
Contents

1 Basic configurations	1
1.1 CLI	1
1.1.1 Introduction.....	1
1.1.2 Levels.....	2
1.1.3 Modes.....	2
1.1.4 Shortcut keys.....	5
1.1.5 Acquiring help.....	6
1.1.6 Display information	9
1.1.7 Command history.....	9
1.1.8 Restoring default value of command line	10
1.1.9 Logging command lines.....	10
1.2 Accessing device	11
1.2.1 Introduction.....	11
1.2.2 Accessing through Console interface	11
1.2.3 Accessing through Telnet	12
1.2.4 Accessing through SSH.....	13
1.2.5 Managing users	15
1.2.6 Checking configurations	17
1.3 Managing files.....	17
1.3.1 Managing BootROM files.....	17
1.3.2 Managing system files	18
1.3.3 Managing configuration files	19
1.3.4 Checking configurations	20
1.4 Load and upgrade	20
1.4.1 Introduction.....	20
1.4.2 Upgrading system software through BootROM.....	21
1.4.3 Upgrading system software through CLI	23
1.4.4 Checking configurations	23
1.5 Configuring time management.....	23
1.5.1 Configuring time and time zone.....	23
1.5.2 Configuring DST	24
1.5.3 Configuring NTP	25

1.5.4 Configuring SNTP	26
1.5.5 Checking configurations	27
1.6 Configuring interface management	27
1.6.1 Introduction.....	27
1.6.2 Default configurations of interface management	28
1.6.3 Configuring basic attributes of interfaces	28
1.6.4 Configuring interface rate statistics	29
1.6.5 Configuring flow control on interfaces	29
1.6.6 Enabling/Disabling interfaces	30
1.6.7 Configuring L2Protocol Peer STP	30
1.6.8 Configuring Console interface	30
1.6.9 Checking configurations	31
1.7 Configuring basic information	31
1.8 Task scheduling	32
1.8.1 Introduction.....	32
1.8.2 Configuring task scheduling	32
1.8.3 Checking configurations	33
1.9 Watchdog.....	33
1.9.1 Introduction.....	33
1.9.2 Preparing for configurations	34
1.9.3 Default configurations of watchdog.....	34
1.9.4 Configuring Watchdog	34
1.9.5 Checking configurations	34
1.1 Configuring Banner.....	34
1.1.1 Preparing for configurations	34
1.1.2 Configuring Banner.....	35
1.1.3 Enabling Banner display	35
1.1.4 Checking configurations	35
2 Ethernet	36
2.1 MAC address table.....	36
2.1.1 Introduction.....	36
2.1.2 Preparing for configurations	38
2.1.3 Default configurations of MAC address table.....	39
2.1.4 Configuring static MAC address.....	39
2.1.5 Configuring blackhole MAC address.....	39
2.1.6 Configuring MAC address learning	39
2.1.7 Configuring MAC address limit.....	40
2.1.8 Configuring aging time of MAC addresses.....	40
2.1.9 Enabling inhibition of MAC address drifting	40
2.1.10 Checking configurations	40
2.1.11 Maintenance	41

2.2 VLAN.....	41
2.2.1 Introduction.....	41
2.2.2 Preparing for configurations	43
2.2.3 Default configurations of VLAN	44
2.2.4 Configuring VLAN attributes	44
2.2.5 Configuring interface mode	45
2.2.6 Configuring VLAN on Access interface	45
2.2.7 Configuring VLAN on Trunk interface.....	46
2.2.8 Checking configurations	47
2.3 QinQ.....	47
2.3.1 Introduction.....	47
2.3.2 Preparing for configurations	48
2.3.3 Default configurations of QinQ	48
2.3.4 Configuring basic QinQ.....	49
2.3.5 Configuring selective QinQ	49
2.3.6 Configuring network-side interface toTrunk mode.....	50
2.3.7 Configuring TPID	50
2.3.8 Checking configurations	50
2.4 VLAN mapping.....	51
2.4.1 Introduction.....	51
2.4.2 Preparing for configurations	51
2.4.3 Default configurations of VLAN mapping	52
2.4.4 Configuring 1:1 VLAN mapping	52
2.4.5 Checking configurations	53
2.5 STP/RTSTP	53
2.5.1 Introduction.....	53
2.5.2 Preparation for configuration	55
2.5.3 Default configurations of STP	55
2.5.4 Enabling STP	56
2.5.5 Configuring STP parameters.....	56
2.5.6 (Optional) configuring RSTP edge interface.....	57
2.5.7 (Optional) configuring RSTP link type	57
2.5.8 Checking configurations	58
2.6 MSTP	58
2.6.1 Introduction.....	58
2.6.2 Preparation for configuration	61
2.6.3 Default configurations of MSTP.....	61
2.6.4 Enabling MSTP.....	62
2.6.5 Configuring MST domain and its maximum number of hops.....	62
2.6.6 Configuring root bridge/backup bridge.....	63
2.6.7 Configuring interface priority and system priority.....	64
2.6.8 Configuring network diameter for switch network	65

