default value is 200,000 2,000,000,100 M, while the 1000M is, when 20,000 default. When the time is less than the port speed, path cost default value 200,000.

Table 155 Configure the path cost

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	Optional
Configure internal port path cost	<code>spanning-tree mst instance <i>instance-num</i> cost <i>cost</i></code>	Optional
Configure the port cost of the external path	<code>spanning-tree mst external <i>cost</i> <i>cost</i></code>	Optional

22.4.9 Configuring Port Priority

In MSTP port priority is based on the parameters of each spanning tree instance, by configuring the priority of the port, a port can make it easier to become the root port.

The smaller the priority value that the higher the priority. Change the priority of Ethernet port can cause spanning tree recalculation. Spanning tree port priority values range from 0 to 240, the value must be a multiple of 16. By default, spanning tree port priority is 128.

Table 156 Configure port priority

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure port priority	<code>spanning-tree mst instance <i>instance-num</i> port-priority <i>priority</i></code>	Optional

22.4.10 Configuring Root Port Protection

As the maintenance of configuration errors or malicious network attacks, network valid root bridge may receive a higher priority configuration information, so the root bridge will lose the current status of the root bridge, causing changes in network topology errors. Assuming the original traffic is forwarded through the high-speed links, this is not legally change will lead to the original high-speed links are to low-speed traffic links, resulting in network congestion. Root protection function to prevent this from happening.

Root-protection function of the port, the port can only be kept for a specified port. Once this port received a high priority on the configuration information, status of the ports will be set to the Discarding state, not forwarding packets (equivalent to the link connected to this port is disconnected). When a long enough period of time does not receive better configuration message, the port will revert to the original state.

In MSTP, this function works for all instances.

Table 157 Configure the root port protection

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure the root port protection	<code>spanning-tree mst root-guard</code>	Optional
Disable configure the root port protection	<code>no spanning-tree mst root-guard</code>	

22.4.11 Configuring Digest Snooping Port

When a switch port uses a proprietary spanning tree with Cisco and other switch is connected, these manufacturers' switches configured with the proprietary spanning tree protocol, even if the same MST region configuration, the switch can't be achieved between the MSTP domain interoperability. Digest snooping feature such a situation. With the use of proprietary spanning tree protocol of the manufacturer's switches connected to the port on the digest snooping feature, when receiving the manufacturer's switches over to send a BPDU, the switch that is from the same packet in an MST region, while the configuration summary record; when BPDU packets sent to these manufacturer's switches, the switch configuration summary to supplement it. This switch is realized and the manufacturer's switches in the MSTP region exchange.

Table 158 Configure digest snooping port

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure digest snooping port	<code>spanning-tree mst config-digest-snooping</code>	Optional
Disable configure digest snooping port	<code>no spanning-tree mst config-digest-snooping</code>	

22.4.12 Configuring Port mcheck Function

In order to flexibly control MSTP, you can open the DISABLE INSTANCE features, disable instance STP mode operating results with the implementation of no spanning-tree similar to the instance of the VLAN mapping of all connections on port forwarding state.

Table 159 Configuration port mcheck function

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configuration port mcheck function	<code>spanning-tree mst mcheck</code>	Optional

Note: mcheck function is a prerequisite for the port must send BPDU packets, so only works on the specified port.

22.4.13 Configuring MSTP Instance Is Enabled

In order to flexibly control MSTP, you can open the DISABLE INSTANCE features, disable instance STP mode operating results with the implementation of no spanning-tree similar to the instance of the VLAN mapping of all connections on port forwarding state.

Table 160 Configuring MSTP instance is enabled

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Does not enable MSTP instance	<code>spanning-tree mst disable <i>instance instance-number</i></code>	Optional
Enable MSTP instances	<code>no spanning-tree mst disable <i>instance instance-number</i></code>	Optional

22.4.14 Displaying and Maintain MSTP

After completing the above configuration, you can use the following command to view configuration.

Table 161 Display and maintain MSTP

OPERATION	COMMAND	REMARKS
MSTP configuration information display identifier	<code>show spanning-tree mst config-id</code>	Performs either of the commands
Show all spanning tree instances and port configuration information	<code>show spanning-tree mst instance brief <i>id</i></code>	
Show spanning tree instance and port configuration information	<code>show spanning-tree mst instance [brief [ethernet interface-list]</code>	

Configuring SNTP

23.1 Brief introduction of SNTP

The Simple Network Time Protocol Version 4 (SNTPv4), which is a subset of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. In common, there is at least one server in the network, it provides reference time for clients, finally, all clients in the network synchronized local clocks.

23.1.1 SNTP Operation Mechanism

SNTPv4 can be worked in four modes: unicast, multicast, broadcast and anycast. In unicast mode, client actively sends a request to server, and server sends reply packet to client according to the local time structure after receiving requirement.

In broadcast and multicast modes, server sends broadcast and multicast packets to client periodically, and client receives packet from server passively.

In anycast mode, client actively sends request to local broadcast or multicast address, and all servers in the network will reply to the client. Client will choose the server whose reply packet is first received to be the server, and drops packets from others. After choosing the server, working mode is the same as that of the unicast.

In all modes, after receiving the reply packet, client resolves this packet to obtain current standard time, and calculates network transmit delay and local time complementary, and then adjusts current time according them.

23.2 Configuring SNTP Client

23.2.1 List of SNTP Client Configuration

Table 162 List of SNTP client configuration

CONFIGURING MSTP TASK		REMARK	DETAILED CONFIGURATION
SNTP Basic configuration	Enable SNTP client	required	23.2.2

Table 162 List of SNTP client configuration

CONFIGURING MSTP TASK		REMARK	DETAILED CONFIGURATION
SNTP advanced configuration	Modify SNTP client mode	optional	23.2.3
	Configure SNTP sever IP address	optional	23.2.4
	Modify broadcast transfer delay	optional	23.2.5
	Configure interval polling	optional	23.2.6
	Configure overtime retransmit	optional	23.2.7
	Configure client summer time	optional	23.2.8
	Configure valid sever list	optional	23.2.9
	Configure MD5 authentication	optional	23.2.10
Display and maintain SNTP client		optional	23.2.11

23.2.2 Enabling SNTP Client

Switch should only be configured SNTP client.

Table 163 startup SNTP client

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
Startup SNTP client	<code>sntp client</code>	required
Close SNTP client	<code>no sntp client</code>	optional

23.2.3 Modifying SNTP Client Operating Mode

Administrators can modify SNTP operating mode according to the network----- unicast, multicast, broadcast or anycast.

Table 164 modifying SNTP client operating mode

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
modifying SNTP client Operation mode	<code>sntp client mode {broadcast unicast multicast anycast [key key]}</code>	optional by default, SNTP client works in broadcast mode

23.2.4 Configuring SNTP Sever Address

SNTP client must configure appointed SNTP sever in the unicast way. You can also use below Commands to configure key when connecting to SNTP server by authentication.

Table 165 configure SNTP sever address

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
configure SNTP sever address	<code>sntp server ip_address</code>	required
configure SNTP backup sever	<code>sntp server backup IP</code>	optional

23.2.5 Modifying Broadcast Transfer Delay

When SNTP client works in the broadcast or multicast way, it needs to use broadcast transfer delay. In the broadcast way, the local time of SNTP client equals the time receiving from sever adds transferring time. Administrators can modify the transferring time according to the actual bandwidth in the network.

Table 166 configure broadcast transfer delay

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
configure broadcast transfer delay	<code>sntp client broadcastdelay time</code>	optional By default, transfer delay time is 3ms

23.2.6 Configuring Interval Polling

Configuring interval polling is necessary when SNTP client works in the unicast or anycast way. SNTP client adjusts the local system time by each interval polling requesting to sever.

Table 167 Configure interval polling

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
Configure interval polling	<code>sntp client poll-interval time</code>	optional By default, interval polling is 1000s

23.2.7 Configuring Overtime Retransmit

This Command is effective in unicast and anycast operating mode. SNTP request packet is UDP packet, overtime retransmission system is adopted because the requirement packet cannot be

guaranteed to send to the destination. Use below Commands to configure retransmit times and the interval.

Table 168 Configure overtime retransmit

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
configure overtime retransmit	<code>sntp client retransmit-interval time</code>	optional By default, retransmit-interval seconds is 5s
configure overtime retransmit times	<code>sntp client retransmit times</code>	optional By default 0, means do not retransmit
Enter global configuration mode	<code>configure terminal</code>	

23.2.8 Configuring Client Summer Time

Configuring summer time.

Table 169 Configure overtime retransmit

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
configure summer time	<code>sntp client summer-time daily {start-month start-day start-time end-month end-day end-time } sntp client summer-time weekly{ start-week Fri mon sat sun thu tue wed start- time end-month end-week Fri mon sat sun thu tue wed end- time}</code>	optional
Enter global configuration mode	<code>configure terminal</code>	

23.2.9 Configuring Valid Servers

In broadcast and multicast mode, SNTP client receives protocol packets from all servers without distinction. When there is malice attacking server (it will not provide correct time), local time cannot be the standard time. To solve this problem, a series of valid servers can be listed to filtrate source address of the packet.

Table 170 Configure valid server

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
configure valid servers	<code>sntp client valid-server IP mask</code>	optional

23.2.10 Configuring MD5 Authentication

To enhance the safety, MD5 authentication can be setup between SNTP sever and SNTP client which only receives the authenticated message. MD5 authentication configures as below:

Table 171 Configure MD5 authentication

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
Startup MD5 authentication	<code>sntp client authenticate</code>	optional
Configure authentication keys	<code>sntp client authentication-key <i>key-number</i> md5 <i>value</i></code>	optional
Configure authentication keys index	<code>sntp trusted-key <i>key-number</i></code>	optional

23.2.11 Displaying and Maintain SNTP Client

After finishing above configuration, you can use below Commands to show SNTP client configuration.

Table 172 Displaying and maintain SNTP client

OPERATION	COMMAND	REMARKS
Display configuration of SNTP client	<code>show sntp client</code>	Perform either of the Commands
Display summer time of SNTP client	<code>show sntp client summer-time</code>	Perform either of the Commands

SSH Terminal Services

24.1 Introduction to SSH

Secure Shell (SSH) can provide information security and powerful authentication to prevent such assaults as IP address spoofing, plain-text password interception when users log on to the Switch remotely through an insecure network environment.

SSH can take the place of the Telnet to provide safe management and configuration.

A Switch can connect to multiple SSH clients, and currently supports SSHv2.0 version.

The communication process between the server and client includes these five stages:

- 1 Version negotiation stage: These operations are completed at this stage:
 - The client sends TCP connection requirement to the server.
 - When TCP connection is established, both ends begin to negotiate the SSH version.
 - If they can work together in harmony, they enter the key algorithm negotiation stage. Otherwise the server clears the TCP connection.
- 2 Key algorithm negotiation stage. These operations are completed at this stage:
 - The server sends the public key in a randomly generated RSA key pair to the client.
 - The client figures out session key based on the public key from the server and the random number generated locally.
 - The client encrypts the random number with the public key from the server and sends the result back to the server.
 - The server then decrypts the received data with the server private key to get the client random number.
 - The server then uses the same algorithm to work out the session key based on server public key and the returned random number.

Then both ends get the same session key without data transfer over the network, while the key is used at both ends for encryption and decryption.
- 3 Authentication method negotiation stage: These operations are completed at this stage:
 - The client sends its username information to the server.
 - The server authenticates the username information from the client.
 - The client authenticates information from the user at the server till the authentication succeeds or the connection is turned off due to authentication timeout.
- 4 Session request stage: The client sends session request messages to the server which processes the request messages.
- 5 Interactive session stage: Both ends exchange data till the session ends.

24.2 SSH Server Configuration

A Switch, as a SSH server, can connect to multiple SSH clients. SSH clients can be both LAN users and WAN users.

The following table describes SSH server configuration tasks.

Table 173 Configure SSHv2.0 server

OPERATION	COMMAND	REMARKS
Enter globally configuration mode	<code>configure terminal</code>	-
Enable SSH	<code>[no] ssh</code>	Use this command in global configuration mode. By default, this function is disabled.
Configure the default key	<code>crypto key generate rsa</code>	Use this command in privileged mode.
Load SSH key	<code>crypto key refresh</code>	Use this command in privileged mode. This command will cover current key.
Clear configured key	<code>crypto key zeroize rsa</code>	Use this command in privileged mode.
Load/upload the key (public or private) through TFTP	<code>{load upload} keyfile {private public} TFTP inet A.B.C.D file_name</code>	Use this command in privileged mode.
Load/upload the key (public or private) through FTP	<code>{load upload} keyfile {private public} FTP inet A.B.C.D file_name Username Password</code>	Use this command in privileged mode.
Show SSH	<code>show ssh</code>	
Show SSH key	<code>show keyfile {public private}</code>	

24.3 Log in Switch from SSH Client

To successfully establish SSH connection, pay attention to following points:

- 1 Create the connection between SSH client and server.
- 2 The version of client and server should be the same.
- 3 The key matched.
- 4 SSH function in server should be enabled.

By default, there is a pair of keys saved in switch. The loaded key can also be used. Pay attention to followings:

- 1 The configured keyfile must be RSA. The keyfile includes public key and private key. It can be default key or loaded keyfile through ftp/tftp. No keyfile is configured in initiation. The default key can be used only after generating by command. The configured key is saved in Flash and can only be used after loading when rebooting.
- 2 User cannot log in device through SSH client if the configured key is not RSA key or the public and private key are not matched.
- 3 There can be comment line and key content in the keyfile. Comment line should contain ":" or space. Key content contain the key encoded by Base64 coding, without ":" and space. Public key cannot be in private keyfile and private keyfile cannot be encrypted by password.

24.4 SSH Server Configuration Example

24.4.1 Use Default Key

Network requirements

As shown in [Figure 46 on page 195](#), the PC (SSH Client) runs the client software which supports SSHv2.0, establish a local connection with the switch (SSH Server) and ensure the security of data exchange.

Network diagram

Figure 46 Network diagram for SSH server configuration



Configuration procedure

- 1 Enable SSH

```
Switch(config)#ssh
Config SSH state successfully.
Switch(config)#
```
- 2 Display SSH configuration to ensure the keyfile can be used.

```
Switch(config)#show ssh
ssh version   : 2.0
ssh state     : on
ssh key file  : available
```
- 3 Open SSH client in PC and log in switch

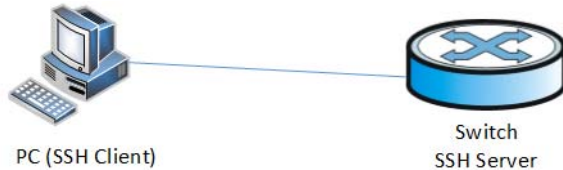
24.4.2 Use Loaded Key

Network requirements

As shown in [Figure 47 on page 196](#), the PC (SSH Client) runs the client software which supports SSHv2.0, establish a local connection with the switch (SSH Server) and ensure the security of data exchange.

Network diagram

Figure 47 Network diagram for SSH server configuration



Configuration procedure

- 1 Use key generated tool to generate a pair of RSA key as [Figure 48 on page 196](#).

Figure 48 Example of correct private key form

```

PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20090624
Private-Lines: 8
AAAAGtIs5qVyP9TEpW+HfiYWRfaKCrhH2EYsQke/r21hJz7BTwzmG8Y/gatMTBw
mMjtn1eAI9MQk5SiPkJEkt6jucJBAL1dpQn50Xw+2TDZ+LEKEMEXGK8CfM6nXPZQ
a3Fmx6RjgHuI9Ey09bD9HvKZDnh9pSuoi8pL1XniFFVV0SSJAAAAQQD1WXgoFLCM
uDsHA/Ysls6ngRzAYjCvPyt8PVpjuz7CETO4Ii5Zxo/jhey6qtEmSvdfYo+dxSzx
BEodj+rrnWGHAAAAQQC12QrR5h2vY/cM1DDxhTFjPkNiuXrCGdYEYpPbws5jxJTl
wtYpyW5yisImMxc5WpVVNGNukww2iNbuzQxO8XtzAAAAQBAM4z8kTff8SMpc60vL
q9rjapCTrfPU9QN0I00LiILO3ju2E0dgrK1qF00QA1o2AMcfA+Hp1HBHY424fTRx
FJ0=
Private-MAC: 37b49b5d489ff022fa3de91b2330fd89a74eaeff
  
```

- 2 Load key

```

Switch#load keyfile private tftp 1.1.1.1 private.ppk
SSH key file will be updated, are you sure(y/n)? [n]y
Loading SSH key file via TFTP...
Load SSH key file via TFTP successfully.
Switch#load keyfile public tftp 1.1.1.1 public.pub
SSH key file will be updated, are you sure(y/n)? [n]y

Loading SSH key file via TFTP...
Load SSH key file via TFTP successfully.
  
```

- 3 Enable SSH

```

Switch(config)#ssh
Config SSH state successfully.
  
```

- 4 Display SSH configuration to ensure the keyfile can be used.

```
Switch(config)#show ssh
ssh version   : 2.0
ssh state     : on
ssh key file  : available
```

- 5 Ensure current key is the loaded key (if it is not the loaded key, use cry key refresh to refresh it)

```
Switch#show key private
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20090624
Private-Lines: 8
AAAAGtIs5qVyP9TEpW+HfiYWRfaKCrhH2EYsQke/r2lhjz7BTwzmG8Y/gatMTBw
mMjtn1eAI9MQk5siPkJEkt6jucJBAL1dpQn50Xw+ZTDZ+LEKEMEXGK8CfM6nXPZQ
a3Fmx6RjgHuI9Ey09bD9HvKZDnh9pSuoi8pL1XniFFVV0SSJAAAAQQD1WXgoFLCM
uDsHA/Ysls6nqRzAYjCvPyt8PVpjuz7CETO4Ii5Zxo/jhey6qtEmSvdfYo+dxSzx
BEodj+rrnWGHAQAQQCl2QrR5hZvY/cM1DDxhTFjPkNiuXrCGdYEPpBws5jxJTl
wtYpyW5yisImMxc5WpVVNGNukww2iNbuzQxO8XtzAAAAQBAM4z8kTff8SMpc60vL
q9rjapCTrfPU9QN0I00LiILO3ju2E0dgrK1qF00QA1o2AMcfA+Hp1HBHY424fTRx
FJ0=
Private-MAC: 37b49b5d489ff022fa3de91b2330fd89a74eaeff

Switch#show key public
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "rsa-key-20090624"
AAAAB3NzaC1yc2EAAAABJQAAAIEAnvKtpIiP4Ee/WH/F9QpvYL3AkWGpUkNDc+Yx
VjWdtm1FMCNpIJWg6ylIzM+acQ3C3akqx7xfk62PV9YhDBEIsHZIFh4seZbNHSiC
ZS2B0txcVPNe6+WtUrhSExzp3fEmNsrB5E5BPKmQyU0+6QS691oQhZUnHN93J1r1
8GelrKU=
----- END SSH2 PUBLIC KEY -----
```

- 6 Open SSH client in PC and log in switch.

Configuration File Management

25.1 Introduction to Configuration File

Configuration file records and stores user configurations performed to a switch. It also enables users to check switch configurations easily.

Upon powered on, the switch loads the saved-configuration file, which resides in the Flash, for initialization. If the Flash contains no configuration file, the system initializes using the default settings. Comparing to saved-configuration file, the configuration file which is currently adopted by a switch is known as the current-configuration.

A configuration file conforms to the following conventions:

The content of a configuration files is a series of commands.

Only the non-default configuration parameters are saved.

The commands are grouped into sections by command configuration mode. The commands at the same configuration mode are grouped into one section. Sections are separated by empty lines or comment lines. (A line is a comment line if it starts with the character ";".)

The sections are listed in this order: system configuration section, physical port configuration section, logical interface configuration section, routing protocol configuration section, and so on.

A configuration file ends with an "exit".

25.2 Configuration File-Related Operations

You can perform the following operations on an S3100 series switch:

Modify uploaded configuration file. The configuration file is in the form of text, which can be uploaded to the PC through FTP and TFTP. Please use text tools (such as windows notepad) to edit the uploaded configuration file.

Modify and save the current configuration to a configuration file.

Removing a configuration file from the Flash;

Execute saved configuration file;

Checking/Setting the configuration file to be used when the switch starts the next time;

Setting a configuration file to be the primary configuration file;

Change the executing mode of configuration file.

Perform the following configuration in privileged configuration mode.

Table 174 Configure a configuration file

OPERATION	COMMAND	REMARKS
Save current operation	<code>copy running-config startup-config</code>	The saved configuration will be the start-up configuration of the next rebooting.
Clear saved configurations	<code>clear startup-config</code>	If the saved configuration is cleared, the system will restore to factory setting after rebooting.
Execute saved configuration	<code>copy startup-config running-config</code>	Configuration file is executed in global configuration mode by default. Enter global configuration mode first by using <code>configure terminal</code> in privilege mode. Prompts for not executable command during execution: [Line:xxxx]invalid: %s—Cannot execute. [Line:xxxx]failed: %s—Execution failed. [Line:xxxx]failed: too long command: %s—Not execute command which is beyond 512 characters. "xxxx" means the line number of the command. "%s" means command characters. Not executable command includes commands with grammar error and unmatched mode.
Show saved configuration	<code>show startup-config [module-list]</code>	
Show current configuration	<code>show running-config [module-list]</code>	
Execute mode of configuration files	<code>buildrun mode {stop continue}</code>	Stop means configuration file executing would be stopped and the error will show if there is an error. Continue means configuration file executing would not be stopped and the error will show if there is an error.

Note: Currently, the extension of a configuration file is bin. Configuration files are saved in the root directory of the Flash.

In the following conditions, it may be necessary for you to remove the configuration files from the Flash:

The system software does not match the configuration file after the software of the Ethernet switch is updated.

The configuration files in the Flash are damaged. The common reason is that wrong configuration files are loaded.

BootROM and Host Software Loading

Traditionally, the loading of switch software is accomplished through a serial port. This approach is slow, inconvenient, and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can upload/download software/files conveniently to the switch through an Ethernet port.

This chapter introduces how to load BootROM and host software to a switch locally and how to do this remotely.

26.1 Introduction to Loading Approaches

You can load software locally by using:

XMODEM through Console port

TFTP through Ethernet port

FTP through Ethernet port

You can load software remotely by using:

FTP

TFTP

Note: The BootROM software version should be compatible with the host software version when you load the BootROM and host software.

26.2 Local Software Loading

If your terminal is directly connected to the switch, you can load the BootROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch to insure successful loading.

Note: The loading process of the BootROM software is the same as that of the host software, except that during the former process, the system gives different prompts. The following text mainly describes the BootROM loading process.

26.2.1 Loading Software Using XMODEM through Console Port

Introduction to XMODEM

XMODEM is a file transfer protocol that is widely used due to its simplicity and good performance. XMODEM transfers files via console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and multiple attempts of error packet retransmission (generally the maximum number of retransmission attempts is ten).

The XMODEM transmission procedure is completed by a receiving program and a sending program: The receiving program sends negotiation characters to negotiate a packet checking method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends an acknowledgement character and the sending program proceeds to send another packet; otherwise, the receiving program sends a negative acknowledgement character and the sending program retransmits the packet.

Loading BootROM software

The following text mainly describes the BootROM loading process. Follow these steps to load the BootROM software:

- 1 enter following command in privileged mode:

```
Switch#load whole-bootrom xmodem
Downloading BootRom via Xmodem...
XMODEM Receive: Waiting for Sender ...
```

- 2 Choose [Transfer/Send File] in the HyperTerminal's window, as shown in [Figure 49 on page 201](#), and click <Browse> in pop-up dialog box. Select the software you need to download, and set the protocol to XMODEM, as shown in [Figure 50 on page 202](#).