2.6.9 Configuring inner path cost for interface	65
2.6.10 Configuring external path cost on interface	66
2.6.11 Configuring maximum transmission rate on interface	66
2.6.12 Configuring MSTP timer	66
2.6.13 Configuring edge interface.....	67
2.6.14 Configuring BPDU filtering.....	68
2.6.15 Configuring BPDU Guard.....	68
2.6.16 Configuring STP/RSTP/MSTP mode switching	69
2.6.17 Configuring link type	69
2.6.18 Configuring root interface protection.....	70
2.6.19 Configuring interface loopguard	70
2.6.20 Checking configurations	71
2.6.21 Maintenance.....	71
2.7 Loop detection.....	71
2.7.1 Introduction.....	71
2.7.2 Preparing for configurations	73
2.7.3 Default configurations of loop detection.....	74
2.7.4 Configuring loop detection	74
2.7.5 Checking configurations	75
2.7.6 Maintenance.....	75
2.8 Interface protection	75
2.8.1 Introduction.....	75
2.8.2 Preparing for configurations	76
2.8.3 Default configurations of interface protection	76
2.8.4 Configuring interface protection	76
2.8.5 Checking configurations	76
2.9 Port mirroring.....	77
2.9.1 Introduction.....	77
2.9.2 Preparing for configurations	78
2.9.3 Default configurations of port mirroring.....	78
2.9.4 Configuring port mirroring on local port	78
2.9.5 Checking configurations	79
2.10 L2CP	79
2.10.1 Introduction.....	79
2.10.2 Preparing for configurations	79
2.10.3 Default configurations of L2CP	79
2.10.4 Configuring global L2CP	80
2.10.5 Configuring L2CP profile	80
2.10.6 Configuring L2CP profile on interface	81
2.10.7 Checking configurations	81
2.10.8 Maintenance.....	81

3 Ring network protection	82
3.1 G.8032.....	82
3.1.1 Introduction.....	82
3.1.2 Preparing for configurations	82
3.1.3 Default configurations of G.8032	83
3.1.4 Creating G.8032 ring.....	83
3.1.5 (Optional) creating G.8032 sub-ring	85
3.1.6 (Optional) configuring G.8032 switching control	87
3.1.7 Checking configurations	88
3.1.8 Maintenance	88
4 IP services	89
4.1 IP basis	89
4.1.1 Introduction.....	89
4.1.2 Preparing for configurations	89
4.1.3 Default configurations of the Layer 3 interface	89
4.1.4 Configuring IPv4 address of VLAN interface	90
4.1.5 Configuring IPv6 address of VLAN interface	90
4.1.6 Checking configurations	90
4.2 Loopback interface.....	91
4.2.1 Introduction.....	91
4.2.2 Preparing for configurations	91
4.2.3 Default configurations of the loopback interface	91
4.2.4 Configuring IP address of the loopback interface	91
4.2.5 Checking configurations	92
4.3 ARP	92
4.3.1 Introduction.....	92
4.3.2 Preparing for configurations	93
4.3.3 Default configurations of ARP.....	93
4.3.4 Configuring static ARP entries.....	93
4.3.5 Configuring dynamic ARP entries	93
4.3.6 Configuring local proxy ARP.....	94
4.3.7 Checking configurations	94
4.3.8 Maintenance	94
4.4 NDP.....	95
4.4.1 Introduction.....	95
4.4.2 Preparing for configurations	96
4.4.3 Default configurations of NDP	96
4.4.4 Configuring static neighbor entries	96
4.4.5 Configuring times of sending NS messages for detecting duplicated addresses.....	96
4.4.6 Configuring maximum number of NDPs allowed to learn on Layer 3 interface	97
4.4.7 Checking configurations	97

4.4.8 Maintenance	98
4.5 Static route	98
4.5.1 Introduction	98
4.5.2 Preparing for configurations	98
4.5.3 Configuring static route	98
4.5.4 Checking configurations	99
4.6 Configuring OSPF	99
4.6.1 Configuring OSPF basic functions	99
4.6.2 Configuring OSPF route properties	100
4.6.3 Configuring OSPF network	101
4.6.4 Optimizing OSPF network	102
4.6.5 Configuring OSPF authentication mode	104
4.6.6 Configuring Stub area	105
4.6.7 Controlling OSPF routing information	106
4.6.8 Configuring OSPF routing policy	108
4.6.9 Configuring BFD for OSPF	110
4.6.10 Configuring OSPF for MPLS-TE	110
4.6.11 Checking configurations	111
4.6.12 Maintenance	111
5 DHCP	112
5.1 DHCP Relay	112
5.1.1 Introduction	112
5.1.2 Preparing for configurations	113
5.1.3 Configuring DHCP v4 Relay	113
5.1.4 Configuring destination IP address for DHCP v4 Relay	114
5.1.5 Checking configurations	114
5.2 DHCP Server	114
5.2.1 Introduction	114
5.2.2 Preparing for configurations	115
5.2.3 Configuring IPv4 address pool	115
5.2.4 Configuring DHCP Server on interface	116
5.2.5 Checking configurations	116
5.3 DHCP Client	116
5.3.1 Introduction	116
5.3.2 Preparing for configurations	119
5.3.3 Default configurations of DHCP Client	119
5.3.4 Configuring DHCP Client	119
5.3.5 Checking configurations	120
5.4 DHCP Snooping	121
5.4.1 Introduction	121
5.4.2 Preparing for configurations	122

5.4.3 Default configurations of DHCP Snooping.....	122
5.4.4 Configuring DHCP Snooping	122
5.4.5 Checking configurations	123
5.5 DHCP Options.....	123
5.5.1 Introduction.....	123
5.5.2 Preparing for configurations	125
5.5.3 Default configurations of DHCP Option.....	125
5.5.4 Configuring DHCP Option field	125
5.5.5 Checking configurations	126
6 QoS.....	127
6.1 Introduction.....	127
6.1.1 Service model.....	127
6.1.2 Priority trust	128
6.1.3 Traffic classification.....	128
6.1.4 Traffic policy.....	130
6.1.5 Priority mapping	131
6.1.6 Congestion management.....	131
6.1.7 Congestion avoidance	133
6.1.8 Rate limiting.....	134
6.2 Configuring priority	134
6.2.1 Preparing for configurations	134
6.2.2 Default configurations of basic QoS	134
6.2.3 Configuring types of priorities trusted by interface	135
6.2.4 Configuring mapping from CoS to local priority.....	136
6.2.5 Configuring mapping from DSCP to local priority and color	136
6.2.6 Configuring DSCP mutation	136
6.2.7 Configuring CoS remarking.....	137
6.2.8 Checking configurations	137
6.3 Configuring congestion management.....	138
6.3.1 Preparing for configurations	138
6.3.2 Default configurations of congestion management.....	138
6.3.3 Configuring SP queue scheduling	138
6.3.4 Configuring WRR or SP+WRR queue scheduling	139
6.3.5 Configuring DRR or SP+DRR queue scheduling	139
6.3.6 Configuring queue bandwidth guarantee	139
6.3.7 Checking configurations	140
6.4 Configuring congestion avoidance.....	140
6.4.1 Preparing for configurations	140
6.4.2 Default configurations of congestion avoidance	140
6.4.3 Configuring WRED	141
6.4.4 Checking configurations	141