Figure 49 Choose [Transfer/Send File]

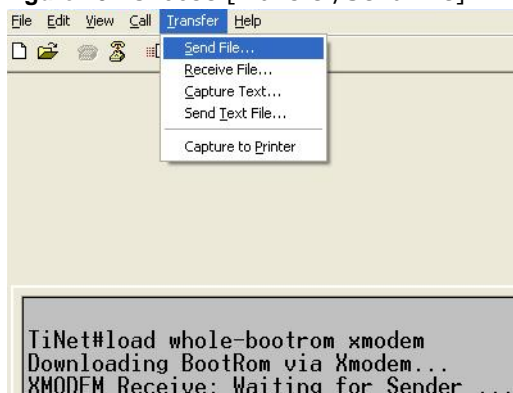
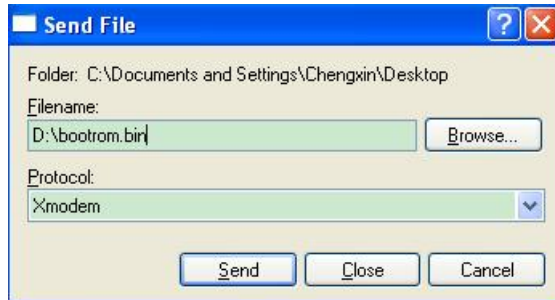
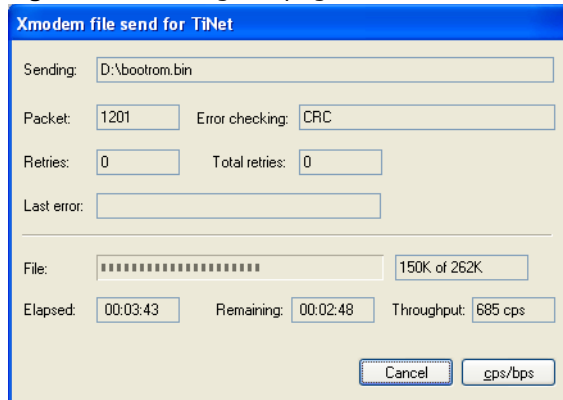


Figure 50 Send file dialog box

- 3 Click <Send>. The system displays the page, as shown in [Figure 51 on page 202](#).

Figure 51 Sending file page

- 4 After the download completes, the system displays the following information:
Download wholeBootRom successfully.
Update BootRom successfully.
Download BootRom via Xmodem successfully.

Loading host software

Follow these steps to load the host software:

- 1 Enter following command in privileged mode:

```
Switch#load application xmodem
Downloading application via Xmodem...
XMODEM Receive: Waiting for Sender ...
```

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

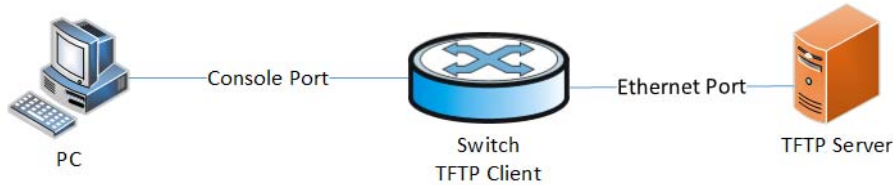
26.2.2 Loading Software Using TFTP through Ethernet Port

Introduction to TFTP

TFTP, one protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It uses UDP to provide unreliable data stream transfer service.

Loading BootROM software

Figure 52 Local loading using TFTP



- 1 As shown in [Figure 52 on page 203](#), connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.

Note: You can use one PC as both the configuration device and the TFTP server.

- 2 Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

TFTP server program is not provided with the Switch Series Ethernet Switches.

- 3 Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the privileged mode. Then set the following TFTP-related parameters as required:

```
Switch#load whole-bootrom tftp tftpserver-ip filename
```

Load File name: bootrom.bin

Switch IP address: A.B.C.D

Server IP address: A.B.C.E

- 4 Press <Enter>. The system displays the following information:
Are you sure to update your bootrom?Yes or No(Y/N)
- 5 Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM software. Upon completion, the system displays the following information:

```
Download wholeBootRom successfully.
Update BootRom successfully.
Download BootRom via TFTP successfully.
```

Loading host software

The subsequent steps are the same as those for loading the BootROM program, except that the system gives the prompt for host software loading instead of BootROM loading.

When loading BootROM and host software using TFTP, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.

26.2.3 Loading Software Using FTP through Ethernet Port

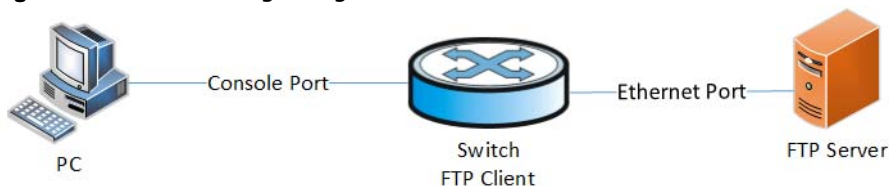
Introduction to FTP

FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

Loading BootROM software

Figure 53 Local loading using FTP client



- 1 As shown in [Figure 53 on page 204](#), connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.

Note: You can use one computer as both configuration device and FTP server.

- 2 Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.
- 3 Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the privileged mode. Then set the following FTP-related parameters as required:

```
Switch#load whole-bootrom ftp ftpserver-ip filename
```

Load File name: bootrom.bin

Switch IP address: A.B.C.D

Server IP address: A.B.C.E

- 4 Press <Enter>. The system displays the following information:
Are you sure to update your bootrom?Yes or No(Y/N)
- 5 Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM software. Upon completion, the system displays the following information:
Download wholeBootRom successfully.
Update BootRom successfully.
Download BootRom via FTP successfully.

Loading host software

The subsequent steps are the same as those for loading the BootROM program, except that the system gives the prompt for host software loading instead of BootROM loading.

When loading BootROM and host software using FTP, you are recommended to use the PC directly connected to the device as FTP server to promote upgrading reliability.

26.3 Remote Software Loading

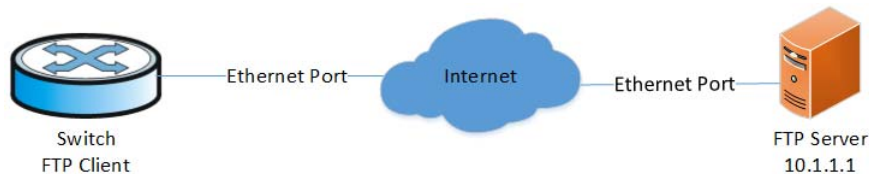
If your terminal is not directly connected to the switch, you can telnet to the switch, by use FTP or TFTP to load BootROM and host software remotely.

26.3.1 Remote Loading Using FTP

Loading BootROM

As shown in [Figure 54 on page 205](#), a PC is used as both the configuration device and the FTP server. You can telnet to the switch and then execute the FTP commands to download the BootROM program bootrom.bin from the remote FTP server (with an IP address 10.1.1.1) to the switch.

Figure 54 Remote loading using FTP



- 1 Open FTP software and set host IP address to be 10.1.1.1. Set the username and password;

Note: When using different FTP server software on PC, different information will be output to the switch.

The subsequent steps are the same as those for [Section 26.2.3 on page 204](#). Make sure the PC can ping the switch.

26.3.2 Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP.

Basic System Configuration & Debugging

This section includes:

- [Basic System Configuration](#)
- [Displaying SNMP](#)
- [SNMP Configuration Example](#)
- [Network Connectivity Test](#)
- [Device Management](#)
- [System Maintenance](#)

27.1 Basic System Configuration

Perform following commands in global privilege mode.

Table 175 Basic system configuration tasks

OPERATION	COMMAND	REMARKS
Configure the host name of the device.	<code>hostname <i>hostname</i></code>	By default, the hostname is Switch.
Configure system clock	<code>clock set HH:MM:SS YYYY/MM/DD</code>	By default, it is 00:00:00 01/01/2000 when the system starts up.
Configure system time zone	<code>clock timezone name hour minute</code>	By default, it is the UTC time zone.

27.2 SNMP

27.2.1 SNMP Overview

By far, the simple network management protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the connectionless transport layer protocol UDP; and is thus widely supported by many products.

SNMP Operation Mechanism

SNMP can be divided into two parts, namely, Network Management Station and Agent: Network management station (NMS) is the workstation for running the client program. At present, the commonly used NM platforms include QuidView, Sun NetManager and IBM NetView.

Agent is the server software operated on network devices.

The NMS can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the NMS, Agent will perform Read or Write operation according to the message types, generate and return the Response message to the NMS.

Agent will send Trap message on its own initiative to the NMS to report the events whenever the device status changes or the device encounters any abnormalities such as restarting the device.

SNMP Versions

Currently SNMP Agent of the device supports SNMP V3, and is compatible with SNMP V1 and SNMP V2C.

SNMP V3 adopts user name and password authentication.

SNMP V1 and SNMP V2C adopt community name authentication. The SNMP packets failing to pass community name authentication are discarded. The community name is used to define the relation between SNMP NMS and SNMP Agent. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password.

You can define the following features related to the community name.

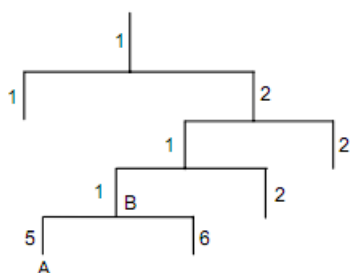
Define MIB view that a community can access.

Set read-only or read-write right to access MIB objects for the community. The read-only community can only query device information, while the read-write community can configure the device.

Set the basic ACL specified by the community name.

MIBs Supported by the Device

The management variable in the SNMP packet is used to describe management objects of a device. To uniquely identify the management objects of the device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree, and each tree node represents a managed object, as shown in [Figure 55 on page 208](#). Thus the object can be identified with the unique path starting from the root.

Figure 55 Architecture of the MIB tree

The management information base (MIB) is used to describe the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

27.2.2 Configuring SNMP Basic Functions

Perform following commands in global configuration mode.

Table 176 Configuring SNMP Basic Functions

OPERATION	COMMAND	REMARKS
Configure community name and some other info	<code>snmp-server community community { ro rw } { deny permit } [view view-name]</code>	
Configure system administrator's contact	<code>snmp-server contact syscontact</code>	If there is space in the <i>syscontact</i> keywords, it should be quoted by quotation mark.
Enable destination host address	<code>snmp-server host host-addr [version { 1 2c 3 [auth noauthpriv priv] }] community-string [udp-port port] [notify-type [notifytype-list]]</code>	The community name in <i>snmp-server host version</i> should not be empty.
Configure system location	<code>snmp-server location syslocation</code>	By default, the <i>syslocation</i> is "sample sysLocation factory default" If there is space in the keywords, it should be quoted by quotation mark.
Configure system name	<code>snmp-server name sysname</code>	By default, the <i>sysname</i> is "Switch " If there is space in the keywords, it should be quoted by quotation mark.
Enable SNMP server to send notification	<code>snmp-server enable traps [notificationtype-list]</code>	The default notification type is trap, and it is defaulted to be disabled.
Configure local engine id or remote engine id.	<code>snmp-server engineid { local engineid-string remote ip-address [udp-port port-number] engineid-string }</code>	By default, the device local engine ID is 134640000000000000000000. The local engine cannot be deleted and at most 32 remote engines can be configured.

Table 176 Configuring SNMP Basic Functions

OPERATION	COMMAND	REMARKS
Configure view	<code>snmp-server view view-name oid-tree { included excluded }</code>	There are three default views: iso, internet and sysview. At most 64 views can be configured. The character number of the view-name plus the number of OID nodes is not more than 62.
Configure access control group	<code>snmp-server group groupname { 3 [auth noauthpriv priv] [context context-name] [read readview] [write writeview] [notify notifyview]</code>	There are two defaulted groups: 1. security model is v3 and security level is initial 2. security model is v3 initial At most 64 groups can be configured.
Configure user in snmpv3	<code>snmp-server user username groupname [remote host [udp-port port]] [auth { md5 sha } { authpassword { encrypt-authpassword authpassword authpassword } authkey { encrypt-authkey authkey authkey } } [priv des { privpassword { encrypt-privpassword privpassword privpassword } privkey { encrypt-privkey privkey privkey } }]</code>	There are three default users: 1. initialmd5 (HMACMD5AuthProtocol), 2. initialsha (HMACSHAAuthProtocol), 3. initialnone (NoauthProtocol) At most 64 users can be configured.
Enter global configuration mode	<code>configure terminal</code>	

27.2.3 Displaying SNMP

After the above configuration is completed, execute the display command in any mode to view the running status of SNMP, and to verify the configuration.

Table 177 Display SNMP

OPERATION	COMMAND	REMARKS
Display the currently configured community name	<code>show snmp community</code>	
Display system administrator's contact	<code>show snmp contact</code>	
Display Trap list information	<code>show snmp host</code>	
Display all notification status	<code>show snmp notify</code>	
Display system location	<code>show snmp location</code>	
Display the engine ID of the current device	<code>show snmp engineid [local remote]</code>	<i>local</i> means to show local engine and <i>remote</i> means to show recognizable remote engine.
Display group information about the device	<code>show snmp group</code>	

Table 177 Display SNMP

OPERATION	COMMAND	REMARKS
Display SNMP user information	<code>show snmp user</code>	
Display the currently configured view	<code>show snmp view</code>	

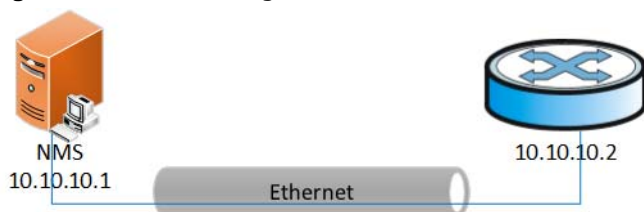
27.2.4 SNMP Configuration Example

Network requirements

An NMS and Switch A are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.

Perform the following configuration on Switch A: setting the community name and access authority, administrator ID, contact and switch location, and enabling the switch to send trap packet.

Network diagram

Figure 56 Network diagram for SNMP

Network procedure

! Set the community name, group name and user.

```

Switch(config)# snmp-server community XXXX ro permit
Switch(config)# snmp-server group grp1 1 read internet write internet notify
Internet
Switch(config)# snmp-server user user1 grp1
  
```

! Enable the SNMP agent to send Trap packets to the NMS whose IP address is 10.10.10.1. The SNMP community is XXXX.

```

Switch(config)#snmp-server host 1.1.1.2 version 3 auth 1 notify-type interfaces
  
```

27.3 Network Connectivity Test

27.3.1 Ping

You can use the ping command to check the network connectivity and the reachability of a host.

Table 178 The ping command

OPERATION	COMMAND
Enter global configuration mode	<code>configure terminal</code>
Check the IP network connectivity and the reachability of a host	<code>ping [-i ttl] [-l packetlength] [-n packetnumber] [-s sourceip] [-t timeout] ip_address</code>

This command can output the following results:

Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.

Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

27.3.2 Tracert

You can use the `tracert` command to trace the gateways a packet passes during its journey from the source to the destination. This command is mainly used to check the network connectivity. It can help you locate the trouble spot of the network.

The executing procedure of the `tracert` command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

Table 179 The tracert command

OPERATION	COMMAND
Trace the gateways a packet passes from the source host to the destination	<code>tracert [-u -c] -f first_ttl -h maximum_hops -w time_out] target_name</code>

27.4 Device Management

The device management function of the Ethernet switch can report the current status and event-debugging information of the boards to you. Through this function, you can maintain and manage your physical device, and restart the system when some functions of the system are abnormal.

27.4.1 Device Management Configuration

Table 180 Device management configuration tasks

OPERATION	DESCRIPTION	RELATED SECTION
MAC address Table management		
Reboot switch		

27.4.2 MAC address Table management

Overview

1 Introduction to MAC Address Learning

An Ethernet switch maintains a MAC address table to forward packets quickly. A MAC address table is a port-based Layer 2 address table. It is the base for Ethernet switch to perform Layer 2 packet forwarding. Each entry in a MAC address table contains the following fields:

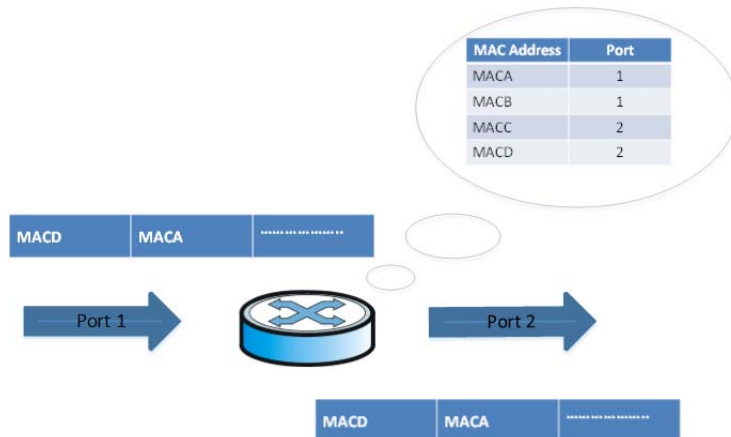
- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding port number

Upon receiving a packet, a switch queries its MAC address table for the forwarding port number according to the destination MAC address carried in the packet and then forwards the packet through the port.

The dynamic address entries (not configured manually) in the MAC address table are learned by the Ethernet switch. When an Ethernet switch learns a MAC address, the following occurs:

When a switch receives a packet from one of its ports (referred to as Port 1), the switch extracts the source MAC address (referred to as MAC-SOURCE) of the packet and considers that the packets destined for MAC-SOURCE can be forwarded through Port 1.

- If the MAC address table already contains MAC-SOURCE, the switch updates the corresponding MAC address entry.
- If MAC-SOURCE does not exist in the MAC address table, the switch adds MAC-SOURCE and Port 1 as a new MAC address entry to the MAC address table.

Figure 57 A switch uses a MAC address table to forward packets

After learning the source address of the packet, the switch searches the MAC address table for the destination MAC address of the received packet:

- If it finds a match, it directly forwards the packet.
- If it finds no match, it forwards the packet to all ports, except the receiving port, within the VLAN to which the receiving port belongs. Normally, this is referred to as broadcasting the packet.

After the packet is broadcast:

- If the network device returns a packet to the switch, this indicates the packet has been sent to the destination device. The MAC address of the device is carried in the packet. The switch adds the new MAC address to the MAC address table through address learning. After that, the switch can directly forward other packets destined for the same network device by using the newly added MAC address entry.
- If the destination device does not respond to the packet, this indicates that the destination device is unreachable or that the destination device receives the packet but gives no response. In this case, the switch still cannot learn the MAC address of the destination device. Therefore, the switch will still broadcast any other packet with this destination MAC address.

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. Aging time only applies to dynamic MAC address entries.

You can manually configure (add or modify) a static or dynamic MAC address entry based on the actual network environment.

Note: The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

2 Entries in a MAC Address Table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- **Static MAC address entry:** This type of MAC address entries are added/removed manually and cannot age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change, but it will be lost after reboot if the configuration is saved.

- **Dynamic MAC address entry:** This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- **Blackhole MAC address entry:** This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries

Permanent MAC address entry: This type of MAC address entries own the same features as the static MAC address entries, but it will be reserved at reboot if the configuration is saved.

Table 181 lists the different types of MAC address entries and their characteristics.

MAC ADDRESS ENTRY	CONFIGURATION METHOD	AGING TIME	RESERVED OR NOT AT REBOOT (IF THE CONFIGURATION IS SAVED)
Static MAC address entry	Manually configured	Unavailable	No
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Reserved
Permanent MAC address entry	Manually configured	Unavailable	Reserved

Configuring MAC Address Table Management

1 Configuring a MAC Address Entry

You can add, modify, or remove one MAC address entry, remove all MAC address entries (unicast MAC addresses only) concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

You can add a MAC address entry in global configuration mode or interface configuration mode.

Perform following commands in global configuration mode.

Table 182 Add a MAC address entry

OPERATION	COMMAND	REMARKS
Enter interface configuration mode	<code>interface {interface_type interface_num interface_name }</code>	Option
Add a MAC address entry	<code>mac-address-table { static permanent dynamic } mac interface interface-num vlan vlan-id</code>	This command for adding static/permanent/dynamic mac address entry.
	<code>mac-address-table blackhole mac vlan vlan-id</code>	This command is only for adding blackhole mac address entry.

When you add a MAC address entry, the port specified by the interface argument must belong to the VLAN specified by the vlan argument in the command. Otherwise, the entry will not be added.

2 Setting the Aging Time of MAC Address Entries

Setting aging time properly helps implement effective MAC address aging. The aging time that is too long or too short results in a large amount of broadcast packets wandering across the network and decreases the performance of the switch.

- If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from varying with network changes in time.

If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Table 183 Set aging time of MAC address entries

OPERATION	COMMAND	DESCRIPTION
Set the aging time of MAC address entries	<code>mac-address-table age-time [agetime disable]</code>	The default aging time is 300 seconds.

This command is used in global configuration mode and applies to all ports. Aging applies to only dynamic MAC addresses that are learnt or configured to age.

Normally, you are recommended to use the default aging time, namely, 300 seconds. The no-aging keyword specifies that MAC address entries do not age out.

3 Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. The switch directly forwards the packets destined for these MAC addresses. A MAC address table too big in size may decrease the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, you can control the number of the MAC address entries the MAC address table can dynamically maintains. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Perform following commands in interface configuration mode.

Table 184 Set the maximum number of MAC addresses a port can learn

OPERATION	COMMAND	DESCRIPTION
Enable MAC addresses table learning	<code>mac-address-table learning</code>	This command can be used in both global configuration mode and interface configuration mode. By default, this function is enabled.
Set the maximum number of MAC addresses the port can learn	<code>mac-address-table max-mac-count max-mac-count</code>	By default, the number of the MAC addresses a port can learn is not limited.

Displaying and Maintaining MAC Address Table Configuration

To verify your configuration, you can display information about the MAC address table by executing the display command in any mode.

Table 185 Display and maintain MAC address table configuration

OPERATION	COMMAND
Display information about the MAC address table	<pre>show mac-address-table show mac-address-table { interface-num [vlan vlan-id] cpu } show mac-address-table mac [vlan vlan-id] show mac-address-table { static dynamic permanent blackhole } [vlan vlan-id] show mac-address-table { static dynamic permanent blackhole } interface interface-num [vlan vlan-id] show mac-address-table vlan vlan-id</pre>
Display the aging time of the dynamic MAC address entries in the MAC address table	<pre>show mac-address-table age-time</pre>
Display MAC addresses table learning status	<pre>show mac-address-table learning</pre>

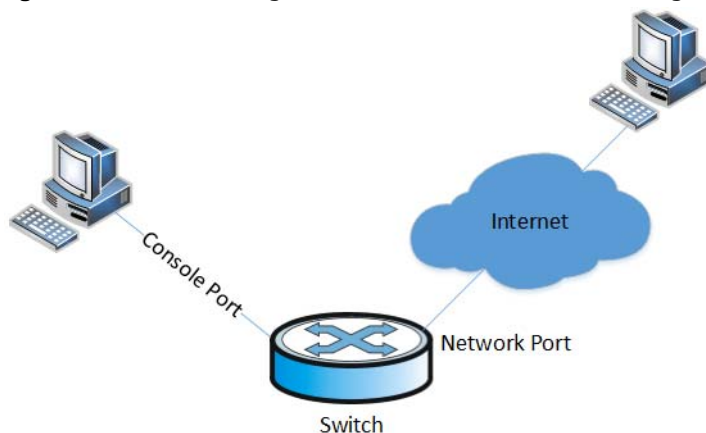
Configuration Example

1 Network requirements

- Log in to the switch through the Console port and enable address table configuration.
- Set the aging time of dynamic MAC address entries to 500 seconds.
- Add a static MAC address entry 00:01:fc:00:0c:01 for GigabitEthernet0/0/2 port (assuming that the port belongs to VLAN 1)

2 Network diagram

Figure 58 Network diagram for MAC address table configuration



3 Configuration procedure

! Add a MAC address, with the VLAN, ports, and states specified.

```
Switch(config)#mac-address-table static 00:01:fc:00:0c:01 interface ethernet 0/0/2
vlan 1
Add ARL table entry successfully.
```

! Set the aging time of dynamic MAC addresses to 500 seconds.

```
Switch(config)#mac-address-table age-time 500
Config MAC address table aging time successfully !
```

! Display the information about the MAC address entries in global configuration mode.

```
Switch(config)#show mac-address-table interface ethernet 0/0/2
MAC Address          VLAN ID  port      status
00:01:fc:00:0c:01    1        0/0/2     static
Total entries: 1 .
```

27.4.3 Restarting the Ethernet Switch

You can perform the following operation in privileged mode when the switch is in trouble or needs to be restarted.

Table 186 Restart the Ethernet switch

OPERATION	COMMAND	DESCRIPTION
Restart the Ethernet switch	reboot	

Note: When rebooting, the system checks whether there is any configuration change. If there is, it prompts you to indicate whether or not to proceed. This prevents you from losing your original configuration due to oblivion after system reboot.