6.5 Configuring traffic classification and traffic policy	141
6.5.1 Preparing for configurations	141
6.5.2 Default configurations of traffic classification and traffic policy	141
6.5.3 Creating traffic classification	142
6.5.4 Configuring traffic classification rules	142
6.5.5 Creating rate limit rule and shapping rule	143
6.5.6 Creating traffic policy	144
6.5.7 Defining traffic policy mapping	144
6.5.8 Defining traffic policy operation	144
6.5.9 Applying traffic policy to interfaces	145
6.5.10 Checking configurations	146
6.6 Configuring rate limiting	146
6.6.1 Preparing for configurations	146
6.6.2 Configuring rate limiting based on interface	146
6.6.3 Checking configurations	147
7 Multicast	148
7.1 Introduction	148
7.1.1 Multicast	148
7.2 Basic functions of Layer 2 multicast	153
7.2.1 Introduction	153
7.2.2 Preparing for configurations	155
7.2.3 Default configurations of Layer 2 multicast basic functions	155
7.2.4 Configuring basic functions of Layer 2 multicast	155
7.2.5 Checking configurations	155
7.2.6 Maintenance	156
7.3 IGMP Snooping	156
7.3.1 Introduction	156
7.3.2 Preparing for configurations	157
7.3.3 Default configurations of IGMP Snooping	157
7.3.4 Configuring IGMP Snooping	157
7.3.5 Checking configurations	158
7.4 IGMP MVR	158
7.4.1 Introduction	158
7.4.2 Preparing for configurations	159
7.4.3 Default configurations of IGMP MVR	159
7.4.4 Configuring IGMP MVR	159
7.4.5 Checking configurations	160
7.5 IGMP filtering	160
7.5.1 Introduction	160
7.5.2 Preparing for configurations	161
7.5.3 Default configurations of IGMP filtering	161

7.5.4 Enabling global IGMP filtering.....	161
7.5.5 Configuring IGMP filter profile.....	162
7.5.6 Configuring maximum number of multicast groups	163
7.5.7 Checking configurations	163
7.6 PIM-SM	164
7.6.1 Introduction.....	164
7.6.2 Preparing for configurations	165
7.6.3 Default configurations of PIM-SM	165
7.6.4 Configuring dynamic RP	165
7.6.5 Configuring static RP.....	166
7.6.6 Configuring Layer 3 multicast forwarding.....	166
7.6.7 Checking configurations	166
8 Security.....	168
8.1 ACL.....	168
8.1.1 Introduction.....	168
8.1.2 Preparing for configurations	168
8.1.3 Configuring MAC ACL	169
8.1.4 Configuring filter	172
8.1.5 Checking configurations	172
8.2 Secure MAC address.....	173
8.2.1 Introduction.....	173
8.2.2 Preparing for configurations	174
8.2.3 Default configurations of secure MAC address	174
8.2.4 Configuring basic functions of secure MAC address.....	175
8.2.5 Configuring static secure MAC address.....	175
8.2.6 Configuring dynamic secure MAC address	176
8.2.7 Configuring Sticky secure MAC address.....	176
8.2.8 Checking configurations	177
8.2.9 Maintenance.....	177
8.3 Dynamic ARP inspection	178
8.3.1 Introduction.....	178
8.3.2 Preparing for configurations	179
8.3.3 Default configurations of dynamic ARP inspection	179
8.3.4 Configuring trusted interfaces of dynamic ARP inspection	179
8.3.5 Configuring static binding of dynamic ARP inspection.....	180
8.3.6 Configuring dynamic binding of dynamic ARP inspection.....	180
8.3.7 Configuring protection VLAN of dynamic ARP inspection	180
8.3.8 Configuring rate limiting on ARP packets on interface	181
8.3.9 Configuring auto-recovery time for rate limiting on ARP packets.....	181
8.3.10 Checking configurations	181
8.4 RADIUS.....	182

8.4.1 Introduction.....	182
8.4.2 Preparing for configurations	182
8.4.3 Default configurations of RADIUS	183
8.4.4 Configuring RADIUS authentication.....	183
8.4.5 Configuring RADIUS accounting.....	184
8.4.6 Checking configurations	184
8.5 TACACS+	185
8.5.1 Introduction.....	185
8.5.2 Preparing for configurations	185
8.5.3 Default configurations of TACACS+.....	185
8.5.4 Configuring TACACS+ authentication	186
8.5.5 Configuring TACACS+ accounting	186
8.5.6 Checking configurations	186
8.5.7 Maintenance.....	187
8.6 Storm control.....	187
8.6.1 Introduction.....	187
8.6.2 Preparing for configurations	188
8.6.3 Default configurations of storm control	188
8.6.4 Configuring storm control.....	188
8.6.5 Configuring DLF packet forwarding	189
8.6.6 Checking configurations	189
8.7 802.1x.....	190
8.7.1 Introduction.....	190
8.7.2 Preparing for configurations	192
8.7.3 Default configurations of 802.1x	192
8.7.4 Configuring basic functions of 802.1x.....	193
8.7.5 Configuring 802.1x re-authentication	194
8.7.6 Configuring 802.1x timers	194
8.7.7 Checking configurations	194
8.7.8 Maintenance.....	195
8.8 IP Source Guard	195
8.8.1 Introduction.....	195
8.8.2 Preparing for configurations	196
8.8.3 Default configurations of IP Source Guard	197
8.8.4 Configuring interface trust status of IP Source Guard	197
8.8.5 Configuring IP Source Guide binding.....	197
8.8.6 Checking configurations	198
8.9 PPPoE+	199
8.9.1 Introduction.....	199
8.9.2 Preparing for configurations	200
8.9.3 Default configurations of PPPoE+	200
8.9.4 Configuring basic functions of PPPoE+.....	201

8.9.5 Configuring PPPoE+ packet information.....	202
8.9.6 Checking configurations	204
8.9.7 Maintenance	204
9 Reliability	205
9.1 Link aggregation	205
9.1.1 Introduction.....	205
9.1.2 Preparing for configurations	206
9.1.3 Configuring manual link aggregation	206
9.1.4 Configuring static LACP link aggregation.....	207
9.1.5 Checking configurations	209
9.2 Interface backup	210
9.2.1 Introduction.....	210
9.2.2 Preparing for configurations	212
9.2.3 Default configurations of interface backup.....	212
9.2.4 Configuring basic functions of interface backup	212
9.2.5 (Optional) configuring FS on interfaces.....	213
9.2.6 Checking configurations	214
9.3 Configuring ELPS.....	214
9.3.1 Preparing for configurations	214
9.3.2 Creating protection pair	215
9.3.3 Configuring ELPS fault detection modes.....	215
9.3.4 (Optional) configuring ELPS switching control	216
9.3.5 Checking configurations	217
9.4 Failover	217
9.4.1 Introduction.....	217
9.4.2 Preparing for configurations	217
9.4.3 Default configurations of failover	218
9.4.4 Configuring failover.....	218
9.4.5 Checking configurations	219
10 OAM	220
10.1 Introduction	220
10.1.1 EFM	220
10.1.2 CFM.....	222
10.2 Configuring EFM	225
10.2.1 Preparing for configurations	225
10.2.2 Configuring basic functions of EFM.....	225
10.2.3 Configuring EFM active function	226
10.2.4 Configuring EFM passive function.....	227
10.2.5 Configuring link monitoring and fault indication	228
10.2.6 Checking configurations	229
10.3 E-LMI.....	230

10.3.1 Introduction.....	230
10.3.2 Preparing for configurations	230
10.3.3 Default configurations of E-LMI	231
10.3.4 Configuring E-LMI on PE	231
10.3.5 Configuring E-LMI on CE.....	234
10.3.6 Checking configurations	235
10.3.7 Maintenance.....	236
11 System management.....	237
11.1 SNMP.....	237
11.1.1 Introduction.....	237
11.1.2 Preparing for configurations.....	239
11.1.3 Default configurations of SNMP.....	239
11.1.4 Configuring basic functions of SNMP v1/v2c	240
11.1.5 Configuring basic functions of SNMP v3	240
11.1.6 Configuring IP authentication by SNMP server.....	242
11.1.7 Configuring other information of SNMP	242
11.1.8 Configuring Trap.....	242
11.1.9 Checking configurations	243
11.2 KeepAlive.....	244
11.2.1 Introduction	244
11.2.2 Preparing for configurations.....	244
11.2.3 Default configurations of KeepAlive	244
11.2.4 Configuring KeepAlive	244
11.2.5 Checking configurations	245
11.3 RMON.....	245
11.3.1 Introduction	245
11.3.2 Preparing for configurations.....	246
11.3.3 Default configurations of RMON.....	246
11.3.4 Configuring RMON statistics.....	247
11.3.5 Configuring RMON historical statistics.....	247
11.3.6 Configuring RMON alarm group	248
11.3.7 Configuring RMON event group	248
11.3.8 Checking configurations	249
11.3.9 Maintenance	249
11.4 LLDP.....	249
11.4.1 Introduction.....	249
11.4.2 Preparing for configurations.....	251
11.4.3 Default configurations of LLDP	251
11.4.4 Enabling global LLDP	252
11.4.5 Enabling interface LLDP	252
11.4.6 Configuring basic functions of LLDP	252