27.5 System Maintenance

27.5.1 Basic Maintenance

Perform following commands in global configuration mode:

Table 187 Basic Maintenance

OPERATION	COMMAND	REMARKS
Configure whether to transmit destination-unknown packet	dlf-forward { multicast unicast }	By default, destination-unknown unicast and multicast packets will be transferred. This command can be used in both global configuration mode and interface configuration mode.
Configure whether to transmit BPDU packet	discard-bpdu	By default, all BPDU packets will be transferred.

Table 187 Basic Maintenance

OPERATION	COMMAND	REMARKS
Enable loopback test	<code>loopback { internal external }</code>	This command can be used in both global configuration mode and interface configuration mode. Insert outer loop wire before external loopback test.
Vct test for combo port.	<code>vct { auto-run run }</code>	This command can only be used in interface configuration mode. This command is only for combo port.
Configure cpu rate for receiving packet	<code>cpu-car target_rate</code>	

27.5.2 Access-limit Management

A switch provides ways to control different types of login users, as Telnet, SNMP and WEB. Here is by IP address. Perform following commands in global configuration mode:

Table 188 Access-limit Management

OPERATION	COMMAND	REMARKS
Configure the permitted IP address for managing switch through web, snmp and telnet	<code>login-access-list { web snmp telnet } ip-address wildcard</code>	Delete IP address 0.0.0.0 255.255.255.255 first.
Display all permitted IP address for managing switch through web, snmp and telnet	<code>show login-access-list</code>	

27.5.3 Telnet Client

After logging in the switch, the Telnet client can be enabled to log in other switch or Telnet server.

Perform following commands in global configuration mode.

Table 189 Telnet Client

OPERATION	COMMAND	REMARKS
Enable telnet client	<code>telnet ip-addr [port-num] [/localecho]</code>	By default, <i>port-num</i> is 23 and local echo is disabled.
Configure the number of user permitted by telnet	<code>login-access-list telnet-limit limit-no</code>	By default, the number of max permitted user is 5.
Force telnet client to stop	<code>stop telnet client { all term-id }</code>	Only the super admin "administrator" can use this command.
Display telnet client	<code>show telnet client</code>	

27.5.4 CPU-alarm

System can monitor CPU utilization. If it is beyond cpu busy threshold, system will send CPU busy alarm. If CPU utilization is under cpu unbusy threshold, system will send CPU busy alarm.

Perform following commands in global configuration mode:

Table 190 CPU-alarm

OPERATION	COMMAND	REMARKS
Enable/disable cpu alarm	<code>alarm cpu</code>	By default, this function is enabled.
Configure CPU busy/unbusy threshold	<code>alarm cpu threshold [busy busy] [unbusy unbusy]</code>	By default, CPU busy threshold is 90 and unbusy threshold is 60. Busy threshold must larger than unbusy threshold.
Display cpu alarm info	<code>show alarm cpu</code>	

27.5.5 Mail-alarm

Perform following commands in global configuration mode:

Table 191 Mail-alarm

OPERATION	COMMAND	REMARKS
Enable mail alarm	<code>mailalarm</code>	By default, this function is disabled.
Configure smtp server	<code>mailalarm server server-addr</code>	By default, the smtp server is 0.
Configure the email address of the mail receiver	<code>mailalarm receiver receiver-addr</code>	By default, the email address of the mail receiver is empty.
Configure Carbon copy receiver	<code>mailalarm ccaddr cc-addr</code>	By default, the Carbon copy receiver is empty. At most 4 Carbon copy receivers can be configured.
Enable smtp authentication and configure the username and password	<code>mailalarm smtp authentication username username { passwd passwd encrypt-passwd encrypt-passwd }</code>	By default, this function is disabled. The keyword "encrypt- password" can only be used in the command generated by de-compilation
Configure the syslog level for sending mail alarm	<code>mailalarm logging level level</code>	By default, the syslog level is 0. The syslog whose level is lower than configured will be sent by email.
Display mail alarm info	<code>show mailalarm</code>	

27.5.6 Anti-Dos Attack

The IP fragment packet number the system can receive does not occupy the all received packet resources, so it can normally deal with non-fragment packets if there is IP fragment attack.

Perform following commands in global configuration mode:

Table 192 Anti-Dos Attack

OPERATION	COMMAND	REMARKS
Configure the max number of IP fragment packet the system can receive	<code>anti-dos ip fragment maxnum</code>	By default, the number is 800.
Display anti-dos info	<code>show anti-dos</code>	

27.5.7 Displaying System Status

You can use the following show commands to check the status and configuration information about the system. For information about protocols and ports, and the associated display commands, refer to relevant sections.

Perform following commands in any mode:

Table 193 System display commands

OPERATION	COMMAND
Display version info	<code>show version</code>
Display	<code>show username</code>
Display the administrator logged in switch	<code>show users</code>
Display system info	<code>show system</code>
Display memory info	<code>show memory</code>
Display system clock	<code>show clock</code>
Display cpu utilization	<code>show cpu-utilization</code>
Display cpu-car value	<code>show cpu-car</code>
Display packet statistics sent to cpu	<code>show cpu-statistics</code>
Clear packet statistics sent to cpu	<code>clear cpu-statistics</code>
Display L3 table of all L3 interfaces or of specific IP	<code>show ip fdb [ip <i>ip-address</i> [mask]]</code>
Display dhcp-server client info	<code>show dhcp-server clients [ip [mask] mac <i>poolname</i>]</code>

LLDP Configuration

28.1 LLDP Protocol Overview

LLDP (Link Layer Discovery Protocol), a L2 protocol, defined by IEEE802.1AB-2005 standard has nothing to do with the manufacturer. It announces its information to other neighbor devices in the network, receives the neighbor's information and saves to standard MIB of LLDP for users to check the downlink devices and connected ports for easy network maintenance and management. Network administrator can know L2 connections by accessing.

1 LLDP Fundamentals

LLDP devices announce their own information through multicast address 01-80-c2-00-00-0e. LLDP devices will send 2 LLDP notice and the sending interval is set by hello-time. After receiving neighbor's advertisement, LLDP device will read the advertisement content and save in LLDP neighbor table. LLDP neighbor table can be aged with TTL value being aging time. If neighbor's LLDP advertisement cannot be received within aging time, the neighbor entry will be removed.

2 LLDP timer

Hello-time: The time interval for sending LLDP packet.

Hold-time: LLDP aging time granularity for neighbor entry.

TTL: TTL equals to hello-time ties hold-time which means aging time of neighbor entry.

28.2 Configure LLDP

28.2.1 LLDP Configuration Task

Table 194 LLDP configuration task

CONFIGURATION TASK		DESCRIPTION	RELATED SECTION
Basic configuration	Enable LLDP	Required	28.2.2
Advanced configuration	Configure LLDP Hello-time	Optional	28.2.3
	Configure LLDP Hold-time	Optional	28.2.4
	Configure LLDP packet sending & receiving mode	Optional	28.2.5
LLDP display and debugging		Optional	28.2.6

28.2.2 Enable LLDP

Only after enabling global LLDP, all related configurations can be effective. Global and port LLDP can be configured and saved no matter the LLDP is enabled. When global LLDP is enabled, the configuration is effective.

Perform following command in global configuration mode.

Table 195 Enable LLDP

OPERATION	COMMAND	DESCRIPTION
Enable LLDP	lldp	Required

28.2.3 Configure LLDP Hello-Time

By default, LLDP Hello-time is 30S.

Perform following command in global configuration mode.

Table 196 Configure LLDP Hello-time

OPERATION	COMMAND	DESCRIPTION
Configure LLDP Hello-time	lldp hello-time <5-32768>s	Optional

28.2.4 Configure LLDP Hold-Time

By default, LLDP Hold-time is 4S.

Perform following command in global configuration mode.

Table 197 Configure LLDP Hold-time

OPERATION	COMMAND	DESCRIPTION
Configure LLDP Hello-time	lldp hold-time <2-10>s	Optional

28.2.5 Configure LLDP Packet Transferring and Receiving Mode on Port

There are three types of mode:

- Rx: receiving only.
- Tx: transferring only.
- Rtx: transferring and receiving.

By default, the mode for all ports is rtx, that is, transferring and receiving all LLDP packets.

Perform following command in global or interface configuration mode.

Table 198 Configure LLDP packet transferring and receiving mode on port

OPERATION	COMMAND	DESCRIPTION
Configure LLDP packet transferring and receiving mode on port	lldp { rx rtx tx }	Optional

28.2.6 LLDP Displaying and Debugging

After the above configurations, you can execute the show commands in any configuration mode to display information, so as to verify your configurations.

Table 199 LLDP displaying and debugging

OPERATION	COMMAND	DESCRIPTION
Show LLDP status	<code>show lldp [interface ethernet device/slot/port]</code>	Execute this command in any configuration mode.

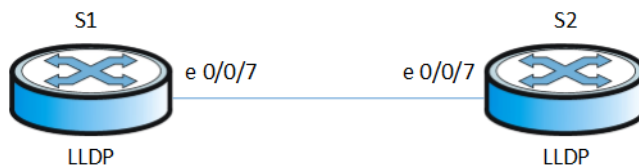
28.2.7 Configuration Example

1 Network requirements

Device S1 and S2 inform their own information through LLDP.

2 Network diagram

Figure 59 LLDP Network diagram



3 Configuration procedure

Configure in S1:

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

Configure in S2:

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

Execute **show lldp** command in any switch, followings will show:

```
*****
**
Switch(config)#sh lldp interface ethernet 0/0/7
System LLDP: enable
LLDP hello-time: 30(s)  LLDP hold-time: 4  LLDP TTL: 120(s)

Interface Ethernet 0/0/18
Port LLDP: rxtx          Pkt Tx: 1          Pkt Rx: 1
Total neighbor count: 1

Neighbor (1):
TTL: 109(s)
Chassis ID: 00:0a:5a:00:04:1e
Port ID: port e0/0/7
System Name: Switch S3200
System Description: MyPower Switch
Port Description: NULL
Management Address: 1.1.1.33
Port Vlan ID: 1
Port SetSpeed: auto
Port ActualSpeed: FULL-1000
Port Link Aggregation: support ,not in aggregation
*****
**
```


PPPoE Plus Configuration

29.1 Introduction

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks. It was developed by UUNET, Redback Networks and RouterWare and is available as an informational RFC 2516.

29.1.1 PPPoE packet format

PPPoE protocol packet is as following:

Figure 60 PPPoE packet format

```

+-----+-----+-----+-----+
| 0x0105 (Vendor-Specific) | TAG_LENGTH |
+-----+-----+-----+-----+
| 0x00000DE9 (Vendor-id) DSL Forum - IANA entry |
+-----+-----+-----+-----+
| SUB-TAG-Number | SUB-TAG-Len | SUB-TAG-Value |
+-----+-----+-----+-----+
| SUB-TAG-Value Cont' |
+-----+-----+-----+-----+

```

29.1.2 PPPoE Plus

PPPoE+ is short for PPPoE Intermediate agent which is proposed early in DSL FORM to define user line mark proportion on RFC 3046. The realization theory is similar to DHCP Option82 which makes some complement on PPPoE protocol packet. After accessing device get PPPoE protocol packet, insert user physical information for uplink direction, and strip it for downlink direction before transmission.

This function should work with PPPoE Plus server.

MyPower switch supports two kinds of PPPoE Plus packet:

- Standard mode: it contains user info: connected port, VLAN, MAC of local switch.

"0 0/0/0:4096.VID Switch MAC/0/0/slot/subslot/port"

- HuaWei mode: it can communicate with HuaWei BRAS. It contains user info: Connected port, VLAN, hostname and MAC of local switch.

"0 0/0/0:4096.VID Switch MAC/hostname/0/slot/sub-slot/port"

29.2 PPPoE Plus Configuration

29.2.1 Enable PPPoE Plus

PPPoE packet will be forwarded to trust port. Trust port should be configured after enable this function. Generally, PPPoE plus will add option content in PPPoE packet. If the PPPoE packet has contained option content before, the handling strategy will be defined.

Table 200 Enabling PPPoE Plus

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet device/slot/port</code>	-
Enabling PPPoE Plus	<code>pppoeplus</code>	Required
Configuring trust port	<code>pppoeplus trust</code>	Required
Configure option strategy	<code>pppoeplus strategy { drop keep replace }</code>	Optional
Drop padi/pado packets	<code>pppoeplus drop {padi pado}</code>	Optional
Specify circuit-id	<code>pppoeplus circuit-id string</code>	Optional

29.2.2 Option Content Configuration

The option content need to be added before PPPoE packet forwarding out, the contents of this option can be determined by a variety of ways. Option content can be specified in interface configuration mode. If the content is not specified, it will be constructed according to configured rules. If PPPoE plus type is self-defined, the format should also be specified.

Table 201 Option content configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure PPPoE Plus packet format	<code>pppoeplus type { huawei standard self-defined { circuit-id { <string> vlan port switch-mac hostname client-mac }* remote-id { <string> switch-mac hostname client-mac }* }</code>	Optional
Configure format	<code>pppoeplus format { binary ascii }</code>	Optional
Configure delimiter	<code>pppoeplus delimiter { colon dot slash space }</code>	Optional
Enter interface configuration mode	<code>interface ethernet device/slot/port</code>	-

29.2.3 PPPoE Plus Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 202 PPPoE Plus monitor and maintenance

OPERATION	COMMAND	REMARKS
Display PPPoE Plus configuration	<code>show pppoeplus [interface-list]</code>	On any configuration mode

CFM Configuration

30.1 Brief Introduction to CFM

CFM (Connectivity Fault Management, the connectivity fault management protocol), defined by the IEEE 802.1ag standard is a Layer 2 link on the VLAN-based end to end OAM mechanism used to Carrier Ethernet fault management.

30.1.1 CFM Concepts

Table 203 CFM concepts

CONCEPT	REMARK
MD	<p>Maintenance field indicates that even the fault detection is covered through a network of its boundary is configured on a port range defined by the MEPs. Maintenance domains are identified by "Names and Levels". According to network planning, levels can be divided into eight levels.</p> <p>Between different domains, they can be maintained adjacent to or nested, but can't cross to each other, and the nested domain can only be maintained by the high-level domain to the low level maintenance nested, that is, low-level maintenance of the domain must be included in the domain of high-level maintenance department.</p>
Maintenance set	<p>Within the maintenance domain can be configured as needed to maintain multiple sets, each set is maintained within some maintenance points. Maintenance set has been identified by " maintain the domain name + maintenance set name".</p> <p>Maintain set service on a VLAN, the packets sent from the maintenance points in the maintenance set have the VLAN tag, and maintenance points can receive the packets from the other maintenance points in the same maintenance set.</p>
Maintenance point	<p>Maintenance points are part of a maintenance set, them can be divided into Maintenance association End Point (MEP) and Maintenance domain Intermediate Point (MIP).</p> <p>MEP ID in order to maintain endpoint identity, which defines the scope and maintenance of the domain boundary. MEP has a directional, sub-UP MEP and DOWN MEP. MEP direction means that the maintenance domain relative to the location of the port. DOWN MEP is the port where to send its message, UP MEP port where it is not sent to the message, but it is the port to the device send its message.</p> <p>MIP is in the maintenance domain between points within the department, not the main action issued CFM protocol packets, but can handle and respond to CFM protocol packets.</p>
Enter global configuration mode	<code>configure terminal</code>

30.1.2 CFM Main Function

Connectivity fault detection is based on a reasonable and effective application deployment and configuration over the network, its function is maintained in the configuration between points, as long as the following functions:

Table 204 CFM main function

COMMAND	REMARKS
Continuity detection	It is a proactive OAM functionality is used to detect the state to maintain connectivity between endpoints. Connectivity failure may be caused by equipment failure or configuration error.
Loopback	It is a kind of on-demand OAM functions for the local device and remote authentication between end devices connected state.
Link tracking	It is a kind of on-demand OAM functions for the local device to determine the path between the remote devices, in order to achieve the positioning of link failure.

30.2 Configuring CFM

CFM function in the configuration before the network should carry the following plan:

- For the maintenance of the entire network to carry out sub-domain level, determine the level of maintenance of the domain boundary.
- Determine the maintenance of the domain name, the same domain on a different device to maintain the same name.
- Required monitoring of VLAN, determine the set of maintenance within the maintenance domain.
- Determine the maintenance set name, the same maintenance domain within the same set on different devices to maintain the same name.
- That the same maintenance domain within the same set of maintenance to maintain a list of endpoints in the different devices should remain the same.
- In the maintenance field and set the boundaries of the maintenance port on the endpoint should be planned maintenance, non-border or port equipment maintenance can be planned on a mid-point.

After the completion of network planning, come line the following configuration.

30.2.1 CFM Configuration Task List

Table 205 CFM Configuration Task List

CONFIGURATION TASKS		REMARK	DETAILED CONFIGURATION
CFM basic configuration	Configured to maintain field	Required	30.2.2
	Configuration and maintenance level domain name	Required	30.2.3
	Configuration to maintain set	Required	30.2.4
	Configuration name and the associated VLAN to maintain set	Required	30.2.5
	Configuration MEPs	Required	30.2.6
	Configure Remote Maintenance endpoint	Required	30.2.7
	Configuring MIPs	Optional	30.2.8
Configuring CFM various functions	Configuration continuity detection	Required	30.2.9
	Configure loopback	Optional	30.2.10
	Configure the link tracking	Optional	30.2.11
Y.1731 Configuration	Y.1731 frame loss detection	Optional	30.2.12
	Y.1731 frame delay detection	Optional	30.2.13
Display and maintenance of the CFM		Optional	30.2.14

30.2.2 Maintain Field Configuration

Table 206 Maintain field configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Create a maintenance domain, and domain configuration into maintenance mode	<code>cfm md md-index</code>	Required
Enter global configuration mode	<code>configure terminal</code>	

30.2.3 Configuration and Maintenance Level Domain Name

In order to distinguish between the various maintenance domain, you can assign different domain name to each maintenance domain, the domain name is composed of format and content, and it must be unique in the network. For showing nested relationship between the maintenance domain,

user must also maintains the domain level, only the level of maintenance of large domain nested level can only be a small maintenance domain.

Table 207 Configuration and maintenance level domain name

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Domain configuration into maintenance mode	<code>cfm md md-index</code>	When domain doesn't exist, create the domain
Configuration without the maintenance of domain names, only the specified field level maintenance	<code>cfm md format none level <i>md-level</i></code>	Either of the two
Equipped with the maintenance of the domain name, and specify the domain name and level of maintenance	<code>cfm md format {dns-name mac-uint string} name <i>md-name</i> level <i>md-level</i></code>	

30.2.4 Maintain Set Configuration

Table 208 Maintain set configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Created to maintain set, and enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	Required

30.2.5 Configuration Name and Associated VLAN to Maintenance Set

In order to maintain the distinction between the various domains to maintenance set, you can specify a different set for each to maintain the instance name, which is composed of format and content, the maintenance domain name and the maintenance set and its instance must be unique in the network.

Table 209 Configuration name and the associated VLAN to maintain set

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
The name of the configuration set and maintain the VLAN associated with the main	<code>cfm ma format {primary-vid string uint16 vpn-id} name <i>ma-name</i> primary-vlan <i>vlan-id</i></code>	Required

30.2.6 Configuration MEPs

CFM is mainly reflected in the maintenance of a variety of endpoints operating on, user can program the network port on the network configuration to maintain the boundary endpoints.

Table 210 Configuration MEPs

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Create a maintenance endpoint, and specify its associated port	<code>cfm mep mep-id direction {up down} [primary-vlan vlan-id] interface ethernet port-id</code>	Required
Enable the state to maintain endpoint management	<code>cfm mep mep-id state {enable disable}</code>	Required Default is off
CCM and configure the endpoint to send maintenance to use the priority LTM	<code>cfm mep mep-id priority priority-id</code>	Optional Default priority is 0

30.2.7 Configure Remote Maintenance Endpoint

Remote maintenance end point is equivalent to the local maintenance of the end points, and in the maintenance of concentration, in addition to the maintenance of the local endpoint, all other maintenance endpoints should be configured in the local endpoint for the remote maintenance.

Table 211 Configure Remote Maintenance endpoint

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Creating remote maintenance end point, and specify the end of its peer MEPs	<code>cfm rmep rmep-id mep mep-id</code>	Required

30.2.8 Configuring MIPs

MIPs used to test the response of CFM message, the user can program the network device or in non-border ports configured to maintain the mid-point.

Table 212 Configuring MIPs

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-

Table 212 Configuring MIPs

OPERATION	COMMAND	REMARKS
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Create a maintenance intermediate point, and specify its associated port	<code>cfm mip mip-id interface ethernet port-id</code>	Optional

30.2.9 Configuration Continuity Detection

Configuring continuity detection can be made to maintain interoperability between endpoint CCM packets to check the connectivity between these endpoints maintain state in order to achieve the link connectivity management.

Table 213 Configuration continuity detection

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Configuration maintenance interval endpoint to send the CCM	<code>cfm cc interval {1 10 60 600}</code>	Optional The default value is 1s
Enable sending MEP ccm	<code>cfm mep mep-id cc {enable disable}</code>	Required Default is off

Different devices at the same maintenance domain and maintain a centralized maintenance endpoint, the sending time interval of CCM must be the same.

30.2.10 Configure Loopback

By configuring the loopback function, you can check the source to the target MEPs or MIPs link between the situations in order to achieve the link connectivity verification.

Table 214 Configure loopback

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Start loopback	<code>cfm loopback mep mep-id {dst-mac mac-address dst-mep rmep-id} [priority pri-id count pkt-num length data-len data pkt-data]</code>	Optional

30.2.11 Configure Link Tracking

By configuring the link tracking, you can find the source to the target MEPs or maintenance intermediate point between the path in order to achieve the positioning of link failure.

Table 215 Configure the link tracking

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Start Tracking link	<code>cfm linktrace mep mep-id {dst-mac mac-address dst-mep rmep-id} [timeout pkt-time ttl pkt-ttl flag {use-mpdb unuse-mpdb}]</code>	Optional

30.2.12 Y.1731 frame loss detection

Table 216 Y.1731 frame loss detection

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Start Tracking link	<code>cfm eth-slm mep mep-id { dst-mac mac-address dst-mep rmep-id } [timeout pkt-time priority priority-identifier interval second /count packet-num]</code>	Optional

30.2.13 Y.1731 frame delay detection

Table 217 Frame delay detection

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
To maintain the domain configuration mode to enter	<code>cfm md md-index</code>	-

Table 217 Frame delay detection

OPERATION	COMMAND	REMARKS
Enter the configuration mode set to maintain	<code>cfm ma ma-index</code>	-
Start Tracking link	<code>cfm eth-2dm mep mep-id { dst-mac mac-address dst-mep rmep-id } [timeout pkt-time priority priority-identifier interval second /count packet-num]</code>	Optional

30.2.14 Display and Maintenance of CFM

After completing the above configuration, you can use the following command to display the CFM configuration.

Table 218 Display and maintenance of the CFM

OPERATION	COMMAND	REMARKS
The Maintenance domain information	<code>show cfm md [md-index]</code>	Perform either of the commands
The Maintenance Set Information	<code>show cfm ma</code>	
Display the end point of maintenance information	<code>show cfm mp local</code>	
Remote maintenance point information display	<code>show cfm mp remote</code>	
Display CCM statistics	<code>show cfm cc</code>	
Clear CCM statistics	<code>clear cfm cc</code>	
CCM database information display	<code>show cfm cc database</code>	
Clear CCM database information	<code>clear cfm cc database</code>	
CFM alarm information display	<code>show cfm errors</code>	

Flex Links Configuration

31.1 Flex Links Overview

Flex links is a layer2 links backup protocol. You can choose Flex links to realize link backup when customers don't want STP in their network. If Flex links is enabled, STP feature must be disabled, you can only choose either one. Flex links consists of a pair of interfaces (can be ports or aggregated interface). When one interface is transmitting data, the other interface will be under standby mode. The backup interface starts transmitting data when there is defect in the master link. The failed interface will go into standby mode, When the failed interface recovers, it will begin to transmit data in 60 seconds when preempt mechanism is configured. Flex links interface can configure bandwidth and delay time being preempt mechanism. The superior interface will be the master one, system also provides trap alarm when master or backup link interface failure.