11.4.7 Configuring LLDP alarm	253
11.4.8 Checking configurations	253
11.4.9 Maintenance	254
11.5 Optical module DDM	254
11.5.1 Introduction	254
11.5.2 Preparing for configurations	255
11.5.3 Default configurations of optical module DDM	255
11.5.4 Enabling optical module DDM	255
11.5.5 Enabling optical module DDM Trap	255
11.5.6 Checking configurations	256
11.6 System log	256
11.6.1 Introduction	256
11.6.2 Preparing for configurations	257
11.6.3 Default configurations of system log	258
11.6.4 Configuring basic information of system log	258
11.6.5 Configuring system log output	259
11.6.6 Checking configurations	260
11.6.7 Maintenance	261
11.7 Alarm management	261
11.7.1 Introduction	261
11.7.2 Preparing for configurations	265
11.7.3 Configuring basic functions of alarm management	265
11.7.4 Checking configurations	267
11.8 Hardware environment monitoring	267
11.8.1 Introduction	267
11.8.2 Preparing for configurations	271
11.8.3 Default configurations of hardware environment monitoring	271
11.8.4 Enabling global hardware environment monitoring	272
11.8.5 Configuring temperature monitoring alarm	272
11.8.6 Configuring voltage monitoring alarm	272
11.8.7 Clearing all hardware environment monitoring alarms manually	273
11.8.8 Checking configurations	273
11.9 CPU monitoring	274
11.9.1 Introduction	274
11.9.2 Preparing for configurations	274
11.9.3 Default configurations of CPU monitoring	274
11.9.4 Showing CPU monitoring information	275
11.9.5 Configuring CPU monitoring alarm	275
11.9.6 Checking configurations	275
11.10 Cable diagnosis	276
11.10.1 Introduction	276
11.10.2 Preparing for configurations	276

11.10.3 Configuring cable diagnosis	276
11.10.4 Checking configurations	276
11.11 Memory monitoring.....	277
11.11.1 Preparing for configurations	277
11.11.2 Configuring memory monitoring	277
11.11.3 Checking configurations.....	277
11.12 Ping	277
11.12.1 Introduction	277
11.12.2 Configuring Ping	278
11.13 Traceroute.....	278
11.13.1 Introduction	278
11.13.2 Configuring Traceroute	279
12 Appendix	280
12.1 Terms	280
12.2 Acronyms and abbreviations	285

1 Basic configurations

This chapter describes basic configurations and configuration process about the SWITCH and provides the related configuration applications, including the following sections:

- CLI
- Accessing device
- Managing files
- Load and upgrade
- Configuring time management
- Configuring interface management
- Configuring basic information
- Task scheduling
- Watchdog



Note

The configuration steps in this manual are in command line mode.

1.1 CLI

1.1.1 Introduction

The Command-line Interface (CLI) is a medium for you communicating with the SWITCH. You can configure, monitor, and manage the SWITCH through the CLI.

You can log in to the SWITCH through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports following features:

- Configure the SWITCH locally through the Console interface.
- Configure the SWITCH locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.

- Shortcut keys can be used to execute commands.
- Check or execute a historical command by checking command history. The last 20 historical commands can be saved on the SWITCH.
- Enter a question mark (?) at the system prompt to obtain online help.
- The SWITCH supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Levels

The SWITCH uses hierarchy protection methods to divide command line into 16 levels from low to high.

- 0–4: visitor, users can execute the commands of **ping**, **clear**, and **history**, etc. in this level;
- 5–10: monitor, users can execute the command of **show** and so on;
- 11–14: operator, users can execute commands for different services like VLAN, IP, etc.;
- 15: administrator, used for system basic running commands.

1.1.3 Modes

Command line mode is the CLI environment. All system commands are registered in one (or some) command line mode, the command can only run under the corresponding mode.

Establish a connection with the SWITCH. If the SWITCH is in default configuration, it will enter user EXEC mode, and the screen will show:

```
Switch>
```



Note

Users under level 11 do not need to input the password when entering privileged EXEC mode.

In privileged EXEC mode, input the **config terminal** command to enter global configuration mode.

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



Note

- The CLI prompts Switch is a default host name. You can modify it by executing the **hostname** *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.

- You can use the **exit** or **quit** command to return to the upper command mode. However, in privileged EXEC mode.
- You can enter the **end** command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

The SWITCH supports the following command line modes:

Mode	Enter method	Description
Privileged EXEC	In user EXEC mode, input the enable command and correct password.	Switch#
Global configuration	In privileged EXEC mode, input the config terminal command.	Switch(config)#
Physical layer interface configuration	In global configuration mode, input the interface { gigaseternet tengigaseternet } <i>unit/slot/interface</i> command.	Switch(config-gigaseternet1/1/ <i>interface</i>)# Switch(config-tengigaseternet1/1/ <i>interface</i>)#
SNMP interface configuration	In global configuration mode, input the interface fastethernet 1/0/1 command.	Switch(config-fastethernet1/0/1)#
Loopback interface configuration	In global configuration mode, input the interface loopback lb-number command.	Switch(config-loopback)#
VLAN configuration	In global configuration mode, input the vlan vlan-id command.	Switch(config-vlan)#
Aggregation group configuration	In global configuration mode, input the interface port-channel channel-number command.	Switch(config-gigaseternet1/1/1-channel)#
Traffic classification configuration	In global configuration mode, input the class-map class-map-name command.	Switch(config-cmap)#
Traffic policy configuration	In global configuration mode, input the policy-map policy-map-name command.	Switch(config-pmap)#
Traffic policy configuration binding with traffic classification	In floe policy configuration mode, input the class-map class-map-name command.	Switch(config-pmap-c)#
Basic IP ACL configuration	In global configuration mode, input the access-list acl-number command. Wherein, <i>acl-number</i> ranges from 1000 to 1999.	Switch(config-acl-ipv4-basic)#
Extended IP ACL configuration	In global configuration mode, input the access-list acl-number command. Wherein, <i>acl-number</i> ranges from 2000 to 2999.	Switch(config-acl-ipv4-advanced)#

Mode	Enter method	Description
MAC ACL configuration	In global configuration mode, input the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 3000 to 3999.	Switch(config-acl-mac)#
User ACL configuration	In global configuration mode, input the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 5000 to 5999.	Switch(config-acl-map)#
MST region configuration	In global configuration mode, input the spanning-tree region-configuration command.	Switch(config-region)#
Profile configuration	In global configuration mode, input the igmp filter profile <i>profile-number</i> command.	Switch(config-igmp-profile)#
cos-remark configuration	In global configuration mode, input the mls qos mapping cos-remark <i>profile-id</i> command.	Switch(cos-remark)#
cos-to-pri configuration	In global configuration mode, input the mls qos mapping cos-to-local-priority <i>profile-id</i> command.	Switch(cos-to-pri)#
dscp-mutation configuration	In global configuration mode, input the mls qos mapping dscp-mutation <i>profile-id</i> command.	Switch(dscp-mutation)#
dscp-to-pri configuration	In global configuration mode, input the mls qos mapping dscp-to-local-priority <i>profile-id</i> command.	Switch(dscp-to-pri)#
pri-to-exp configuration	In global configuration mode, input the mls qos mapping local-priority-to-exp <i>profile-id</i> command.	Switch(pri-to-exp)#
SRED profile configuration	In global configuration mode, input the mls qos sred profile <i>profile-id</i> command.	Switch(sred)#
Flow profile configuration	In global configuration mode, enter the mls qos flow-queue profile <i>flow-profile-id</i> command.	Switch(flow-queue)#
CMAP configuration	In global configuration mode, enter the class-map <i>class-map-name</i> command.	Switch(config-cmap)#