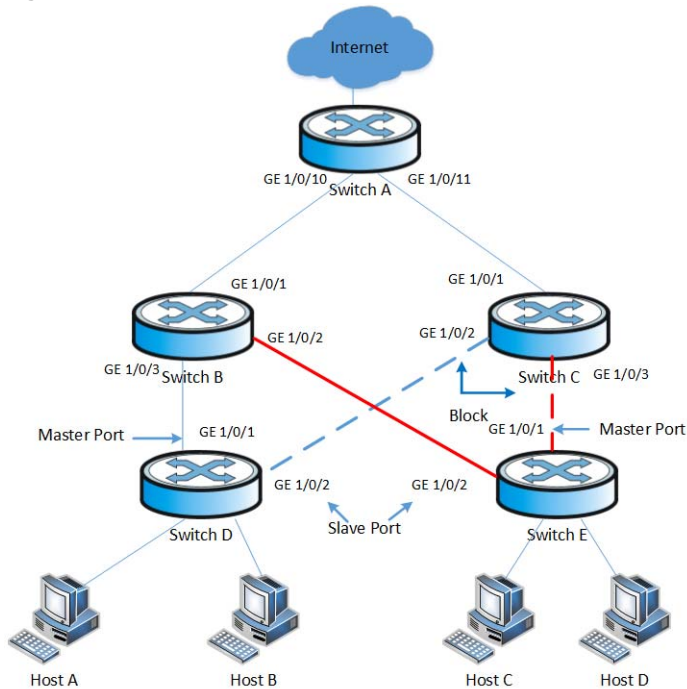
Flex Link is dedicated to dual-uplink networks. It delivers the following benefits:

- Keeping one uplink connected and the other blocked, thus preventing broadcast storms caused by network loops and also provides an un-interrupted uplink interface.
- Fast switching the traffic to the backup link within a few sub-seconds once the primary link fails. Thus, we can keep the normal traffic continue to forward in the network.
- Easy to configure.

31.1.1 Basic Concept of Flex Links

1 Flex Links group

A Flex link group consists of only two member ports: the master and the slave. Only one port is active for forwarding, and the other port is blocked, that is, in the standby state. When link failure occurs on the active port due to port shutdown or unidirectional link failure, the standby port will become active to take over and at the same time, the original active port will transit to the blocked state.

Figure 61 Flex Link application scenario

As shown in [Figure 61 on page 237](#), GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch D form a Flex link group (marked in blue). GigabitEthernet 1/0/1 is in the forwarding state (marked by a continuous line), and GigabitEthernet 1/0/2 is in the blocked state (marked by a broken line). GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch E form another Flex link group (marked in red). GigabitEthernet 1/0/1 is in the blocked state (marked by a broken line), and GigabitEthernet 1/0/2 is in the forwarding state (marked by a continuous line).

2 Master port

The master port of a Flex link group is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

As shown in [Figure 61 on page 237](#), the active port in the Flex link group configured on Switch D is the master port GigabitEthernet 1/0/1, while that in the Flex link group on Switch E is the slave port GigabitEthernet 1/0/2. Although GigabitEthernet 1/0/1 of Switch E is blocked, it is still the master port.

3 Slave port

The slave port of a Flex link group is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface. The link on which the slave port resided is the backup link.

As shown in [Figure 61 on page 237](#), the blocked port in the Flex link group on Switch D is the slave port GigabitEthernet 1/0/2, while that in the Flex link group on Switch E is the master port GigabitEthernet 1/0/2. Although GigabitEthernet 1/0/1 of Switch E is in the forwarding state, it is still the slave port.

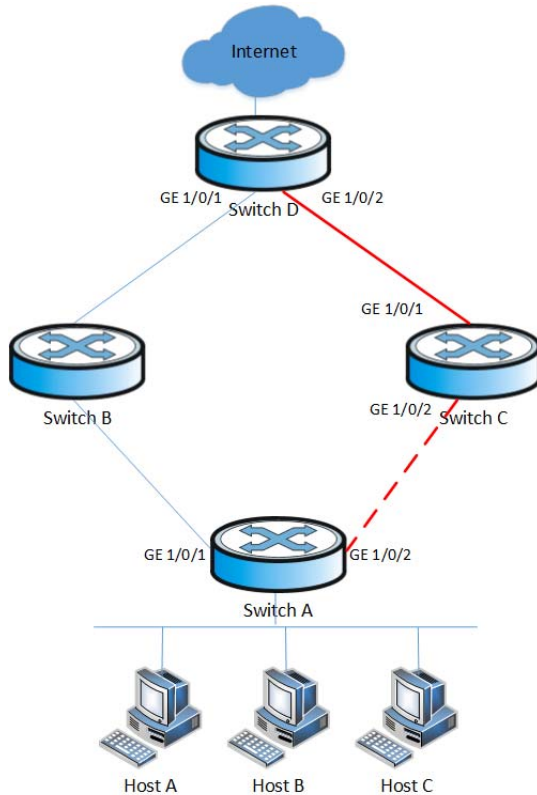
4 MMU (MAC address-table Move Update) message

When link switchover occurs in a Flex link group, the old forwarding entries are no longer useful for the new topology. Therefore, all devices in the network need to refresh their MAC address forwarding entries. Flex Link notifies devices to refresh their MAC address forwarding entries by sending MMU messages to them.

31.1.2 Operating Mechanism of Flex Link

This section uses the network shown in [Figure 62 on page 238](#) to describe the Flex link mechanism as the link status transiting from normal, to faulty, and then to recovery.

Figure 62 Flex Link application scenario



31.1.2.1 Link-Normal Operating

GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A form a Flex link group, with the former as the master port and the latter as the slave port. When both uplinks are healthy, the master port is in the forwarding state, while the slave port is in the standby state, and the links on which the two ports are resided respectively are called the primary link and the backup link. In this case, data is transmitted along the link indicated by the blue line. There is no loop in the network, hence no broadcast storms as well.

31.1.2.2 Link-Faulty Handling

When the primary link on Switch A fails, the master port GigabitEthernet 1/0/1 transits to the standby state, while the slave port GigabitEthernet 1/0/2 transits to the forwarding state, this is a link switchover occurring. After the link switchover, the MAC address forwarding entries kept on the devices of the network may become incorrect, and must be refreshed, otherwise the traffic loss will

happen. Currently, there is one mechanism available for refreshing MAC address forwarding entries: MMU message-notified refreshing.

This mechanism is applicable when the upstream devices (such as Switch B, Switch C, and Switch D in [Figure 62 on page 238](#)) support Flex Link and are able to recognize MMU messages.

To enable rapid link switchover, you need to enable Switch A to send MMU messages, and all upstream devices' ports that are on the dual uplink network to receive and process MMU messages.

After link switchover occurs on Switch A, MMU messages are sent to the new primary link, that is, through GigabitEthernet 1/0/2. When an upstream device receives and processes a MMU message, transmit MAC address carried in the MMU message to the receiving port.

After that, when Switch D receives a data packet destined for Host A, Host B, Host C, switch D will flood the packet at Layer 2; Switch C will lookup MAC address table after receiving it, and then forward to Switch A via GE1/0/2; Switch A forward it to Host A, Host B, Host C. In this way, data traffic can be forwarded correctly.

This mechanism will update MAC address without waiting for entry aged out. Generally, the whole network will be recovered in milliseconds without traffic lost.

31.1.2.3 Link-Recovery Working Modes

Flex Link supports three working modes: role preemption, non-role preemption and bandwidth preemption. Under different modes, the port state changes are different:

- If role preemption is configured, when the primary link recovers, the master port enters the forwarding state and takes over the traffic, while the slave port enters the standby state. The slave port transits from standby to forwarding only when the primary link fails.
- If non-role preemption is configured, when the primary link recovers, the slave port remains in the forwarding state, while the master port remains in the standby state, so as to keep the traffic stable.
- If bandwidth preemption is configured, when the primary link recovers, the slave port remains in the forwarding state if it occupies more bandwidth, while the master port remains in the standby state; the slave port transits from forwarding to standby only when master port occupies more bandwidth.

As shown in [Figure 62 on page 238](#), if role preemption is configured on the Flex link group on Switch A, when the link of GigabitEthernet 1/0/1 on Switch A recovers, GigabitEthernet 1/0/2 is immediately blocked and transits to the standby state, while GigabitEthernet 1/0/1 transits to the forwarding state. If non-role preemption is configured, when the link of GigabitEthernet 1/0/1 on Switch A recovers, GigabitEthernet 1/0/1 remains in the standby state, and no link switchover occurs, thus keeping the traffic stable.

31.2 Flex Links Configuration

31.2.1 Flex Links Configuration Tasks

Table 219 Flex Links Configuration Tasks

OPERATION		DESCRIPTION	RELATED SECTION
Flex Links basic configuration	Configure Flex Links group	Required	31.2.2
Advanced Flex Links configuration	Configure Flex Links preemption mode	Optional	31.2.3
	Configure Flex links preemption delay	Optional	31.2.4
	Configure Flex links MMU	Optional	31.2.5
Flex Links monitor and maintenance		Optional	31.2.6

31.2.2 Configure Flex Links group

Configuring Flex Links group needs specify master and slave port. If master port is Ethernet port, the configuration should be in interface configuration mode; if master port is channel-group port member, the configuration should be in global configuration mode.

Table 220 Configure Flex Links group

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure Flex Links group	<code>channel-group channel-group-number_1 backup { interface device/slot/port_2 channel-group channel-group-number_2 }</code>	<i>channel-group-number_1</i> is master port, <i>port_2/channel-group-number_2</i> is slave port
Delete Flex Links group	<code>no channel-group channel-group-number_1 backup</code>	Optional
Enter interface configuration mode	<code>interface ethernet device/slot/port_1</code>	-
Configure Flex Links group	<code>switchport backup { interface device/slot/port_2 channel-group channel-group-number_2 }</code>	<i>port_1</i> is master port, <i>port_2/channel-group-number_2</i> is slave port
Delete Flex Links group	<code>no switchport backup</code>	Optional

Note: The STP of master port and slave port should be disabled, and cannot be ERRP port.

31.2.3 Configure Flex Links Preemption Mode

Only one port can be active for forwarding, and the other port is in the standby state. When link failure occurs on the active port due to port shutdown or presence of unidirectional link for

example, the standby port becomes active to take over while the original active port transits to be blocked or standby state.

Table 221 Configure Flex Links preemption mode

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	-
Configure Flex Links preemption mode	channel-group <i>channel-group-number_1</i> backup { interface <i>device/slot/port_2</i> channel-group <i>channel-group-number_2</i> } preemption mode { Forced Bandwidth Off }	<i>channel-group-number_1</i> is master port, <i>port_2</i> / <i>channel-group-number_2</i> is slave port
Enter interface configuration mode	interface ethernet <i>device/slot/port_1</i>	-
Configure Flex Links preemption mode	switchport backup { interface <i>device/slot/port_2</i> channel- group <i>channel-group-number_2</i> } preemption mode { Forced Bandwidth Off }	<i>port_1</i> is master port, <i>port_2/channel-group- number_2</i> is slave port

31.2.4 Configure Flex Links Preemption Delay

After configuring Flex Links preemption mode, the port will not be in active state immediately. There is a preemption delay time, default delay is 45 sec.

Table 222 Configure Flex links preemption delay

OPERATION	COMMAND	REMARKS
Enter global configuration mode	configure terminal	-
Configure Flex links preemption delay	channel-group <i>channel-group-number_1</i> backup { interface <i>device/slot/port_2</i> channel-group <i>channel-group-number_2</i> } preemption delay <1-60>	<i>channel-group-number_1</i> is master port, <i>port_2</i> / <i>channel-group-number_2</i> is slave port
Enter interface configuration mode	interface ethernet <i>device/slot/port_1</i>	-
Configure Flex links preemption delay	switchport backup { interface <i>device/slot/port_2</i> channel- group <i>channel-group-number_2</i> } preemption mode <1-60>	<i>port_1</i> is master port, <i>port_2/channel-group- number_2</i> is slave port

31.2.5 Configure Flex Links MMU

MMU messages are used by a Flex link group to notify other switches to refresh their MAC address forwarding entries and ARP/ND entries when link switchover occurs in the Flex link group. MMU

messages are a unicast data packets, and will be dropped if the receiving port is blocked. This function is disabled by default, you must enable it if you need.

Table 223 Configure Flex links MMU

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure Flex links MMU	<code>mac-address-table move update { transmit receive }</code>	<i>port_1</i> is master port, <i>port_2/channel-group-number_2</i> is slave port

31.2.6 FLex Links Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 224 FLex Links monitor and maintenance

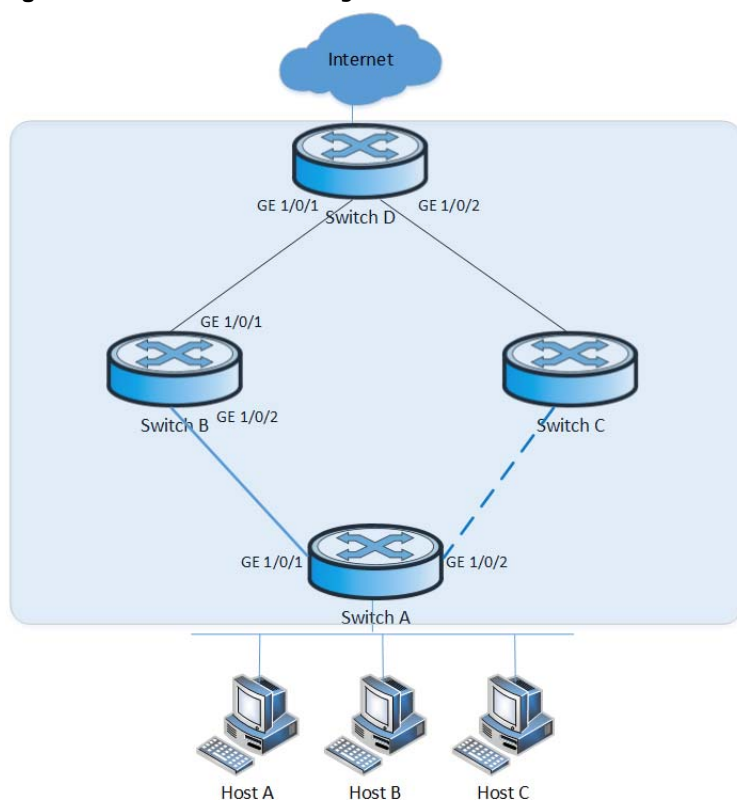
OPERATION	COMMAND	REMARKS
Display configured Flex Links group	<code>show interface switch backup</code>	On any configuration mode
Display Flex Links MMU status	<code>sh mac-address-table move update</code>	On any configuration mode

Monitor Link Configuration

32.1 Monitor Link Overview

32.1.1 Background

Figure 63 Monitor Link background



As shown in [Figure 63 on page 243](#), a Flex link group is configured on Switch A for link redundancy purpose, with GigabitEthernet 1/0/1 as the master port, and GigabitEthernet 1/0/2 as the slave port.

When the primary link on which GigabitEthernet 1/0/1 fails, traffic will switch to the backup link on which GigabitEthernet 1/0/2 within a few sub-seconds. Flex Link can provide reliable link redundancy and rapid convergence.

However, when the link on which the uplink port GigabitEthernet 1/0/1 of Switch B resides fails, link switchover will not happen in the Flex link group configured on Switch A because the link on which the master port GigabitEthernet 1/0/1 resided is healthy. But in fact, traffic of Switch A can no longer reach Switch D through GigabitEthernet 1/0/1, and the traffic is thus interrupted. To address this problem, the Monitor Link technology is introduced.

32.1.2 Benefits

Monitor Link is developed to complement the Flex Link feature. By monitoring the uplink, Monitor Link feature will synchronize the downlink interface with the uplink one, it can trigger the switchover of Flex links group between the primary and backup links, thus makes the Flex links feature more useful and complete.

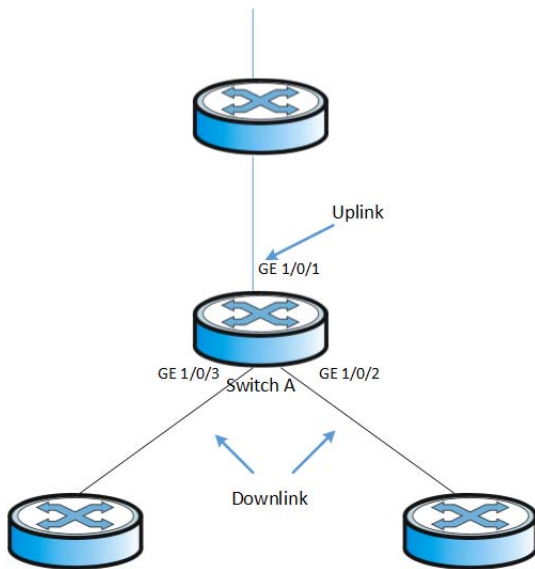
32.2 Monitor Link Implementation

32.2.1 Basic Concepts in Monitor Link

32.2.1.1 Monitor Link Group

A monitor link group is a set of uplink and downlink ports. Downlink ports will follow the state changing of uplink ports.

Figure 64 Monitor Link basic concepts



As shown in [Figure 64 on page 244](#), ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of Switch A form a monitor link group.

1 Uplink Port

An uplink port is a monitored port in a monitor link group. It is a port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

As shown in [Figure 64 on page 244](#), GigabitEthernet 1/0/1 of Switch A is the only uplink port of the monitor link group configured on the device.

For a monitor link group that has multiple uplink ports, as long as at least one of its uplink ports is in the forwarding state, the monitor link group is up. Once all uplink ports of the monitor-link group fails, the monitor-link group will go down, and then shutting down all the downlink ports. If no

uplink port is specified in a monitor link group, the system will consider the uplink ports of the monitor-link group is incorrect, and thus shuts down all the downlink ports in the monitor link group.

2 Downlink Port

A downlink port is a monitoring port in a monitor link group. It is another port role specified using commands. It can be an Ethernet port (electrical or optical), or an aggregate interface.

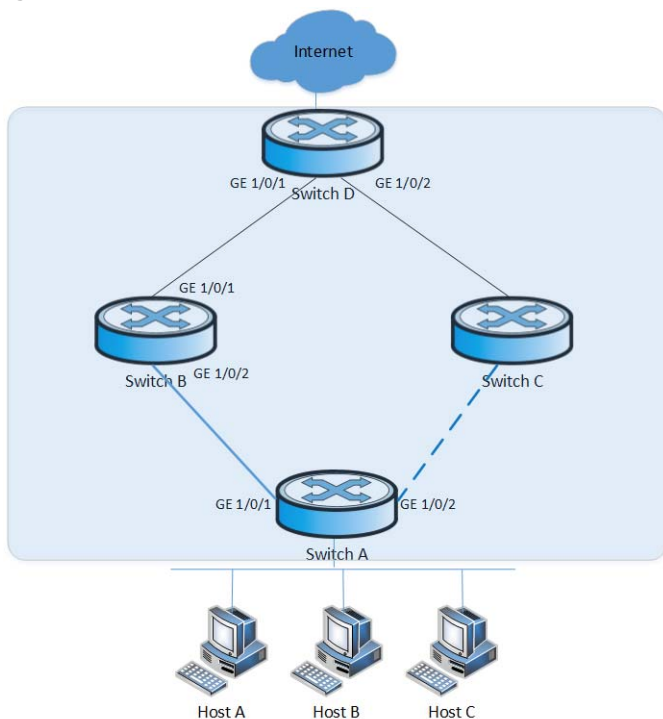
As shown in [Figure 64 on page 244](#), GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A are two downlink ports of the monitor link group configured on the device.

Note: When a monitor link group's uplink ports recover, only downlink ports that were blocked due to uplink port failure will be brought up. Downlink ports manually shut down will not be brought up automatically. The failure of a downlink port does not affect the uplink ports or other downlink ports.

32.2.1.2 Monitor Link Mechanism

As shown in [Figure 65 on page 245](#), to provide reliable access to the Internet for the hosts, a Flex link group is configured on Switch A. GigabitEthernet 1/0/1 is the master port of the Flex link group, and is in the forwarding state. GigabitEthernet 1/0/2 is the slave port.

Figure 65 Monitor Link mechanism



To avoid traffic interruption due to the failure of the link on which GigabitEthernet 1/0/1 of Switch B resides, configure a monitor link group on Switch B, and specify GigabitEthernet 1/0/1 as the uplink port, and GigabitEthernet 1/0/2 as the downlink port.

When the link on which GigabitEthernet 1/0/1 of Switch B resided fails, the monitor link group shuts down its downlink port GigabitEthernet 1/0/2, and a link switchover is triggered in the Flex link group configured on Switch A.

When the link on which GigabitEthernet 1/0/1 of Switch B resided recovers, the downlink port GigabitEthernet 1/0/2 is also brought up, and another link switchover is triggered in the Flex link group if role preemption is configured in the Flex link group on Switch A.

Collaboratively, Monitor Link and Flex Link can provide reliable link redundancy and fast convergence for dual-uplink networks.

32.3 Configuring Monitor Link

32.3.1 Monitor Link Configuration Tasks

Table 225 Flex Links Configuration Tasks

OPERATION		REMARKS	RELATED SECTIONS
Monitor Link configuration	For channel-group	Required	32.3.2
	For port	Required	32.3.2
Monitor Link monitor and maintenance		Optional	32.3.3

32.3.2 Configure Monitor Links Group

If the port is Ethernet port, configuration should be in interface configuration mode; if port is channel-group member, configuration should be in global configuration mode.

Table 226 Configure Monitor Links group

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Monitor Link for channel-group	<code>channel-group <i>channel-group-number</i> monitor-link-group <i>group-ID</i> { uplink downlink }</code>	-
Delete channel-group from Monitor Link group	<code>No channel-group <i>channel-group-number</i> monitor-link-group <i>group-ID</i> { uplink downlink }</code>	Optional
Enter interface configuration mode	<code>interface ethernet <i>device/slot/port</i></code>	-
Monitor Link for port	<code>switchport monitor-link-group <i>group-ID</i> { uplink downlink }</code>	-
Delete port from Monitor Link group	<code>No switchport monitor-link-group <i>group-ID</i> { uplink downlink }</code>	Optional

32.3.3 Monitor Link Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 227 Monitor Link monitor and maintenance

OPERATION	COMMAND	REMARKS
Show Monitor Link group	show monitor-link-group	On any configuration mode

32.4 Monitor Link Configuration Example

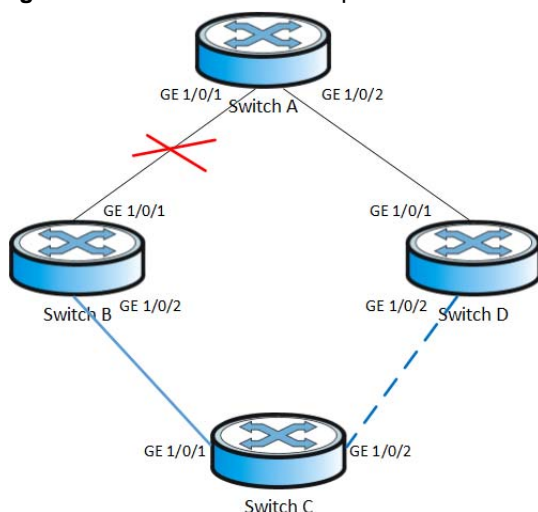
Network requirements

In [Figure 66 on page 247](#), Device C is Flex Links Device, Device A, Device B and Device D is the neighbor devices. The traffic of Device C double uplinks to Device A through Flex Links group.

Through configuration, Device C can make double uplink backup. When the link between Device A and Device B, Device C can detect the failure and shift the uplink .

Network diagram

Figure 66 Monitor link example



Configuration procedure

Device C

Disable STP on GE1/0/1 and GE1/0/2, configure them as Trunk

```
Device-C(config)#interface range ethernet 1/0/1 ethernet 1/0/2
Device-C(config-if-range)#no spanning-tree
Device-C(config-if-range)#switchport mode trunk
Device-C(config-if-range)#exit
```

Configure Flex Links group, GE1/0/1 is the master port and GE1/0/2 is the slave port. The preemption is role preemption and the delay is 5s

```
Device-C(config-if-ethernet-1/0/1)#switchport backup interface ethernet 1/0/2
Device-C(config-if-ethernet-1/0/1)#switchport backup interface ethernet 1/0/2
preemption mode forced
Device-C(config-if-ethernet-1/0/1)#switchport backup interface ethernet 1/0/2
preemption delay 5
Device-C(config-if-ethernet-1/0/1)#exit
```

Enable MMU packet sending

```
Device-C(config)#mac-address-table move update transmit
```

#Show Flex Links

```
Device-C(config)#show interface switchport backup
ActiveInterface  BackupInterface  State
-----
e1/0/1          e1/0/2          active up /backup Standby
Preemption mode: Forced
Preemption Delay: 5 seconds

Total record 1.
```

```
Device-C(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/Off,Xmt Off/On
Rcv Count:            : 0
Xmt Count:            : 0
```

Device A

Configure GE1/0/1 and GE1/0/2 to be Trunk and enable MMU packet receiving

```
Device-A(config)#interface range ethernet 1/0/1 ethernet 1/0/2
Device-A(config-if-range)#switchport mode trunk
Device-A(config-if-range)#exit
Device-A(config)#mac-address-table move update receive
```

Device B

Configure GE1/0/1 and GE1/0/2 to be Trunk and enable MMU packet receiving

```
Device-B(config)#interface range ethernet 1/0/1 ethernet 1/0/2
Device-B(config-if-range)#switchport mode trunk
Device-B(config-if-range)#exit
Device-B(config)#mac-address-table move update receive
```

Configure GE1/0/1 to be uplink port of Monitor Link group 1,GE1/0/2 to be downlink port of Monitor Link group 1

```
Device-B(config)#interface ethernet 1/0/1
Device-B(config-if-ethernet-1/0/1)#switchport monitor-link-group 1 uplink
Device-B(config-if-ethernet-1/0/1)#exit
Device-B(config)#interface ethernet 1/0/2
Device-B(config-if-ethernet-1/0/2)#switchport monitor-link-group 1 downlink
Device-B(config-if-ethernet-1/0/2)#exit
```


#Show Monitor Link

```
Device-C(config)#show monitor-link-group
Monitor-link Group
```

```
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        UP
DownlinkID    DownlinkStatus
e1/0/2        UP
```

```
Device D
```

#Configure GE1/0/1 and GE1/0/2 to be Trunk and enable MMU packet receiving

```
Device-D(config)#interface range ethernet 1/0/1 ethernet 1/0/2
Device-D(config-if-range)#switchport mode trunk
Device-D(config-if-range)#exit
Device-D(config)#mac-address-table move update receive
```

Configure GE1/0/1 to be uplink port of Monitor Link group 1,GE1/0/2 to be downlink port of Monitor Link group 1

```
Device-DB(config)#interface ethernet 1/0/1
Device-D(config-if-ethernet-1/0/1)#switchport monitor-link-group 1 uplink
Device-D(config-if-ethernet-1/0/1)#exit
Device-D(config)#interface ethernet 1/0/2
Device-D(config-if-ethernet-1/0/2)#switchport monitor-link-group 1 downlink
Device-D(config-if-ethernet-1/0/2)#exit
```

#Show Monitor Link

```
Device-D(config)#show monitor-link-group
Monitor-link Group
```

```
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        UP
DownlinkID    DownlinkStatus
e1/0/2        UP
```

When there is failure between Device A and Device B,show Flex Links and Monitor Link in Device B:

```
Device-B(config)#show monitor-link-group
Monitor-link Group
```

```
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        DOWN
DownlinkID    DownlinkStatus
e1/0/2        DOWN
```

```
Device-B(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/On,Xmt Off/Off
Rcv Count:            : 0
Xmt Count:            : 0
```

show Flex Links and Monitor Link in Device C:

```
Device-C(config)#show interface switchport backup
ActiveInterface  BackupInterface  State
-----
e1/0/1          e1/0/2          active Standby /backup up
Preemption mode: Forced
Preemption Delay: 5 seconds

Total record 1.
```

```
Device-C(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/Off,Xmt Off/On
Rcv Count:            : 0
Xmt Count:            : 1
```

show Flex Links and Monitor Link in Device D:

```
Device-D(config)#show monitor-link-group
Monitor-link Group
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        UP
DownlinkID    DownlinkStatus
e1/0/2        UP

Device-D(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/On,Xmt Off/Off
Rcv Count:            : 1
Xmt Count:            : 0
```

When the link between Device A and Device B recovers, GE1/0/1 of Device C will turn into forwarding after 5s. Show Flex Links and Monitor Link in Device B:

```
Device-B(config)#show monitor-link-group
Monitor-link Group
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        UP
DownlinkID    DownlinkStatus
e1/0/2        UP

Device-B(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/On,Xmt Off/Off
Rcv Count:            : 1
Xmt Count:            : 0
```

show Flex Links and Monitor Link in Device C:

```
Device-C(config)#show interface switchport backup
ActiveInterface  BackupInterface  State
-----
e1/0/1          e1/0/2          active up /backup Standby
Preemption mode: Forced
Preemption Delay: 5 seconds

Total record 1.
```

```
Device-C(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/Off,Xmt Off/On
Rcv Count:            : 0
Xmt Count:            : 2
```

show Flex Links and Monitor Link in Device D:

```
Device-D(config)#show monitor-link-group
Monitor-link Group
-----
Group 1:
UplinkID      UplinkStatus
e1/0/1        UP
DownlinkID    DownlinkStatus
e1/0/2        UP

Device-D(config)#show mac-address-table move update
Dst mac-address:      : 01:80:c2:00:00:10
Default/Current settings: : Rcv Off/On,Xmt Off/Off
Rcv Count:            : 1
Xmt Count:            : 0
```

EFM/OAM Configuration

33.1 Brief Introduction to EFM/OAM

EFM (Ethernet of First Mile)/Ethernet OAM (Operations, Administration and Maintenance) as described in IEEE 802.3ah is a link monitoring protocol, it utilizes OAM Protocol Data Units or OAM PDU's to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

The Switch supports the following IEEE 802.3ah functions:

33.1.1 EFM/OAM Main Function

EFM Ethernet can effectively improve the management and maintenance capabilities to ensure the stable operation of the network, its main features include:

Table 228 EFM main function

FUNCTION	REMARKS
EFM auto-discovery	IEEE 802.3ah provides a mechanism to detect the presence of an 802.3ah-capable Network Device (ND) on the other end of the Ethernet link. To this end, the 802.3ah-capable ND sends specified OAMPDUs in a periodic fashion, normally once a second. During the OAM Discovery process, the 802.3ah-capable ND monitors received OAMPDUs from the remote ND and based upon local and remote state and configuration settings allows 802.3ah OAM functionality to be enabled on the link. In other words, it supports OAM capability discovery function and hence eliminates the need for operator configuration.
Remote failure indication	<p>IEEE 802.3ah provides a mechanism to indicate to a peer Network Device (ND) that its receive path is non-operational.</p> <p>When the device detects a link event of an emergency, the fault will end EFM entity's Flag by using OAMPDU fault information field (the type of emergency event link) EFM notification to the peer entity. In this way, administrators can log information by observing the dynamic understanding of the link state, the corresponding error in a timely manner for processing.</p> <p>The event types include emergency Link Fault, Dying Gasp and Critical Event...etc.</p>

Table 228 EFM main function

FUNCTION	REMARKS
Link monitoring capabilities	<p>IEEE 802.3ah provides a mechanism to support event notification across the link to communicate the following statistics regarding link health. It allows the operator to configure the corresponding thresholds to monitor signal degradation (i.e., frame errors).</p> <p>Link monitoring function is used in a variety of environments and found that the link layer fault detection, EFM through interactive Event Notification OAMPDU to monitor the link: When the end of the EFM to detect the general physical link event, the Event Notification sent to its peer OAMPDU for notification, the administrator could observe, log the information and analyze the events if it's necessary.</p> <p>Event types include general link-errored-symbol-period, errored-frame, errored-frame-period, errored-frame-seconds four.</p>
Remote loopback	<p>IEEE 802.3ah provides a mechanism to support a data link layer frame-level loopback mode. With this function, the operator may test the performance of the link prior to placing a link in service. Once the Ethernet physical link is verified to be operational and error-free, the operator takes the link out of remote loopback and places it in service.</p> <p>Operator can use the function understand the link quality and positioning of link failure.</p>
Remote access to MIB variable function	EFM entities can interact with Variable Request / Response OAMPDU far end of the entity to obtain the MIB variable value. Include Ethernet MIB variable chain on the road all the performance parameters and error statistics. It provides a local EFM physical entity on the far side of the general performance and error detection mechanisms.

Description:

We said so to the EFM port functions as "EFM Entities.

33.1.2 EFM/OAM Protocol Packets

EFM working in the data link layer, the protocol packet is called OAMPDU (OAM Protocol Data Units, OAM protocol data unit). EFM is through regular interaction between the device OAMPDU to report link status, enabling network administrators to effectively manage the network.

Table 229 EFM protocol packets

MESSAGE TYPE	EFFECT
Information OAMPDU	EFM entity status for the information (including local information, the remote information and custom information) sent to the remote entity EFM, EFM connections to maintain.
Event Notification OAMPDU	Generally used for link monitoring on local and remote connected EFM physical link failures in the warning.
Loopback Control OAMPDU	Mainly use for remote loopback control in order to control the EFM loopback state of remote device. The packet has the information of enabling or disabling loopback. Enabling or disabling remote loopback based on this information.
Variable Request / Response OAMPDU	Mainly used for remote MIB variable values, in order to achieve the end of the remote state prosecution.

33.2 Configuration EFM/OAM

33.2.1 EFM/OAM Configuration Task List

Table 230 EFM configuration task list

CONFIGURATION TASKS		REMARK	DETAILED CONFIGURATION
EFM basic configuration	Start EFM	Required	33.2.2
	EFM mode configuration	Optional	33.2.2
EFM timer parameter configuration	Configure the interval to send handshake packets EFM	Optional	33.2.3
	Configure the connection timeout EFM	Optional	33.2.3
	Response timeout configuration	Optional	33.2.3
Configure remote failure indication		Optional	33.2.4
Configure link monitoring capabilities	Start link monitoring capabilities	Optional	33.2.5
	Configure errored-symbol-period event detection parameters	Optional	33.2.5
	Configure errored-frame event detection parameters	Optional	33.2.5
	Configure errored-frame-period event detection parameters	Optional	33.2.5
	Configure errored-frame-seconds event detection parameters	Optional	33.2.5
Configure remote access function MIB variable	Start the remote access function MIB variable	Optional	33.2.6
	MIB variable access requests initiated by remote	Optional	33.2.7
Display and maintenance of EFM		Optional	33.2.8

33.2.2 EFM/OAM Basic Configuration

EFM mode of operation is divided into active mode and passive mode, when the EFM function enabled, the Ethernet port started to use the default mode of operation and the establishment of its peer port connected EFM.

Table 231 EFM basic configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-

Table 231 EFM basic configuration

OPERATION	COMMAND	REMARKS
Start EFM	<code>efm</code>	Required By default, EFM is off
EFM mode configuration	<code>efm mode {passive active}</code>	Optional By default, EFM mode to active mode

33.2.3 EFM/OAM Timer Parameter Configuration

EFM connection is established, both ends of the EFM entity will send the information OAMPDU with a time interval to detect whether the connection is normal, the interval is called - the interval to send handshake packets. If one end of the connection timeout EFM entity within an entity does not receive remote EFM sent Information OAMPDU, EFM is considered disconnected.

EFM handshake by adjusting packet transmission interval and the connection timeout, the connection can change the EFM detection accuracy. With configuring OAMPDU remote request message to the response timeout, then discard the message which receiving the later response message to the OAMPDU if the time is out.

Table 232 EFM timer parameter configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-
Configure the interval to send handshake packets EFM	<code>efm pdu-timeout time</code>	Optional The default value is 1s
Configure the connection timeout EFM	<code>efm link-timeout time</code>	Optional The default value is 5s
Response timeout configuration	<code>efm remote-response-timeout time</code>	Optional The default value is 2s

Because EFM connection times out, the local entity will EFM EFM aging and physical connection to the end of the relationship, the EFM connection is broken, so the connection must be greater than the timeout interval to send handshake packets (Recommended for 3 times or more) , otherwise it will lead to EFM connection instability.

33.2.4 Configuring Remote Failure Indication

Table 233 Configure remote failure indication

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-
Start remote failure indication	<code>efm remote-failure {link-fault dying-gasp critical-event}</code>	Optional By default, remote failure indication is enabled

Description:

Remote failure indication function device supports a single-pass function required to detect the local emergency link to the remote event notification, in the single-pass functions are not supported on the device, the local emergency is detected only in the event link end of reporting alarms and can't notify the remote.

33.2.5 Configuring Link Monitoring Capabilities

Table 234 Configure link monitoring capabilities

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-
Start link monitoring capabilities	<code>efm link-monitor {errored-symbol-period errored-frame errored-frame-period errored-frame-seconds}</code>	Optional By default, the link monitoring is enabled
Configure errored-symbol-period event detection cycle	<code>efm link-monitor errored-symbol-period window high win-value1 low win-value2</code>	Optional
Configure errored-symbol-period event detection threshold	<code>efm link-monitor errored-symbol-period threshold high th-value1 low th-value2</code>	Optional
Configure errored-frame event detection cycle	<code>efm link-monitor errored-frame window win-value</code>	Optional
Configure errored-frame event detection threshold	<code>efm link-monitor errored-frame threshold th-value</code>	Optional
Configure errored-frame-period event detection cycle	<code>efm link-monitor errored-frame-period window win-value</code>	Optional
Configure errored-frame-period event detection threshold	<code>efm link-monitor errored-frame-period threshold th-value</code>	Optional

Table 234 Configure link monitoring capabilities

OPERATION	COMMAND	REMARKS
Configure errored-frame-seconds event detection cycle	<code>efm link-monitor errored-frame-seconds window win-value</code>	Optional
Configure errored-frame-seconds event detection threshold	<code>efm link-monitor errored-frame-seconds threshold th-value</code>	Optional

Description:

- errored-symbol-period threshold event detection cycle and a 64-bit integer value, **high** and **low** parameter values, respectively, after the value of the high and low 32-bit, that is, the integer value = **(high * (2 ^ 32)) + low**.

33.2.6 Starting Remote Access Function MIB Variable

Table 235 Start the remote access function MIB variable

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-
Start the remote access function MIB variable	<code>efm variable-retrieval</code>	Optional By default, remote access to MIB variable is enabled

33.2.7 MIB Variable Access Requests Initiated by Remote

Table 236 MIB variable access requests initiated by remote

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter port configuration mode.	<code>interface ethernet device / slot / port</code>	-
Port for the remote device MIB variable value	<code>show efm port port-id-list remote-mib {phyadminstate autonegadminstate}</code>	Optional

Description:

- Only when the port EFM connection has been created, EFM working model is for the proactive mode, the far side far side port supports MIB variable access function to the port on the far end of the MIB variable for initiating the request.
- Currently only supports remote query capability of FEC, FEC mode, port status and port to enable auto-negotiation enabled, the other MIB variables can later be added on demand to achieve.

33.2.8 Display and Maintenance of EFM/OAM

After completing the above configuration, you can use the following command to display the EFM configuration.

Table 237 Display and maintenance of EFM

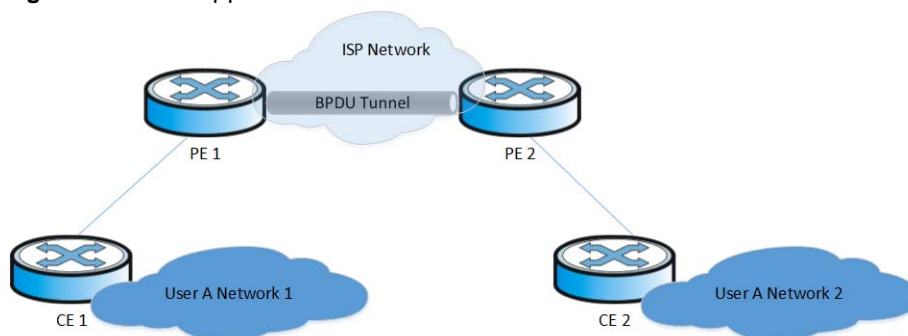
OPERATION	COMMAND	REMARKS
Show EFM protocol running	<code>show efm status interface [interface-name]</code>	Perform either of the commands
Display summary information EFM	<code>show efm summary</code>	
Display EFM find information	<code>show efm discovery interface [interface-name]</code>	
Show EFM protocol packet statistics	<code>show efm statistics interface [interface-name]</code>	
Clear EFM protocol packet statistics	<code>clear efm statistics interface [interface-name]</code>	

L2TP Configuration

34.1 L2TP Overview

L2TP (Layer 2 Tunneling Protocol) is a Layer 2 tunneling technology, L2TP enables Layer 2 protocol packets from geographically dispersed customer networks to be transparently transmitted over specific tunnels across a service provider network.

Figure 67 L2TP application scenario



With L2TP feature, Layer 2 protocol packets from customer networks can be transparently transmitted in the service provider network without being dropped.

- 1 After receiving a Layer 2 protocol packet from User A network 1, PE1 will encapsulate the packet when incoming to the service provider network by replacing its destination MAC address with a specific multicast MAC address, and then forwards the packet to the service provider network.
- 2 The encapsulated Layer 2 protocol packet (called bridge protocol data unit, BPDU for short) is forwarded to PE2 at the other end of the service provider network, which will de-capsulate the packet, that's to restore the original destination MAC address of the packet, and then sends the packet to User A network 2.

34.2 L2TP Configuration

34.2.1 Configure L2-Tunnel Packet

Table 238 Configure the L2-tunnel packet

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enter interface configuration mode	<code>interface ethernet <i>interface-num</i></code>	-
Configure the L2-tunnel packet	<code>l2-tunnel [cdp lacp pagp stp udld vtp]</code>	Required

34.2.2 Advanced L2TP Configuration

By default, L2TP will be up to CPU. This command will configure the rate for up to cpu.

Table 239 Advanced L2TP configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Configure the rate for up to cpu	<code>l2-tunnel drop-threshold [cdp lacp pagp stp udld vtp] <i>rate</i></code>	Optional

34.2.3 L2TP Monitor and Maintenance

After finishing above configuration, user can check the configurations by command below.

Table 240 L2TP monitor and maintenance

OPERATION	COMMAND	REMARKS
Show L2TP configuration	<code>show l2-tunnel interface [ethernet <i>interface-num</i>]</code>	On any configuration mode
Show the rate for up to cpu	<code>show l2-tunnel drop-threshold</code>	On any configuration mode

QinQ Configuration

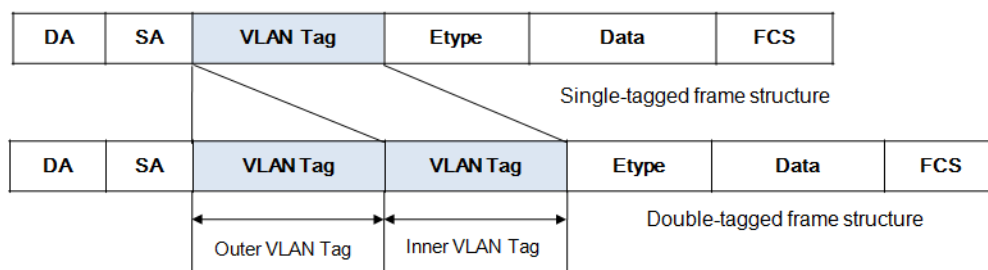
When configuring QinQ, go to these sections for information you are interested in:

- [Introduction to QinQ](#)
- [Implementations of QinQ](#)
- [Configuring QinQ](#)

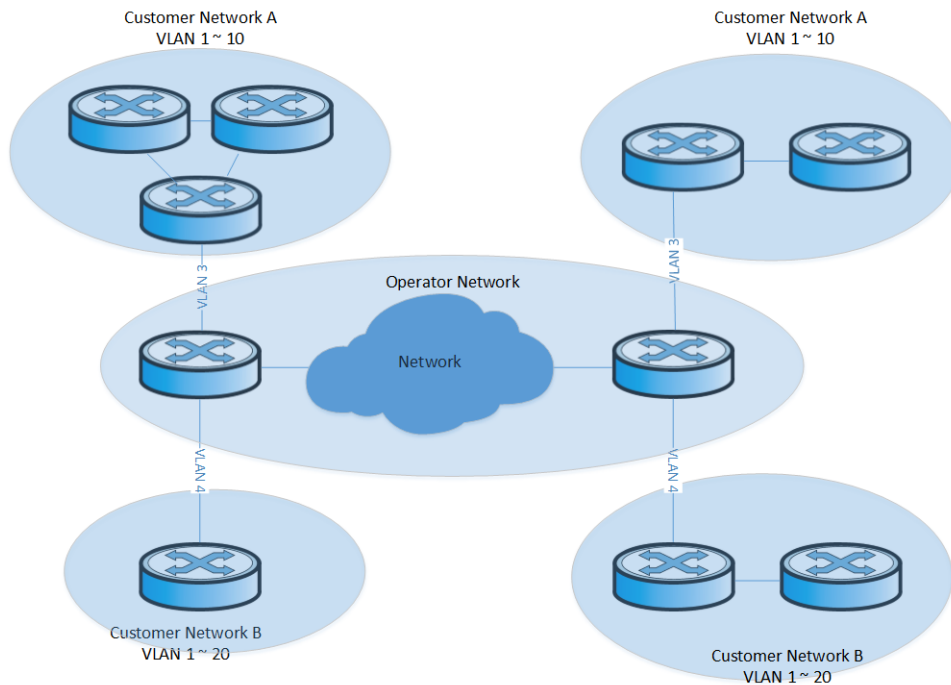
35.1 Introduction to QinQ

In the VLAN tag field defined in IEEE 802.1Q, only 12 bits are used for VLAN ID, so a switch can support maximum 4,094 VLAN. In actual applications, however, a large number of VLAN are required to isolate users, especially in metropolitan area networks (MANs), and 4,094 VLAN are far from satisfying such requirements. Shows the structure of 802.1Q-tagged and double-tagged Ethernet frames. The QinQ feature enables a device to support up to 4,094 x 4,094 VLAN to satisfy the requirement for the amount of VLAN in the MAN.

Figure 68 QinQ Ethernet frame structure



The port QinQ feature is flexible, easy-to-implement Layer 2 VPN technique, which enables the access point to encapsulate an outer VLAN tag in Ethernet frames from customer networks (private networks), so that the Ethernet frames will travel across the service provider's backbone network (public network) with double VLAN tags. The inner VLAN tag is the customer network VLAN tag while the outer one is the VLAN tag assigned by the service provider to the customer. In the public network, frames are forwarded based on the outer VLAN tag only, with the source MAC address learned as a MAC address table entry for the VLAN indicated by the outer tag, while the customer network VLAN tag is transmitted as part of the data in the frames.

Figure 69 QinQ application

TPID (tag protocol identifier) is the field of VLAN tag, IEEE 802.1Q defines the value of this field as 0x8100. The device can identify whether there is corresponded VLAN Tag according to TPID. If configured TPID is the same as the corresponded field, packet is regarded as with VLAN Tag.

The systems of different vendors may set the TPID of the outer VLAN tag of QinQ frames to different values. For compatibility with these systems, the S3750-48 series switches allow you to modify the TPID value so that the QinQ frames, when sent to the public network, carry the TPID value identical to the value of a particular vendor to allow interoperability with the devices of that vendor.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling in the network, you cannot set the TPID value to any of the values in the table below.

Table 241 Reserved protocol type values

PROTOCOL TYPE	VALUE
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

Table 241 Reserved protocol type values

PROTOCOL TYPE	VALUE
GnLink	0x0765
GSTP	0X5524

35.2 Implementations of QinQ

35.2.1 Static QinQ

There are two type for each port: *customer* and *uplink*. When enable dtag, the default value of port type is uplink.

After enabling dtag, if there is no configuration for insert and pass-through rule on each port, the frames are forwarding by static QinQ, the static QinQ forwarding flow following as below:

- Uplink port:

Uplink port decides whether should insert the outer tag by VLAN tag of frames being same as port outer-tpid or not.

- If VLAN first tpid is same as port outer-tpid, then device recognizes as that the frame has outer-tag, and forwards the frame by its outer VLAN tag without inserting the other tag. If the VLAN of the frame outer-tag doesn't exist, the frame wouldn't been forwarded.
- If VLAN first tpid is different with port outer-tpid, device inserts a VLAN tag with port tpid, then forwards it.
- Custom port:

No matter the frames are tagged or untagged, same as outer-tpid or inner-tpid, customer port will insert VLAN tag with port tpid, then forwards the frames by this VLAN tag.

When the frame outgoing from customer port and uplink port, the frame tpid always is same as port outer-tpid.

35.2.2 Dynamic QinQ

- Uplink port cannot configure insert or pass-through rule, the frames forwarding flow is same as static QinQ.
- After customer port determines the frame weather be handled by dynamic QinQ, if the frame doesn't satisfy dynamic QinQ, then the frame is handled by static QinQ or pass-through rule. The following is a determination flow:
 - 1 First, according to the frame tpid and inner-tpid settings, if frame tpid is different with inner-tpid settings, the frame is handled by static QinQ, stacking a VLAN tag with port pvid.
 - 2 If frame tpid is same as inner-tpid settings, but frame VID is not in the range of insert or pass-through rule, then the frame is handled by static QinQ, stacking a VLAN tag with port pvid.
 - 3 If frame tpid is same as inner-tpid settings, and frame VID is in the range of insert rule, then handling the frame under the insert rule.

- 4 If frame tpid is same as inner-tpid settings, and frame VID is in the range of pass-through rule, then handling the frame under the pass-through rule.

35.3 Configuring QinQ

35.3.1 Static QinQ Configuration

Table 242 Static QinQ Configuration

OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable global QinQ	<code>[no] dtag</code>	Required
Enter port mode	<code>interface Ethernet device/slot/port</code>	-
Set port QinQ mode	<code>dtag mode {customer uplink}</code>	Required, default value is uplink
Recovery port QinQ mode to default	<code>no dtag mode</code>	Optional
Show QinQ configuration	<code>show dtag</code>	Any mode

35.3.2 Dynamic QinQ Configuration

Table 243 Dynamic QinQ Configuration

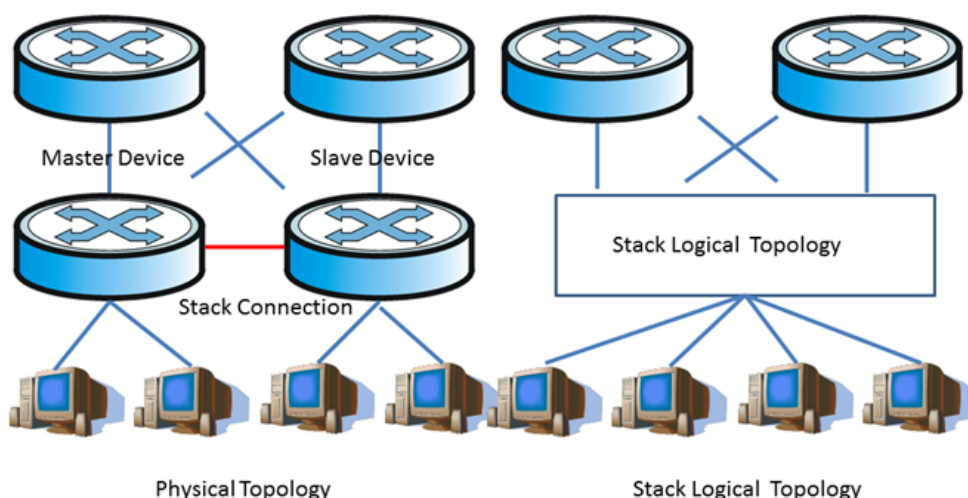
OPERATION	COMMAND	REMARKS
Enter global configuration mode	<code>configure terminal</code>	-
Enable global QinQ	<code>[no] dtag</code>	Required
Enter port mode	<code>interface Ethernet device/slot/port</code>	-
Set port QinQ mode	<code>dtag mode {customer uplink}</code>	Required, default value is uplink
Recovery port QinQ mode to default	<code>no dtag mode</code>	Optional
Set QinQ insert rule	<code>dtag insert start-vlan end-vlan service-vlan</code>	Required, only can set customer port
Delete insert rule	<code>no dtag insert {all start-vlan end-vlan}</code>	Optional
Show QinQ configuration	<code>show dtag</code>	Any mode

Stack Configuration

36.1 Stack Overview

Stack means multiple devices are connected via stack port to form a fictitious logic device, and users perform the management via performing the management on fictitious logic device.

Figure 70 Schematic Diagram of Stack Networking Applications



1 Technical advantages of stack

Stack possesses the following advantages:

- **Network scalability.** At the early stage of the network construction, it uses less devices to build the network and it will expand the port number and bandwidth via adding the stack devices in middle and later periods of the network construction.
- **Reliability.** Stack system is made up by a master device and multiple slave devices. Master device takes the responsibility to finish the administration and maintenance of the stack system whereas slave devices take part in service data processing. If there is something wrong with master device, system will select a new master device to perform the backup job. In addition, physical ports between devices support aggregation function to help to finish the port backup job.
- **Available management.** Any port of any device in stack system can be able to login stack system to perform management configuration, and there is no need to perform separate management configuration on each member device.
- **Low cost on operations and maintenance.** Network upgrading needn't to replace existing devices, just add the new devices will be OK. Multiple devices form a logic device can effectively reduce maintenance cost

2 Stack basic conception

- master-slave devices

There are two types devices in stack system:

Master device is the management device of the stack system.

Slave device. The backup device of the master device and it will be selected as the master device if there is something wrong with the master device.

Master-slave equipment is produced automatically by the system. There is only one master device and multiple slave devices in a stack system.

- Device ID

Each device in the system must be manually specified a non-repeatable to uniquely identify the ID number of this equipment, and the device port is shown as "device ID/ slot number/ port number", for example, "0/0/1" means that device ID is "0", and its slot number is 0 and port number is 1.

All devices in one stack system should not exist the same ID.

The smaller the device ID is, the higher priority it will be.

- Stack port

Devices connect with each other via stack port in stack system. Stack port can use dedicated stack interface or normal device port to perform devices connection.

All device stack port in one stack system should be the same or it cannot form the stack. For example, if SW1 uses port{1,2,3,4} as stack port, SW2 must use port{1,2,3,4} as stack port as a consequence. Or these two DUT cannot form stack.

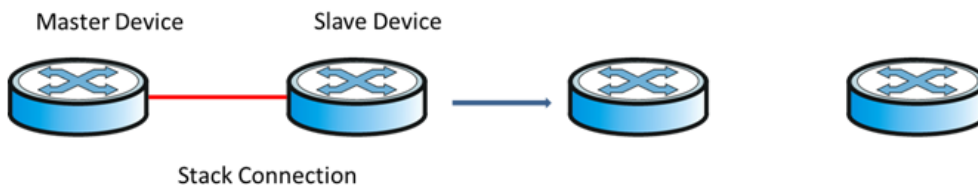
- service port

Other ports are called as service port except stack port.

- Split and merge

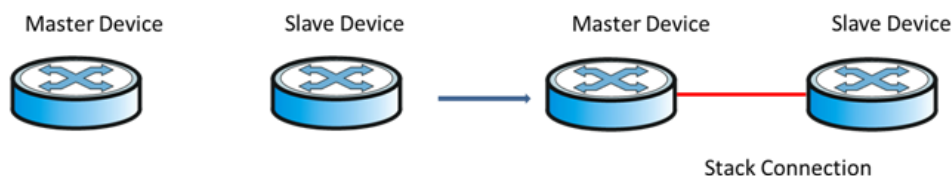
In stack system, it will split two independent stack systems if the device port lose connection.

Figure 71 Schematic Diagram of Stack Split



In reverse, two independent stack systems will be merged in one stack system because of the adding connection of the stack ports.

Figure 72 Schematic Diagram of Stackmerge



3 Stack Topology

Currently, stack can only use the devices with the same capacities to help to form loop topology structure and rectilinear topology structure.

"same capacities" refers to the same software version number and the same hardware type.

4 left-right virtual port

For example, stack is just like few people hand in hand to form a loop or rectilinear figure.

Left-right port is geared to virtual port, forming by one or multiple physical stack port or no physical stack port.

In stack system, stack port must be left-right virtual port connection, that is, the virtual port left-left virtual port connection and right-right virtual port connection are not allowed.

5 Master-Slave Selection

In stack system, there will be a master device of automatic select according to stack protocol, and the other devices will act as slave devices.

To understand the master-slave selection mechanism, you need to understand different stack scenarios:

- Power on the devices at the same time: devices connect with each other via stack port before start up, and then power on at the same time;
- Add the devices which are booting to existing stack system: devices connect to an existing stack system through the stack port, then starts to power on.
- Add the devices which have finished booting to existing stack system: it is geared to stack merge. Devices have finished booting and formed its own stack, and then this stack system will connect with the other system via stack port. Stack merger occurs at this time.
- Re-select slave device: if there is something wrong with the master device or the stack splitting, device needs to re-select a master device.

Selection mechanism is as following:

- Running priority. This rule applies to the situation when the stack is added during boot process. If the device discovers the existing master device during boot process, it will add the existing master device to the stack system as a slave device.
- Number of members. This rule applies to the stack merging situation. In the process of stack merging, the master devices with large number of members will stay to be master device while the master devices with fewer number of members will turn into slave devices.
- Device ID. The device with small device ID will be selected to be master device in the following situation: multiple devices establish stack system at the same time; master device re-selection situation because of master device losing; members of the same number when stack merging.

6 Device mode

stack equipment can work in two different working modes:

- Standalone Mode. It is the same as ordinary switch, that is, it does not offer stack function.
- Stack Profile. This mode can enable stack function as well as to form a stack system with other device.

7 MAD Multi-Active Detection

If there is something wrong with a certain stack link, it will disconnect with Master device while it can still connect with multiple Slave devices and select one of them to be the new Master device. So there will be two or multiple master devices with the same configuration in stack system, and it is the so called Multi-Active.

As to the networking devices in the external stack system, logical devices corresponding to stack system are divided into two or multiple logical devices with the same configuration. Therefore, it will appear network configuration conflict and then lead to transmission confusion between uplink and downlink. For this reason, multi-active arises at the historic moment. Multi-Active can be able to detect stack line fault in the shortest time and then perform duly handle.

Therefore, it asks to ensure the following networking function when stack system splitting:

7a Multi-Active Detection

It judges whether there exists multiple logical devices from one stack system and they are now in **active** state via LACP and BFD.

7b Conflict resolution

After stack system splitting, it will be detected that there are multiple logical devices are in active state via multi-activedetection mechanism. Conflict resolution will make the logical device with the highest ActivePriority continue the regular work (remain *Active* state) while the other logical devices will be moved to *Recovery* state (Disable state) via a certain election algorithm. When the logical devices are in the *Recovery* state, it will perform Recovery Action: disabled VLAN interface (except the saving-port) and all service port which are in the Recovery state to ensure the logical devices completely disconnected with the network.

7c Failure recovery

Stack system reminder user to restore the stack link by log record. After restoring the stack link, conflicting equipment will reboot and then restore the stack system. At the same time, the closed port will also restore the service transmission.

Note: In MAD, use device-id as activePriority; save the small id number as active state, and the other as recovery state.

36.2 Overview for Stack Configuration

Table 244 Overview for Stack Configuration

CONFIGURATION TASK		DESCRIPTION	DETAILED CONFIGURATION
stack basic configuration	Stand-Alone Mode Configuration	optional	36.3.1
	Stack Mode Configuration	required	36.3.2
	LACP Multi-Active Detection	required	36.3.4
	BFD Multi-Active Detection	required	36.3.6

36.3 Stack

36.3.1 Stand-Alone Mode Configuration

Table 245 Stand-Alone Mode Configuration

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Configure stack	<code>[no] stack</code>	required
Configure device ID	<code>stack device-id value</code>	required

Table 245 Stand-Alone Mode Configuration

OPERATION	COMMAND	REMARK
configure stack port	[no] stack { left-port right-port } port-num	required
Configure device priority	[no] stack priority value	optional
Display stack information	show stack	optional

Note: 1. Stack function will go into effect after rebooting. Except for debug configuration, all stack configuration will be written into Flash and will not shown in show running;

2. Stack configuration cannot be deleted via the command of clear startup-config, and it should be use the command of no command to delete one by one.

36.3.2 Stack Mode Configuration

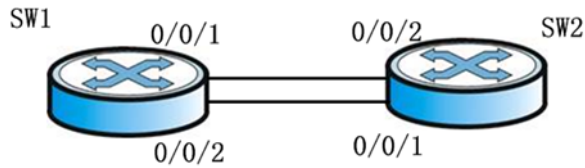
Table 246 Stack Mode Configuration

OPERATION	COMMAND	REMARK
Enter global configuration mode	configure terminal	-
Configure device ID	stack device-id <0-3>	optional
Configure stack port	[no] stack { left-port right-port } port-num	optional
Configure device priority	[no] stack priority value	optional
Display stack information	show stack	optional
Configure stack debug function	[no] stack debug { all default error event packet packet-detail smd smd-msg state }	optional
Display stack debug function configuration	show stack debug	optional
Display stack member information	show stack members device-id	optional
Display stack neighbor information	show stack neighbors	optional
Display statistical information of stack packet	show stack statistic	optional
Configure keeping active time	[no] stack hello-timeout value	optional
Configure detection delay	[no] stack linkdown-delay	optional
Enter privileged mode	exit	required
Reboot and designate member	reboot device-id	optional

36.3.3 Stack Configuration Examples

1 Network Requirements

It is shown as following. SW1 acts as Master, and SW2 acts as Slave.

Figure 73 Schematic Diagram of Stack Networking

2 Configuration procedure

```

#SW1 configuration:
# enabel stack
SW1(config)#stack
# configure device-id, 0 by default, SW1 is optional to modify;
SW1(config)#stack device-id 0
# configure SW1 left-port
SW1(config)#stack left-port 0/0/1
SW1(config)#stack left-port 0/0/2
# configure the priority of SW1
SW1(config)#stack priority 200
# reboot. Reboot to bring stack into effect
SW1(config)#ex
SW1#reboot

#SW2 configuration
SW2(config)#stack
SW2(config)#stack device-id 1
SW2(config)#stack right-port 0/0/1
SW2(config)#stack right-port 0/0/2
SW2(config)#stack priority 100
SW2(config)#exit
SW2#reboot

```

3 Verification result

After two switches rebooting, perform the connect operation according to network construction. SW2 will be selected as Slave and it will be reboot. After rebooting, the stack light of Master device will keep coruscating whereas the stack light of Slave device will keep bum steady. All configurations can only be performed in Master device.

3a stack system port information after finishing the stack:

```

SW1(config)#show interface brief

```

Port	Desc	Link	shutdn	Speed	Pri	PVID	Mode	TagVlan	UtVlan
e0/0/3		down	false	auto	0	1	hyb		1
e0/0/4		down	false	auto	0	1	hyb		1
e0/0/5		down	false	auto	0	1	hyb		1
e0/0/6		down	false	auto	0	1	hyb		1
e0/0/7		down	false	auto	0	1	hyb		1
.....									
e1/0/1		down	false	auto	0	1	hyb		1
e1/0/2		down	false	auto	0	1	hyb		1
e1/0/3		down	false	auto	0	1	hyb		1
e1/0/4		down	false	auto	0	1	hyb		1
e1/0/5		down	false	auto	0	1	hyb		1

3b Display all stack members' information

```
SW1(config)#show stack members
Informations of stack devices:
switch 1 <local>
  macaddress 00:01:7a:fd:ef:2d device id 0 priority 200
  master device left hops 0 right hops 0
  stack identity fdef2d003e4a
  it's master device 00:01:7a:fd:ef:2d device id 0

switch 2
  macaddress 00:01:7a:fd:ee:d2 device id 1 priority 100
  slave device left hops 1 right hops infinite
  stack identity fdef2d003e4a
  it's master device 00:01:7a:fd:ef:2d device id 0

Total entries: 2
```

3c Display all neighbors' information

```
SW1(config)#show stack neighbors
Informations of neighbor devices:
switch 1 <local>
  macaddress 00:01:7a:fd:ef:2d device id 0 priority 200
  master device left hops 0 right hops 0
  stack identity fdef2d003e4a
  it's master device 00:01:7a:fd:ef:2d device id 0

switch 2
  macaddress 00:01:7a:fd:ee:d2 device id 1 priority 100
  slave device left hops 1 right hops infinite
  stack identity fdef2d003e4a
  it's master device 00:01:7a:fd:ef:2d device id 0

Total entries: 2
```

3d establish vlan?and then add members:

```
SW1(config)#vlan 100
SW1(config-if-vlan)#sw e 0/0/3 e 1/0/3
SW1(config-if-vlan)#show vlan 100
show VLAN information
VLAN ID          : 100
VLAN status      : static
VLAN member      : e0/0/3,e1/0/3.
Static tagged ports :
Static untagged Ports : e0/0/3,e1/0/3.
Dynamic tagged ports :

Total entries: 1 vlan.
```

3e upgrade stack system:

```
SW1#load application tftp inet 192.168.1.99 host.arj
Downloading application via TFTP...
  Master device 0 operation complete, successful.
  Slave device 1 operation complete, successful.
Download application via TFTP successfully.
```

36.3.4 LACP MAD

Table 247 Display LACP MAD settings

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Enable lacp mad	<code>[no] channel-group <i>value</i> lacp mad</code>	required
Configure lacp mad domain	<code>[no] lacp mad domain <i>value</i></code>	optional
Display lacp mad information	<code>show lacp mad</code>	optional

Table 248 LACP MAD relay device configuration

OPERATION	COMMAND	REMARK
Enter global configuration mode	<code>configure terminal</code>	-
Configure LACP expansion field	<code>channel-group <i>group-id</i> lacp mad</code>	required
Display LACP expansion field	<code>show lacp extend-tlv-relay</code>	optional

Table 249 Configure MAD to save the port

OPERATION	COMMAND	REMARK
port configuration mode	<code>interface ethernet <i>port-num</i></code>	-
Configure mad to save the port	<code>[no] stack mad exclude</code>	required
Display port configuration	<code>show stack mad exclude interface [ethernet <i>port-num</i>]</code>	optional

Note: LACP MAD only supports dynamic lacp;

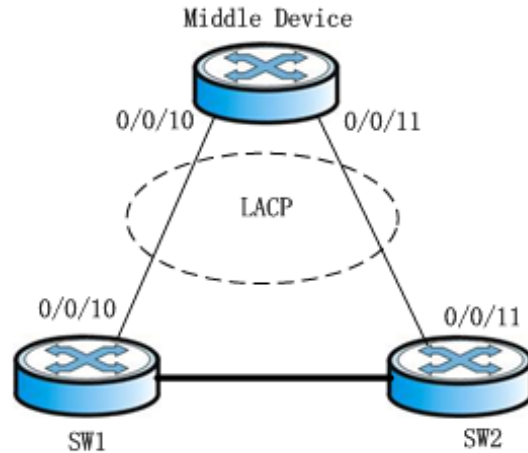
LACP MAD relay device should be able to support LACP expansion field, or it can not take effect;

LACP MAD configuration will not be written in Flash directly;

36.3.5 LACP MAD Configuration Instance

1 Network requirements

Shown as follow. Two SW form stack system, construct network with the other SW via LACP.

Figure 74 LACP MAD Schematic Diagram

2 configuration procedure

stack configuration (please refer to stack configuration content for more details)

configure dynamic LACP

```
SW1(config)# interface range ethernet 0/0/10 ethernet 1/0/10
```

```
SW1(config-if-ethernet-0/0/10)#channel-group 1 mode active
```

configure LACP MAD in stack system

enable lacp mad

```
SW1(config)#channel-group 1 lacp mad
```

configure mad domain (optional configuration, 255 by default)

```
SW1(config)#lacp mad domain 200
```

configure the port (optional)

```
SW1(config)#in e 0/0/12
```

```
SW1(config-if-ethernet-0/0/10)#stack mad exclude
```

configure LACP extension field in relay device configuration

```
MilddleDUT#configure terminal
```

```
MilddleDUT (config)# interface ethernet 0/0/10
```

```
MilddleDUT (config-if-ethernet-0/0/10)#channel-group 1 mode active
```

```
MilddleDUT (config-if-ethernet-0/0/10)#ex
```

```
MilddleDUT(config)#channel-group 1 extend-info-relay
```

3 verification result:

```

SW1(config)# logging monitor 0
SW1(config)#debug link_aggregation
SW1(config)#debug stack
    # manually disconnect all the stack line;
00:26:06: SW1: %stack-5-state: stack port 1/0/1 link down
00:26:08: SW1: %stack-5-state: stack port 0/0/1 link down
00:26:08: SW1: %stack-5-state: isf_devinfo_timeout_hello:device 1 leave stack mac
00:01:7a:fd:ee:d2
    # the MAD which has been detected ;
00:26:08: SW1: %LINK_AGGREGATION-7-isfMad: A multi-active conflict detected on
channel group 1(local ActiveId = 0, peer ActiveId = 1).
    # only save and linkup port and lacp mad port, shutdown the other ports
SW1(config)#show interface brief
Port      Desc      Link shutdn Speed          Pri PVID Mode TagVlan    UtVlan
e0/0/3          down false  auto              0   1   hyb         1
e0/0/4          down false  auto              0   1   hyb         1
e0/0/5          down false  auto              0   1   hyb         1
e0/0/6          down false  auto              0   1   hyb         1
e0/0/7          down false  auto              0   1   hyb         1
e0/0/8          down false  auto              0   1   hyb         1
e0/0/9          down false  auto              0   1   hyb         1
e0/0/10         up   false  auto-f1000        0   1   hyb         1
e0/0/11         down false  auto              0   1   hyb         1
e0/0/12         up   false  auto-f1000        0   1   hyb         1
e0/0/13         down false  auto              0   1   hyb         1
e0/0/14         down false  auto              0   1   hyb         1
.....
e0/0/21         down false  auto              0   1   hyb         1
e0/0/22         down false  auto              0   1   hyb         1
e0/0/23         down false  auto              0   1   hyb         1
Total entries: 50 .

```

Note: All the above are just to demonstrate the effect, the actual use don't need to open the debug.

36.3.6 BFD MAD**Table 250** DisplayBFD MAD settings

OPERATION	COMMAND	REMARK
enter global configuration mode	configure terminal	-
enable/disable bfd	bfd { enable disable }	required
establish BFD layer-3 interface	interface vlan-interface <i>vlan-id</i>	optional
disable STP	no spanning-tree	required
Configure member ip of mad detection	[no] mad device-id <0-3> ip address <i>A.B.C.D mask</i>	required
enable/disable mad bfd	mad bfd {enable disable}	required
Display mad bfd information	show mad bfd	optional
Display bfd session information	show bfd session	optional

Table 251 Configure MAD to save the port

OPERATION	COMMAND	REMARK
port configuration mode	<code>interface ethernet <i>port-num</i></code>	-
Configure mad to save the port	<code>[no] stack mad exclude</code>	required
Display port configuration	<code>show stack mad exclude interface [ethernet <i>port-num</i>]</code>	optional

Note: 1. BFD MAD port asks to disable the spanning tree to avoid detection failure on account of the port in Blocking state and then discard the BFD packet.

2. It asks to use BFD VLAN to isolate MAD port and the other ports so as to avoid the storm.

3. BFD MAD has no requirement on VLAN type of detection port (Access/Trunk/Hybrid) while it requires to ensure the VLAN connectivity.

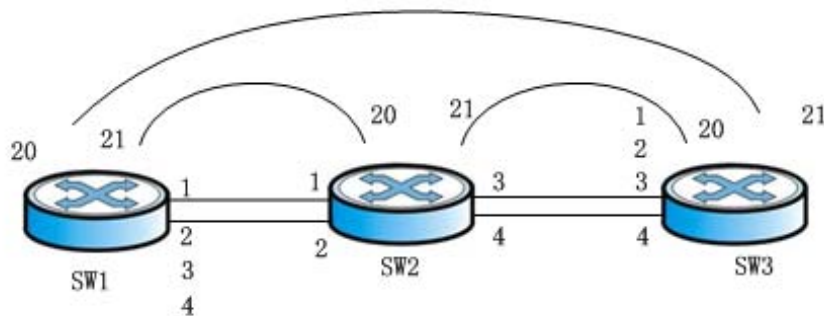
4. It asks to use the command of mad member member-id ip address to configure MAD IP address. Remember do not configure other IP addresses (for example, use the command of ip address to configure normal IP address, interface IP address, VRRP vlan IP address, etc) for fear that it will affect MAD function.

5. It asks to ensure the mesh connection of all stack members when BFD MAD do not use relay device to construct networking; it asks to ensure each member has connected with relay device when using relay device to construct networking.

36.3.7 BFD MAD Configuration Examples

1 Network requirements

Networking is shown as following:

Figure 75 Bfd Mad Schematic Diagram

2 configuration procedure

```
# stack configuration:
SW1(config)#stack
SW1(config)#stack priority 200
SW1(config)#stack device-id 0
SW1(config)#stack left-port 0/0/3
SW1(config)#stack left-port 0/0/4
SW1(config)#stack right-port 0/0/1
SW1(config)#stack right-port 0/0/2

SW2(config)#stack
SW2(config)#stack priority 190
SW2(config)#stack device-id 1
SW2(config)#stack left-port 0/0/1
SW2(config)#stack left-port 0/0/2
SW2(config)#stack right-port 0/0/3
SW2(config)#stack right-port 0/0/4

SW3(config)#stack
SW3(config)#stack priority 170
SW3(config)#stack device-id 2
SW3(config)#stack left-port 0/0/3
SW3(config)#stack left-port 0/0/4
SW3(config)#stack right-port 0/0/1
SW3(config)#stack right-port 0/0/2

#MAD BFD port configuration: using vlan100 interface to perform the MAD detect with
each SW 20 and SW 21 port, and then save the BFD port;
SW1(config)#vlan 100
SW1(config-if-vlan)#switchport ethernet 0/0/20 to ethernet 0/0/21
SW1(config-if-vlan)#switchport ethernet 1/0/20 to ethernet 1/0/21
SW1(config-if-vlan)#switchport ethernet 2/0/20 to ethernet 2/0/21
SW1(config-if-vlan)#interface range ethernet 0/0/20 ethernet 0/0/21
SW1(config-if-range)#switchport default vlan 100
SW1(config-if-range)#no spanning-tree
SW1(config-if-range)#stack mad exclude
SW1(config-if-range)#interface range ethernet 1/0/20 ethernet 1/0/21
SW1(config-if-range)#switchport default vlan 100
SW1(config-if-range)#no spanning-tree
SW1(config-if-range)#stack mad exclude
SW1(config-if-range)#interface range ethernet 2/0/20 ethernet 2/0/21
SW1(config-if-range)#switchport default vlan 100
SW1(config-if-range)#no spanning-tree
SW1(config-if-range)#stack mad exclude

#MAD BFD configuration
SW1(config)#interface vlan-interface 100
SW1(config-if-vlanInterface-100)#mad bfd enable
SW1(config-if-vlanInterface-100)#mad device-id 0 ip address 20.20.20.20
255.255.255.0
SW1(config-if-vlanInterface-100)#mad device-id 1 ip address 20.20.20.21
255.255.255.0
SW1(config-if-vlanInterface-100)#mad device-id 2 ip address 20.20.20.22
255.255.255.0
```

3 verification result

3a when under normal circumstances, BFD session state will be as following:

```
SW1(config)#show bfd session
Total Session Num: 2
Init Mode: Active
Session Working Under Asynch Mode
LD          SourceAddr      DestAddr      State      Holdtime Interface
0x0add68e8  20.20.20.20          20.20.20.21   DOWN       0ms  Vlan100
Init Mode: Active
Session Working Under Asynch Mode
LD          SourceAddr      DestAddr      State      Holdtime Interface
0x0add699c  20.20.20.20          20.20.20.22   DOWN       0ms  Vlan100
```

3b manually disconnect all the STACK line between SW2 and SW3, the conflict that BFD MAD has detected will be shown as following:

```
SW1(config)#s bfd session
Total Session Num: 2
Init Mode: Active
Session Working Under Asynch Mode
LD          SourceAddr      DestAddr      State      Holdtime Interface
0x0add68e8  20.20.20.20          20.20.20.21   DOWN       0ms  Vlan100
Init Mode: Active
Session Working Under Asynch Mode
LD          SourceAddr      DestAddr      State      Holdtime Interface
0x0add699c  20.20.20.20          20.20.20.22   UP         1890ms Vlan100
```

3c enter SW3, the state that stack handles recovery will be shown:

```
SW1(config)#show stack
Config in flash:
  enable stack, device id is 2, priority is 200
  left port  2/0/3 2/0/4
  right port  2/0/1 2/0/2

Config in running:
  enable stack, device id is 2, priority is 170
  left port  2/0/3 2/0/4
  right port  2/0/1 2/0/2

Local device is master devcie, state is STATE_MASTER

Linkdown-delay is FALSE, hello-timeout is 30

Mad status: recovery

Left-port load-sharing mode: source port
Right-port load-sharing mode: source port

Infomation of stack port:
  stack port 2/0/1 is link down speed is unknown
  stack port 2/0/2 is link down speed is unknown
  stack port 2/0/3 is link down speed is unknown
  stack port 2/0/4 is link down speed is unknown
```

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See <http://www.zyxel.com/homepage.shtml> and also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Asia

China

- ZyXEL Communications (Shanghai) Corp.
- ZyXEL Communications (Beijing) Corp.
- ZyXEL Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- ZyXEL Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- ZyXEL Kazakhstan
- <http://www.zyxel.kz>

Korea

- ZyXEL Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- ZyXEL Philippines
- <http://www.zyxel.com.ph>

Singapore

- ZyXEL Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com/tw/zh/>

Thailand

- ZyXEL Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- ZyXEL BY
- <http://www.zyxel.by>

Belgium

- ZyXEL Communications B.V.
- <http://www.zyxel.com/be/nl/>
- <http://www.zyxel.com/be/fr/>

Bulgaria

- ZyXEL България
- <http://www.zyxel.com/bg/bg/>

Czech Republic

- ZyXEL Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- ZyXEL Communications A/S
- <http://www.zyxel.dk>

Estonia

- ZyXEL Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- ZyXEL Communications
- <http://www.zyxel.fi>

France

- ZyXEL France
- <http://www.zyxel.fr>

Germany

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- ZyXEL Hungary & SEE
- <http://www.zyxel.hu>

Italy

- ZyXEL Communications Italy
- <http://www.zyxel.it/>

Latvia

- ZyXEL Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- ZyXEL Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- ZyXEL Benelux
- <http://www.zyxel.nl>

Norway

- ZyXEL Communications
- <http://www.zyxel.no>

Poland

- ZyXEL Communications Poland
- <http://www.zyxel.pl>

Romania

- ZyXEL Romania
- <http://www.zyxel.com/ro/ro>

Russia

- ZyXEL Russia
- <http://www.zyxel.ru>

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- ZyXEL Communications ES Ltd
- <http://www.zyxel.es>

Sweden

- ZyXEL Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG

- <http://www.zyxel.ch/>

Turkey

- ZyXEL Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- ZyXEL Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- ZyXEL Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Brazil

- ZyXEL Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Ecuador

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Israel

- ZyXEL Communication Corporation
- <http://il.zyxel.com/homepage.shtml>

Middle East

- ZyXEL Communication Corporation
- <http://www.zyxel.com/me/en/>

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- <http://www.zyxel.com/us/en/>

Oceania

Australia

- ZyXEL Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

Legal Information

Copyright

Copyright © 2016 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- 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 his own expense.

Canada

The following information applies if you use the product within Canada area.

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union



The following information applies if you use the product within the European Union.

CE EMC statement

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

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Caution: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- This device must be grounded. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.

Environment Statement

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.



















Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



Environmental Product Declaration

Български (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
Екологична продуктова декларация RoHS Директива 2011/65/EC WEEE Директива 2012/19/EC PPW Директива 94/62/EC REACH РЕГЛАМЕНТ (ЕО) № 1907/2006 Име/ : Richard Hsu / Quality Management titlu : Division Senior Manager Подпис : Дата (dd/mm/yyyy): 01/10/2014  	Environmentální prohlášení o produktu RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/62/ES REACH Nařízení (ES) č. 1907/2006 Jméno/ : Richard Hsu / Quality Management titul : Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014  	Miljøvederklæring RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 Navn/ : Richard Hsu / Quality Management titel : Division Senior Manager Underskrift : Dato (dd/mm/åååå): 01/10/2014  	Produkt-Umweltdeklaration RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/62/EG REACH VERORDNUNG (EG) Nr. 1907/2006 Name/ : Richard Hsu / Quality Management titel : Division Senior Manager Unterschrift : Datum (gg/mm/jj): 2014/10/01  
Eesti keel (Estonian) Toote keskkonnadeklaratsioon RoHS Direktiiv 2011/65/EL WEEE Direktiiv 2012/19/EU PPW Direktiiv 94/62/EU REACH MÄÄRUS (EÜ) nr 1907/2006 Nimil/ : Richard Hsu / Quality Management pealkiri : Division Senior Manager Allkiri : Kuupäev (pp/kk/aaaa): 01/10/2014  	English Environmental product declaration RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/62/EC REACH Regulation (EC) No 1907/2006 Name/ : Richard Hsu / Quality Management title : Division Senior Manager Signature : Date (dd/mm/yyyy): 01/10/2014  	Español (Spanish) Declaraciones Ambientales de Producto RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGLAMENTO (CE) nº 1907/2006 Nombre/ : Richard Hsu / Quality Management título : Division Senior Manager Firma : Fecha (aaaa/mm/dd): 2014/10/01  	Français (French) Profil environnemental de produit RoHS Directive 2011/65/UE WEEE Directive 2012/19/UE PPW Directive 94/62/CE REACH REGLEMENT (CE) N° 1907/2006 Nom/ : Richard Hsu / Quality Management titre : Division Senior Manager Signature : Date (aaaa/mm/jj): 2014/10/01  
Hrvatski (Croatian) Deklaraciju o zbrinjavanju proizvoda RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/EZ REACH Uredbe (EZ) br. 1907/2006 Ime/ : Richard Hsu / Quality Management naslov : Division Senior Manager Potpis : Datum (dd/mm/yyyy): 01/10/2014  	Italiano (Italian) Dichiarazione ambientale di prodotto RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) n. 1907/2006 Nome/ : Richard Hsu / Quality Management titolo : Division Senior Manager Firma : Data (aaaa/mm/gg): 2014/10/01  	Latviešu valoda (Latvian) Produkta vides ietekmējuma deklarācija RoHS Direktīva 2011/65/ES WEEE Direktīva 2012/19/ES PPW Direktīva 94/62/EK REACH Regula (EK) Nr. 1907/2006 Nosaukums : Richard Hsu / Quality Management s/ tituls : Division Senior Manager Paraksts : Datums (dd/mm/gggg): 01/10/2014  	Lietuvių kalba (Lithuanian) Aplinkosauginę gaminių deklaraciją RoHS Direktyva 2011/65/ES WEEE Direktyva 2012/19/ES PPW Direktyva 94/62/EB REACH REGLAMENTAS (EB) Nr. 1907/2006 Vardas/ : Richard Hsu / Quality Management titulas : Division Senior Manager Parašas : Data (aaaa/mm/mmm): 01/10/2014  
Magyar (Hungarian) Környezetvédelmi terméknyilatkozatot RoHS 2011/65/EU irányelve WEEE 2012/19/EU irányelve PPW 94/62/EK irányelve REACH 1907/2006/EK Rendelet Név/ : Richard Hsu / Quality Management cím : Division Senior Manager Aláírás : Dátum (éééé/hh/nn): 2014/10/01  	Malta (Maltese) Dikjarazzjoni Ambjentali dwar il-Prodott RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/KE REACH REGOLAMENTO (KE) NRU 1907/2006 Isem/ : Richard Hsu / Quality Management titolu : Division Senior Manager Firma : Data (ssss/xx/jj): 2014/10/01  	Nederlands (Dutch) Milieuproduktverklaring RoHS Richtlijn 2011/65/EU WEEE Richtlijn 2012/19/EU PPW Richtlijn 94/62/EG REACH Verordening (EG) nr. 1907/2006 Naam/ : Richard Hsu / Quality Management titel : Division Senior Manager Handtekening : Datum (dd/mm/jaar): 01/10/2014  	Polski (Polish) Deklarację środowiskową produktu RoHS Dyrektywa 2011/65/UE WEEE Dyrektywa 2012/19/UE PPW Dyrektywa 94/62/WE REACH Rozporządzenie (WE) nr 1907/2006 Nazwisko : Richard Hsu / Quality Management tytuł : Division Senior Manager Podpis : Data (rrr/mm/vdd): 2014/10/01  
Português (Portuguese) Declaração ambiental do produto RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH Regulamento (CE) n.º 1907/2006 Nome/ : Richard Hsu / Quality Management título : Division Senior Manager Assinatura : Data (dd/mm/aaaa): 01/10/2014  	Română (Romanian) Declarație de mediu privind produsele RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGULAMENTUL (CE) NR 907/2006 Numele/ : Richard Hsu / Quality Management titlu : Division Senior Manager Semnătura : Data (zz/ll/aaaa): 01/10/2014  	Slovenčina (Slovak) Vyhlasenie o environmentálnom výrobku RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EU PPW Smernica 94/62/ES REACH Nariadenie (ES) č. 1907/2006 Meno/ : Richard Hsu / Quality Management titul : Division Senior Manager Podpis : Datum (dd/mm/yyyy): 01/10/2014  	Slovenščina (Slovene) Okoljsko deklaracijo izdelka RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/ES REACH Uredba (ES) št. 1907/2006 Ime/ : Richard Hsu / Quality Management naziv : Division Senior Manager Podpis : Datum (dd/mm/lllll): 01/10/2014  
Suomi (Finnish) Standardiin perustuva ympäristötutusteloste RoHS Direktiivi 2011/65/EU WEEE Direktiivi 2012/19/EU PPW Direktiivi 94/62/EY REACH ASETUS (EY) N:o 1907/2006 Nimil/ : Richard Hsu / Quality Management otsikko : Division Senior Manager Allekirjoitus : Päivämäärä (pp/kk/vvvv): 01/10/2014  	Svenska (Swedish) Miljöproduktdeklaration RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EG REACH Förordning (EG) nr 1907/2006 Namn/ : Richard Hsu / Quality Management titel : Division Senior Manager Namnteckning : Datum (dd/mm/åååå): 01/10/2014  	Ελληνικά (Greek) Περιβαλλοντική δήλωση προϊόντος RoHS Οδηγία 2011/65/ΕΕ WEEE Οδηγία 2012/19/ΕΕ PPW Οδηγία 94/62/ΕΚ REACH Κανονισμός (ΕΚ) αριθ. 1907/2006 Άνωμο/ : Richard Hsu / Quality Management τίτλος : Division Senior Manager Υπογραφή : Ημερομηνία (ηη/μμ/εεεε): 01/10/2014  	Norsk (Norwegian) Miljødeklarasjon RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 Navn/ : Richard Hsu / Quality Management tittel : Division Senior Manager Signatur : Dato (dd/mm/åååå): 01/10/2014  

台灣

警告使用者：

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。」





安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則
 - 先連接電源線至設備連，再連接電源。
 - 先斷開電源再拔除連接至設備的電源線。
 - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of

purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (ZyXEL Network Operating System) and ZON (ZyXEL One Network) are registered trademarks of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index of Commands

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

wins primary-ip ipaddress	107
(no) garp permit vlan vlan-list	71
(no) gvrp	70
(no) spanning-tree	182
(no) spanning-tree mst portfast	184
(no)alarm all-packets	48
(no)alarm all-packets	48
(no)alarm cpu	49
(no)spanning-tree	149
[brief [ethernet interface-list]	187
[no] dtag	264
[no] dtag	264
[no] mad device-id <0-3> ip address A.B.C.D mask	274
[no] ssh	194
[no] stack	268
[no] stack { left-port right-port } port-num	269
[no] stack { left-port right-port } port-num	269
[no] stack debug { all default error event packet packet-detail smd smd-msg state }	269
[no] stack hello-timeout value	269
[no] stack linkdown-delay	269
[no] stack mad exclude	272
[no] stack mad exclude	275
[no] stack priority value	269
[no] stack priority value	269
{ interface device/slot/port_2 channel-group channel-group-number_2 } preemption mode { Forced Bandwidth Off }	241
{ interface device/slot/port_2 channel-group channel-group-number_2 } preemption mode <1-60> 241	
{ permit deny } [protocol] [cos vlan-pri] ingress { { [source-vlan-id] [source-mac- addr source-mac-wildcard] [interface interface- num] } any } egress { { [dest-mac- addr dest-mac-wildcard] [interface interface-num cpu] } any } [time-range name]	124
{ permit deny } [protocol] [established] { source-IPv4/v6 source-wildcard any ipv6any } [source-port wildcard] { dest-IPv4/v6 dest-wildcard any ipv6any } [dest-port wildcard] [icmp-type icmp-code] [igmp-type] [traffic-class traffic-class] [[prece- dence precedence] [tos tos] [dscp dscp]] [fragments] [time-range name] 122	
{ permit deny } { source-IPv4/v6 source- wildcard any ipv6any } [time-range name] 120	
{acct-secret-key auth-secret-key} key	32
{load upload} keyfile {private public} FTP inet A.B.C.D file_name Username Password 194	
{load upload} keyfile {private public} TFTP inet A.B.C.D file_name	194
{primary-acct-ip primary-auth-ip } A.B.C.D { accounting port authentication port } 32	
aaa	163
aaa	163
aaa	163
aaa	164
aaa	32
absolute start HH:MM:SS YYYY/MM/DD [end HH:MM:SS YYYY/MM/DD]	118
access-group [ip-group name num] [subitem num] [link-group name num] [subitem num] 125	
access-group [ip-group name num] [subitem num] [link-group name num] [subitem num] 125	

access-limit { enable number disable }	164
access-list extended name	121
access-list extended name match-order { config auto }	121
access-list link name	124
access-list link name match-order { config auto }	124
access-list num { permit deny } [protocol] [cos vlan-pri] ingress { { [source-vlan-id] [source-mac-addr source-mac-wildcard] [interface interface-num] } any } egress { { [dest-mac-addr dest-mac-wildcard] [interface interface-num cpu] } any } [time-range name]	124
access-list num { permit deny } [protocol] [established] { source-IPv4/v6 source-wildcard any ipv6any } [port [portmask]] { dest- IPv4/v6 dest-wildcard any ipv6any } [port [portmask]] { [precedence precedence] [tos tos] [dscp dscp] } [time-range name]	121
access-list num { permit deny } { source-IPv4/v6 source-wildcard any ipv6any } [time-range name]	120
access-list num match-order { config auto }	120
access-list num match-order { config auto }	121
access-list num match-order { config auto }	123
access-list standard name	120
access-list standard name match-order { config auto }	120
accounting-on { enable sen-num disable }	164
acct -secret-key keystring	163
alarm all-packets threshold {exceed threshold normal threshold }	48
alarm cpu	219
alarm cpu threshold [busy busy] [unbusy unbusy]	219
alarm cpu threshold <busy unbusy> busy_threshold_value unbusy unbusy_threshold_value	49
anti-dos ip fragment maxnum	219
arp {ipaddress mac mac }	79
arp {ipaddress mac mac vid vid port port }	79
arp aging-time aging-time	79
arp anti-flood	85
arp anti-flood action {deny-arp deny-all} threshold threshold	85
arp anti-flood recover {H:H:H:H:H:H all}	85
arp anti-flood recover-time time	85
arp anti-flood threshold threshold	85
arp anti-spoofing	82
arp anti-spoofing	83
arp anti-spoofing unknown {diacard flood}	83
arp anti-spoofing unknown {diacard flood}	83
arp anti-spoofing valid-check	83
arp anti-spoofing valid-check	83
arp bind dynamic {ipaddress all}	79
arp overwrite	79
arp peer {ipaddress mac port}	79
arp probe [poll-timer value retransmit {count value interval value }]	81
arp probe ip {ip}	80
arp-proxy	81
arp-proxy broadcast	81
arp-reply-repeat	80
arp-reply-repeat interval interval times times	80
auth-secret-key keystring	163
bandwidth egress target-rate	134
bandwidth ingress target-rate	134
bfd { enable disable }	274
buildrun mode {stop continue}	199
cfm cc interval {1 10 60 600}	233
cfm eth-2dm mep mep-id { dst-mac mac-address dst-mep rmep-id } [timeout pkt-time priority priority-identifier interval second count packet-num]	235
cfm eth-slm mep mep-id { dst-mac mac-address dst-mep rmep-id } [timeout pkt-time priority	

priority-identifier interval second count packet-num]	234
cfm linktrace mep mep-id {dst-mac mac-address dst-mep rmep-id} [timeout pkt-time ttl pkt-ttl flag {use-mpdb unuse-mpdb}]	234
cfm loopback mep mep-id {dst-mac mac-address dst-mep rmep-id} [priority pri-id count pkt-num length data-len data pkt-data]	233
cfm ma format {primary-vid string uint16 vpn-id} name ma-name primary-vlan vlan-id	231
cfm ma ma-index	231
cfm ma ma-index	231
cfm ma ma-index	232
cfm ma ma-index	232
cfm ma ma-index	233
cfm ma ma-index	233
cfm ma ma-index	233
cfm ma ma-index	234
cfm ma ma-index	234
cfm ma ma-index	235
cfm md format {dns-name mac-uint string} name md-name level md-level	231
cfm md format none level md-level	231
cfm md md-index	230
cfm md md-index	231
cfm md md-index	231
cfm md md-index	231
cfm md md-index	232
cfm md md-index	232
cfm md md-index	232
cfm md md-index	233
cfm md md-index	233
cfm md md-index	234
cfm md md-index	234
cfm md md-index	234
cfm mep mep-id cc {enable disable}	233
cfm mep mep-id direction {up down} [primary-vlan vlan-id] interface ethernet port-id	232
cfm mep mep-id priority priority-id	232
cfm mep mep-id state {enable disable}	232
cfm mip mip-id interface ethernet port-id	233
cfm rmep rmep-id mep mep-id	232
channel-group channel-group-number mode {active passive}	55
channel-group channel-group-number	54
channel-group channel-group-number	55
channel-group channel-group-number mode on	54
channel-group channel-group-number monitor-link-group group-ID { uplink downlink }	246
channel-group channel-group-number_1 backup { interface device/slot/port_2 channel-group channel-group-number_2 }	240
channel-group channel-group-number_1 backup { interface device/slot/port_2 channel-group channel-group-number_2 } preemption delay <1-60>	241
channel-group channel-group-number_1 backup { interface device/slot/port_2 channel-group channel-group-number_2 } preemption mode { Forced Bandwidth Off }	241
channel-group group-id lacp mad	272
channel-group id spanning-tree cost path-cost	151
channel-group load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}	54
channel-group load-balance {dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac}	55
clear cfm cc	235
clear cfm cc database	235
clear cpu-statistics	220
clear efm statistics interface [interface-name]	258
clear interface [interface-num slot-num]	41
clear startup-config	199
clear traffic-statistic { [all [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]]] }	138

clock set HH:MM:SS YYYY/MM/DD	206
clock timezone name hour minute	206
Config mirrored port successfully !	47
Config monitor port successfully !	47
config terminal	29
configure terminal	106
configure terminal	107
configure terminal	107
configure terminal	109
configure terminal	111
configure terminal	115
configure terminal	118
configure terminal	120
configure terminal	120
configure terminal	121
configure terminal	121
configure terminal	123
configure terminal	124
configure terminal	125
configure terminal	127
configure terminal	133
configure terminal	134
configure terminal	134
configure terminal	135
configure terminal	135
configure terminal	135
configure terminal	135
configure terminal	136
configure terminal	136
configure terminal	137
configure terminal	138
configure terminal	149
configure terminal	150
configure terminal	150
configure terminal	151
configure terminal	151
configure terminal	151
configure terminal	151
configure terminal	151
configure terminal	152
configure terminal	152
configure terminal	152
configure terminal	153
configure terminal	153
configure terminal	153
configure terminal	153
configure terminal	154
configure terminal	163
configure terminal	163
configure terminal	163
configure terminal	163
configure terminal	164
configure terminal	165
configure terminal	166
configure terminal	166
configure terminal	166
configure terminal	166
configure terminal	167
configure terminal	182
configure terminal	182
configure terminal	183
configure terminal	183

configure terminal	184
configure terminal	184
configure terminal	185
configure terminal	185
configure terminal	186
configure terminal	186
configure terminal	186
configure terminal	187
configure terminal	189
configure terminal	189
configure terminal	190
configure terminal	190
configure terminal	191
configure terminal	191
configure terminal	191
configure terminal	191
configure terminal	191
configure terminal	192
configure terminal	194
configure terminal	209
configure terminal	211
configure terminal	226
configure terminal	226
configure terminal	230
configure terminal	230
configure terminal	231
configure terminal	231
configure terminal	231
configure terminal	232
configure terminal	232
configure terminal	232
configure terminal	233
configure terminal	233
configure terminal	234
configure terminal	234
configure terminal	234
configure terminal	234
configure terminal	240
configure terminal	241
configure terminal	241
configure terminal	242
configure terminal	246
configure terminal	254
configure terminal	255
configure terminal	256
configure terminal	256
configure terminal	257
configure terminal	257
configure terminal	260
configure terminal	260
configure terminal	264
configure terminal	264
configure terminal	268
configure terminal	269
configure terminal	272
configure terminal	274
configure terminal	32
configure terminal	35
configure terminal	35
configure terminal	36

configure terminal	36
configure terminal	37
configure terminal	48
configure terminal	49
configure terminal	60
configure terminal	65
configure terminal	65
configure terminal	66
configure terminal	66
configure terminal	67
configure terminal	67
configure terminal	70
configure terminal	70
configure terminal	71
configure terminal	79
configure terminal	79
configure terminal	80
configure terminal	80
configure terminal	82
configure terminal	83
configure terminal	85
configure terminal	87
configure terminal	87
configure terminal	88
configure terminal	88
configure terminal	88
configure terminal	89
configure terminal	89
configure terminal	90
configure terminal	90
configure terminal	90
configure terminal	91
configure terminal	91
configure terminal	91
configure terminal	97
configure terminal	97
configure terminal	98
copy running-config startup-config	199
copy running-config startup-config	29
copy running-config startup-config	30
copy running-config startup-config	30
copy running-config startup-config	31
copy running-config startup-config	83
copy running-config startup-config	83
copy startup-config running-config	199
cpu-car target_rate	218
crypto key generate rsa	194
crypto key refresh	194
crypto key zeroize rsa	194
default domain-name domain-name	163
description description-list	38
description string<1-32>	65
dhcp max-hops number <1-16>	107
dhcp option82	115
dhcp option82 circuit-id {string user-defined}	115
dhcp option82 format {henan normal verbose}	115
dhcp option82 remote-id {string user-defined}	115
dhcp option82 strategy {drop keep replace}	115
dhcp-relay	107

dhcp-relay hide server-ip	107
dhcp-server number	107
dhcp-server number ip ipaddress	106
dhcp-server traps	107
dhcp-snooping	109
dhcp-snooping max-clients <0-2048>	110
dhcp-snooping max-clients <0-2048>	110
dhcp-snooping port-down-action fast-remove	110
dhcp-snooping trust	109
discard-bpdu	217
dlf-forward { multicast unicast }	217
Dns {primary-ip second-ip third-ip fourth-ip suffix} dns server address	107
domain name	163
dot1x daemon [interface-list]	166
dot1x daemon time time [interface-list]	166
dot1x detect [interface-list]	167
dot1x detect interval time	167
dot1x eap-finish eap-transfer	165
dot1x max-user [interface-list]	167
dot1x method { macbased portbased }	166
dot1x port-control { auto forceauthorized forceunauthorized } [interface-list]	166
dot1x re-authenticate [interface-list]	166
dot1x re-authentication [interface-list]	166
dot1x timeout re-authperiod time [interface-list]	166
dot1x user cut {username name mac-address mac [vlan vid]}	167
dtag insert start-vlan end-vlan service-vlan	264
dtag mode {customer uplink}	264
dtag mode {customer uplink}	264
duplex { auto full half }	38
efm	255
efm link-monitor {errored-symbol-period errored-frame errored-frame-period errored-frame-seconds}	256
efm link-monitor errored-frame threshold th-value	256
efm link-monitor errored-frame window win-value	256
efm link-monitor errored-frame-period threshold th-value	256
efm link-monitor errored-frame-period window win-value	256
efm link-monitor errored-frame-seconds threshold th-value	257
efm link-monitor errored-frame-seconds window win-value	257
efm link-monitor errored-symbol-period threshold high th-value1 low th-value2 ...	256
efm link-monitor errored-symbol-period window high win-value1 low win-value2 ...	256
efm link-timeout time	255
efm mode {passive active}	255
efm pdu-timeout time	255
efm remote-failure {link-fault dying-gasp critical-event}	256
efm remote-response-timeout time	255
efm variable-retrieval	257
Enable	29
end	83
end	83
exit	269
exit	29
Exit	30
exit	30
exit	31
exit	54
exit	55
flow-control	40
garp permit multicast mac-address mac vlan vid	97
gateway gateway address subnet mask	107

gmrp	97
gmrp	97
gvrp	70
h3c-cams { enable disable }	164
hostname hostname	206
igmp-snooping	87
igmp-snooping {permit deny} {group all vlan vid}	89
igmp-snooping {permit deny} group MAC vlan vid	89
igmp-snooping {permit deny} group-range MAC multi-count num vlan vid	89
igmp-snooping drop query	90
igmp-snooping drop report	91
igmp-snooping fast-leave	88
igmp-snooping general-query source-ip ip	89
igmp-snooping group-limit number	88
igmp-snooping host-aging-time time	87
igmp-snooping max-response-time time	87
igmp-snooping multicast vlan vid	90
igmp-snooping preview	91
igmp-snooping preview {time-once time-once time-interval time-interval time-reset time-reset permit-times preview-times }	91
igmp-snooping preview group-ip ip vlan vid interface ethernet interface-num	91
igmp-snooping profile profile-id	91
igmp-snooping profile refer profile-list	92
igmp-snooping querier	89
igmp-snooping querier-vlan vid	89
igmp-snooping query-interval interval	89
igmp-snooping query-max-respond time	89
igmp-snooping record-host	90
igmp-snooping route-port forward	89
igmp-snooping route-port vlan vid interface {All ethernet interface-num}	90
igmp-snooping router-port-age {on off age-time}	90
ingress acceptable-frame { all tagged }	39
ingress filtering	39
interface {interface_type interface_num interface_name }	214
interface ethernet device/slot/port	127
interface ethernet device/slot/port	149
interface ethernet device/slot/port	226
interface ethernet device/slot/port	226
interface ethernet device/slot/port	246
interface ethernet device/slot/port_1	240
interface ethernet device/slot/port_1	241
interface ethernet device/slot/port_1	241
interface ethernet interface-num	182
interface ethernet { device-num/slot-num/port-num }	35
interface ethernet device / slot / port	254
interface ethernet device / slot / port	255
interface ethernet device / slot / port	256
interface ethernet device / slot / port	256
interface ethernet device / slot / port	257
interface ethernet device / slot / port	257
interface ethernet device/slot/port	134
interface Ethernet device/slot/port	264
interface Ethernet device/slot/port	264
interface ethernet device/slot/port	60
interface ethernet device/slot/port	65
interface ethernet device/slot/port	66
interface ethernet device/slot/port	66
interface ethernet device/slot/port	79
interface ethernet device/slot/port	80

interface ethernet device/slot/port	80
interface ethernet device/slot/port	97
interface ethernet device-num/slot-num/port-num	36
interface ethernet device-num/slot-num/port-num	36
interface ethernet device-num/slot-num/port-num	37
interface ethernet interface-num	109
interface ethernet interface-num	110
interface ethernet interface-num	111
interface ethernet interface-num	115
interface ethernet interface-num	151
interface ethernet interface-num	151
interface ethernet interface-num	151
interface ethernet interface-num	152
interface ethernet interface-num	152
interface ethernet interface-num	152
interface ethernet interface-num	153
interface ethernet interface-num	153
interface ethernet interface-num	154
interface ethernet interface-num	154
Interface ethernet interface-num	184
interface ethernet interface-num	184
interface ethernet interface-num	185
interface ethernet interface-num	185
interface ethernet interface-num	186
interface ethernet interface-num	186
interface ethernet interface-num	186
interface ethernet interface-num	260
interface ethernet interface-num	48
interface ethernet interface_num	54
interface ethernet interface_num	55
interface ethernet interface-num	70
interface ethernet interface-num	70
interface ethernet interface-num	88
interface ethernet interface-num	88
interface ethernet interface-num	89
interface ethernet interface-num	90
interface ethernet interface-num	90
interface ethernet interface-num	90
interface ethernet interface-num	91
interface ethernet interface-num	92
interface ethernet port-num	272
interface ethernet port-num	275
interface range ethernet interface_list	55
interface range ethernet interface_list	54
interface range interface-list	35
interface vlan-interface vlan id	107
interface vlan-interface vlan-id	274
ip pool name	107
ip range start-ip end-ip [vlan vlan-id]	92
ip-source-guard {ip ip-mac ip-mac-vlan}	111
ip-source-guard bind {ip A.B.C.D mac HH:HH:HH:HH:HH:HH interface ethernet device-num<0>/slot- num<0-2>/port-num<1-48>}	111
ip-source-guard permit igmp	111
ip-source-guard vlan VLAN list	111
l2-tunnel [cdp lacp pagp stp udld vtp]	260
l2-tunnel drop-threshold [cdp lacp pagp stp udld vtp] rate	260
lacp port-priority priority	55
lacp system-priority priority	55
lease time	107

linkup gratuitous-arp	80
lldp	222
lldp { rx rxtx tx }	222
lldp hello-time <5-32768>s	222
lldp hold-time <2-10>s	222
local-user username name password pwd [vlan vid]	163
login-access-list { web snmp telnet telnet-limit } ip-address wildcard	218
login-access-list telnet-limit limit-no	218
loopback { internal external }	218
mac range start-mac end-mac [vlan vlan-id]	92
mac-address-table { static permanent dynamic } mac interface interface-num vlan vlan-id 214	
mac-address-table age-time [agetime disable]	215
mac-address-table blackhole mac vlan vlan-id	214
mac-address-table learning	215
mac-address-table max-mac-count max-mac-count	215
mac-address-table move update { transmit receive }	242
mad bfd {enable disable}	274
mailalarm	219
mailalarm ccaddr cc-addr	219
mailalarm logging level level	219
mailalarm receiver receiver-addr	219
mailalarm server server-addr	219
mailalarm smtp authentication username username { passwd passwd encrypt-passwd encrypt-passwd }	219
mirror destination-interface interface-num	46
mirror destination-interface	45
mirror source-interface	45
mirror source-interface { interface-list cpu } { both egress ingress }	46
mirrored-to { ip-group { acl-number acl-name } [subitem subitem] link-group { acl-number acl-name } [subitem subitem] } interface ethernet interface-num	45
mirrored-to	45
muser radius name {chap pap} [local]	32
muser tacacs+ {account [local] author [local] local}	33
nas-ipaddress ipaddr	163
no access-group all	125
no access-list [num all]	124
no access-list { name all }	122
no access-list { num all }	121
no arp {dynamic static all ipaddress }	79
no arp overwrite	79
no arp peer	79
no arp probe ip {all ip}	80
no arp-proxy	81
no arp-proxy broadcast	81
no arp-reply-repeat	80
no channel-group channel-group-number	54
no channel-group channel-group-number	54
no channel-group channel-group-number	55
no channel-group channel-group-number	55
No channel-group channel-group-number monitor-link-group group-ID { uplink downlink } 246	
no channel-group channel-group-number_1 backup	240
no dhcp option82 circuit-id {string user-defined}	115
no dhcp option82 remote-id {string user-defined}	115
no dhcp-server traps	107
no dhcp-snooping max-clients	110
no dhcp-snooping port-down-action fast-remove	110
no dhcp-snooping trust	109
no dns {primary-ip second-ip third-ip fourth-ip suffix}	107

no dtag insert {all start-vlan end-vlan}	264
no dtag mode	264
no duplex	38
no flow-control	40
no gvrp	70
no igmp-snooping drop query	90
no igmp-snooping drop report	91
no ingress acceptable-frame	39
no ingress filtering	39
no ip pool name	107
no ip-source-guard permit igmp	111
no ip-source-guard vlan VLAN list	111
no lease	107
no linkup gratuitous-arp	80
no mirrored-to	45
no mirrored-to { ip-group { acl-number acl-name } [subitem subitem] link-group { acl-number acl-name } [subitem subitem] }	45
no port-isolation uplink all	60
no priority	38
no router	107
no section ID	107
no snmp client	189
no spanning-tree	182
no spanning-tree	274
no spanning-tree bpdu-filter	154
no spanning-tree bpdu-filter	154
no spanning-tree bpdu-guard	153
no spanning-tree bpdu-guard	154
no spanning-tree loop-guard	153
no spanning-tree mst config-digest-snooping	186
no spanning-tree mst disable instance instance-number	187
no spanning-tree mst instance instance-num vlan vlan-list	183
no spanning-tree mst root-guard	186
no spanning-tree root-guard	153
no speed	38
no switchport { all ethernet port_list }	67
no switchport backup	240
no switchport default vlan	65
no switchport default vlan	66
no switchport default vlan	66
no switchport hybrid { tagged untagged } vlan { all vlan-id }	66
no switchport hybrid vlan vlan-list	38
no switchport mode	65
no switchport mode	66
No switchport monitor-link-group group-ID { uplink downlink }	246
no switchport trunk allowed vlan { all vlan-id }	66
no switchport trunk allowed vlan vlan-list	38
no username username	31
no vlan {vlan-list all}	67
no wins {primary-ip second-ip}	107
periodic days-of-the-week hh:mm:ss to [day-of-the-week] hh:mm:ss	118
ping [-i ttl] [-l packetlength] [-n packetnumber] [-s sourceip] [-t timeout] ip_address	211
port-isolation uplink ethernet device/slot/port	60
pppoeplus	226
pppoeplus circuit-id string	226
pppoeplus delimiter { colon dot slash space }	226
pppoeplus drop {padi pado}	226

pppoeplus format { binary ascii }	226
pppoeplus strategy { drop keep replace }	226
pppoeplus trust	226
pppoeplus type { huawei standard self-defined { circuit-id { <string> vlan port switch-mac hostname client-mac }* remote-id { <string> switch-mac hostname client-mac }* }	226
primary-auth-ip ipaddr port	163
priority priority-value	38
profile limit {permit deny}	91
queue-scheduler cos-map queue-number packed-priority	136
queue-scheduler dscp-map dscp-value 802.1p-priority	137
queue-scheduler dscp-map	137
queue-scheduler sp-wrr queue1-weight queue2-weight queue3-weight	136
queue-scheduler strict-priority	136
queue-scheduler wrr queue1-weight queue2-weight queue3-weight queue4-weight	136
radius 8021p enable	164
radius accounting	164
radius bandwidth-limit enable	165
radius host binding radius-name	164
radius host name	163
radius host name	32
radius mac-address-number enable	165
radius server-disconnect drop 1x	164
radius vlan enable	164
rate-limit { input output } { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } target-rate	133
rate-limit { input output } { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } two-rate-policer policer-id	134
realtime-account	163
realtime-account interval <time>	163
reboot	217
reboot device-id	269
router ipaddress	107
scheme { local radius [local] }	163
second-auth-ip ipaddr port	163
section ID start ipaddress end ipaddress	107
sh mac-address-table move update	242
show access-list config {all num name name}	126
show access-list config statistic	126
show access-list runtime {all num name name}	126
show alarm all-packets	49
show alarm all-packets interface [ethernet interface-num]	49
show alarm cpu	219
show alarm cpu	49
show anti-dos	219
show arp {dynamic static all}	79
show arp anti-flood	85
show arp anti-spoofing	83
show arp anti-spoofing	84
show arp probe	81
show arp-proxy	81
show bandwidth-control interface Ethernet [interface-num]	139
show bfd session	274
show cfm cc	235
show cfm cc database	235
show cfm errors	235
show cfm ma	235
show cfm md [md-index]	235
show cfm mp local	235

show cfm mp remote	235
show clock	220
show cpu-car	220
show cpu-statistics	220
show cpu-utilization	220
show description interface [interface-list]	41
show dhcp option82	115
show dhcp-relay	108
show dhcp-relay hide server-ip	108
show dhcp-server clients	108
show dhcp-server clients [ip [mask] mac poolname]	220
show dhcp-server interface {vlan-interface if-id supervlan-interface if-id} ..	108
show dhcp-server server-id	108
show dhcp-snooping clients	112
show dhcp-snooping interface {ethernet pon} interface-num	112
show dhcp-snooping vlan	112
show dtag	264
show dtag	264
show efm discovery interface [interface-name]	258
show efm port port-id-list remote-mib {phyadminstate autonegadminstate}	257
show efm statistics interface [interface-name]	258
show efm status interface [interface-name]	258
show efm summary	258
show garp permit multicast	98
show garp permit vlan	71
show gmrp	98
show gmrp interface [ethernet interface-num]	98
show gvrp	71
show gvrp interface [ethernet device/slot/port]	71
show igmp-snooping	92
show igmp-snooping preview	92
show igmp-snooping preview status	92
show igmp-snooping profile [interface ethernet interface-num] [profile-list]	92
show igmp-snooping record-host [interface ethernet interface-num]	92
show igmp-snooping router-dynamic	92
show igmp-snooping router-static	92
show interface [interface-num]	41
show interface ethernet device-num/slot-num/port-num	36
show interface switch backup	242
show ip fdb [ip ip-address [mask]]	220
show ip-source-guard	112
show ip-source-guard bind [ip A.B.C.D]	112
show ip-source-guard permit igmp	112
show ip-source-guard vlan	112
show keyfile {public private}	194
show l2-tunnel drop-threshold	260
show l2-tunnel interface [ethernet interface-num]	260
show lacp extend-tlv-relay	272
show lacp internal [channel-group-number]	55
show lacp neighbor [channel-group-number]	55
show lacp sys-id	55
show lldp [interface ethernet device/slot/port]	223
show login-access-list	218
show mac-address-table { interface-num [vlan vlan-id] cpu }	216
show mac-address-table { static dynamic permanent blackhole } [vlan vlan-id]	216
show mac-address-table { static dynamic permanent blackhole } interface interface-num [
vlan vlan-id]	216
show mac-address-table age-time	216
show mac-address-table blackhole	84

show mac-address-table learning	216
show mac-address-table mac [vlan vlan-id]	216
show mac-address-table vlan vlan-id	216
show mac-address-table	216
show mad bfd	274
show mailalarm	219
show memory	220
show mirror	46
show monitor-link-group	247
show multicast	98
show multicast igmp-snooping [interface ethernet interface-num]	92
show muser	32
show muser	33
Show port-isolation	60
show pppoeplus [interface-list]	227
show qos-info all	139
show qos-info statistic	139
show qos-info traffic-copy-to-cpu	139
show qos-info traffic-priority	139
show qos-info traffic-redirect	139
show qos-info traffic-statistic	139
show qos-interface [interface-num] rate-limit	139
show qos-interface all	139
show qos-interface statistic	139
show queue-scheduler cos-map	139
show queue-scheduler dscp-map	139
show queueY-scheduler	139
show running-config [module-list]	199
show snmp community	209
show snmp contact	209
show snmp engineid [local remote]	209
show snmp group	209
show snmp host	209
show snmp location	209
show snmp notify	209
show snmp user	210
show snmp view	210
show sntp client	192
show sntp client summer-time	192
show spanning-tree interface [brief [ethernet device/slot/port]]	154
show spanning-tree mst config-id	187
show spanning-tree mst instance	187
show spanning-tree mst instance brief id	187
show ssh	194
show stack debug	269
show stack	269
show stack	269
show stack mad exclude interface [ethernet port-num]	272
show stack mad exclude interface [ethernet port-num]	275
show stack members device-id	269
show stack neighbors	269
show stack statistic	269
show startup-config [module-list]	199
show statistic dynamic interface	41
show statistics interface [interface-num]	41
show storm-control interface ethernet slot/port	127
show system	220
show tacacs+	33
show telnet client	218

show username	220
show username	29
show username	30
show username	31
show username	31
show users	220
show users	31
show utilization interface	41
show version	220
show vlan vlan-id / brief	65
show vlan vlan-id / brief	67
show vlan vlan-id / brief	67
show vlan vlan-id brief	65
show vlan vlan-id brief	66
show vlan vlan-id brief	66
shutdown	38
snmp-server community community { ro rw } { deny permit } [view view-name]	208
snmp-server contact syscontact	208
snmp-server enable traps [notificationtype-list]	208
snmp-server engineid { local engineid-string remote ip-address [udp-port port-number] engi- neid-string }	208
snmp-server group groupname { 3 [auth noauthpriv priv] [context context-name]} [read read- view] [write writeview] [notify notifyview]	209
snmp-server host host-addr [version {1 2c 3 [auth noauthpriv priv]}] community-string [udp-port port] [notify-type [notifytype-list]]	208
snmp-server location syslocation	208
snmp-server name sysname	208
snmp-server user username groupname [remote host [udp-port port]] [auth { md5 sha } { authpassword { encrypt-authpassword authpassword authpassword } authkey { encrypt- authkey authkey authkey } } [priv des { privpassword { encrypt-privpassword privpass- word privpassword } privkey { encrypt-privkey privkey privkey } }]	209
snmp-server view view-name oid-tree { included excluded }	209
sntp client	189
sntp client authenticate	192
sntp client authentication-key key-number md5 value	192
sntp client broadcastdelay time	190
sntp client retransmit times	191
Sntp client retransmit-interval time	191
sntp client summer-time daily {start-month start-day start-time end-month end-day end-time } 191	
sntp client summer-time weekly{ start-week Fri mon sat sun thu tue wed start-time end-month end-week Fri mon sat sun thu tue wed end-time}	191
sntp client valid-server IP mask	191
sntp server backup IP	190
sntp server ip_address	190
sntp trusted-key key-number	192
sntp client mode {broadcast unicast multicast anycast [key key]}	189
spanning-tree	149
spanning-tree	182
spanning-tree bpdu-filter	154
spanning-tree bpdu-filter	154
spanning-tree bpdu-guard	153
spanning-tree bpdu-guard	154
spanning-tree cost path-cost	151
spanning-tree forward-time seconds	150
spanning-tree hello-time seconds	150
spanning-tree loop-guard	153
spanning-tree max-age seconds	150
spanning-tree mcheck	151

spanning-tree mode mstp	182
spanning-tree mode stp	149
spanning-tree mst config-digest-snooping	186
spanning-tree mst disable instance instance-number	187
spanning-tree mst external cost cost	185
spanning-tree mst forward-time forward-time	182
spanning-tree mst hello-time hello-time	182
spanning-tree mst instance instance-num cost cost	185
spanning-tree mst instance instance-num port-priority priority	185
spanning-tree mst instance instance-num priority priority	183
spanning-tree mst instance instance-num vlan vlan-list	183
spanning-tree mst link-type point-to-point auto	184
spanning-tree mst link-type point-to-point forcefalse	184
spanning-tree mst link-type point-to-point forcetrue	184
spanning-tree mst max-age max-age	182
spanning-tree mst max-hops max-hops	182
spanning-tree mst mcheck	186
spanning-tree mst name name	183
spanning-tree mst revision revision-level	183
spanning-tree mst root-guard	186
spanning-tree point-to-point auto	152
spanning-tree point-to-point forcefalse	152
spanning-tree point-to-point forcetrue	152
spanning-tree portfast	152
spanning-tree port-priority priority	151
spanning-tree priority bridge priority	150
spanning-tree root-guard	153
spanning-tree root-guard action {block-port drop-packets}	153
spanning-tree transit-limit transit-limit	152
speed { speed-value auto }	38
stack device-id <0-3>	269
stack device-id value	268
state { active block }	164
stop telnet client { all term-id }	218
Storm-control type {broadcast multicast unicast } rate <64-32000000>	127
Switch(config)#mirror destination-interface ethernet 0/1/1	47
Switch(config)#mirror source-interface ethernet 0/0/1 to ethernet 0/0/12 egress ..	47
switchport backup	241
switchport backup	241
switchport backup { interface device/slot/port_2 channel-group channel-group-number_2 } ..	240
switchport default vlan vlan_id	36
switchport default vlan vlan-id	65
switchport default vlan vlan-id	66
switchport ethernet device /slot /port	65
switchport hybrid { tagged untagged } vlan { all vlan-id }	66
switchport hybrid tagged vlan vlan-list	37
switchport hybrid untagged vlan vlan-list	37
switchport mode {access hybrid trunk}	36
switchport mode access	65
switchport mode hybrid	66
switchport mode trunk	66
switchport monitor-link-group group-ID { uplink downlink }	246
switchport trunk allowed vlan { all vlan-id}	66
switchport trunk allowed vlan vlan-list	38
tacacs+ { priamary secondary } server ipaddress [key keyvalue] [port portnum] [timeout time- value]	33
telnet ip-addr [port-num] [/localecho]	218
time-range name	118
tracert [-u -c] -f first_ttl -h maximum_hops -w time_out] target_name ..	211

traffic-copy-to-cpu { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } 135
traffic-priority { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } { [dscp dscp-value] [cos { pre-value from-ipprec }] [local-precedence pre-value] } 135
traffic-redirect { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } { [interface interface-num cpu] } 135
traffic-statistic { [ip-group { num name } [subitem subitem]] [link-group { num name } [subitem subitem]] } 138
two-rate-policer { [mode {color-aware color-bind} [set-pre-color dscp-value {green red yellow}]] } 134
username change-password 30
username username privilege privilege < pri-value > password encryption-type < 0 7> password	29
username username privilege privilege <0-15> encryption-type <0 7> password 30
username-format { with-domain without-domain } 163
vct { auto-run run } 218
vlan <vlanid> 81
vlan vlan_list 110
VLAN vlan-list 65
vlan vlan-list 67
wins second-ip ipaddress 107