Mode	Enter method	Description
Traffic monitoring profile configuration	In global configuration mode, enter the mls qos policer-profile <i>policer-name</i> [single] command.	Switch(traffic-policer)#
PMAp configuration	In global configuration mode, enter the policy-map <i>policy-map-name</i> command.	Switch(config-pmap)#
Traffic policy bound with traffic classification configuration	In PMAp configuration mode, enter the class-map <i>class-map-name</i> command.	Switch(config-pmap-c)#

1.1.4 Shortcut keys

The SWITCH supports the following shortcut keys:

Shortcut key	Description
Up cursor key (↑)	Show the previous command if there is any command input earlier; the display has no change if the current command is the earliest one in history records.
Down cursor key (↓)	Show the next command if there is any newer command; the display has no change if the current command is the newest one in history records.
Left cursor key (←)	Move the cursor one character to left; the display has no change if the cursor is at the beginning of command.
Right cursor key (→)	Move the cursor one character to right; the display has no change if the cursor is at the end of command.
Backspace	Delete the character before the cursor; the display has no change if the cursor is at the beginning of command.
Tab	<p>Click Tab after inputting a complete keyword, cursor will automatically appear a space to the end; click Tab again, the system will show the follow-up inputting keywords.</p> <p>Click Tab after inputting an incomplete keyword, system automatically executes partial helps:</p> <ul style="list-style-type: none"> • The system uses the complete keyword to replace input if the matched keyword is the one and only, and leave one word space between the cursor and end of keyword; • In case of mismatch or matched keyword is not the one and only, display prefix at first, then click Tab to check words circularly, no space from cursor to the end of keyword, click Space key to input the next word; • If input incorrect keyword, click Tab will change to the next line and prompt error, the input keyword will not change.
Ctrl+A	Move the cursor to the head of line.

Shortcut key	Description
Ctrl+B	Identical to the left cursor key.
Ctrl+C	Break off some running operation, such as ping, traceroute and so on.
Ctrl+D or Delete	Delete the cursor location characters
Ctrl+E	Move the cursor to the end of line.
Ctrl+F	Identical to the right cursor key.
Ctrl+K	Delete all characters behind the cursor (including cursor location).
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the down cursor key.
Ctrl+W	Identical to the up cursor key.
Ctrl+X	Delete all characters before the cursor (except cursor location).
Ctrl+Y	Show history commands .
Ctrl+Z	Return to privileged EXEC mode from other modes (except user EXEC mode).
Space or Y	When the terminal printing command line information exceeds the screen, continue to show the information in next screen.
Enter	When the terminal printing command line information exceeds the screen, continue to show the information in next line.

1.1.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to display a list of commands and brief descriptions available for each command mode.

```
switch>?
```

The command output is displayed as below.

```
clear      Clear screen
enable     Turn on privileged mode command
```

```
exit      Exit current mode and down to previous mode
help      Message about help
history   Most recent history command
language  Language of help message
list      List command
quit      Exit current mode and down to previous mode
terminal  Configure terminal
```

- After you enter a keyword, press **Space** and enter a question mark (?), all correlated commands and their brief descriptions are displayed if the question mark (?) matches another keyword.

```
Switch(config)#ntp ?
```

The command output is displayed as below.

```
peer      Configure NTP peer
refclock-master Set local clock as reference clock
server    Configure NTP server
```

- After you enter a keyword, press **Space** and enter a question mark (?), the value range and descriptions are displayed if the question mark (?) matches a parameter.

```
Switch(config)#interface ip ?
```

The command output is displayed as below.

```
<0-254> IP interface number
```

Incomplete help

You can acquire incomplete help under following three conditions:

- After you enter part of a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Switch(config)#c?
```

The command output is displayed as below.

```
cache      Cache information
```

class-map	Set class map
clear	Clear screen
cluster	Cluster configuration mode
cluster-autoactive	Cluster autoactive function
command-log	Log the command to the file
cpu	Configure cpu parameters
create	Create static VLAN

- After you enter a command, press **Space**, and enter a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

Switch(config)#**show li?**

The command output is displayed as below.

```
link-aggregation  Link aggregation
link-state-tracking  Link state tracking
```

- After you enter a partial command name and press **Tab**, the full form of the keyword is displayed if there is a unique match command. Otherwise, press **Tab** continuously to display different keywords and then you can select the required one.

Error messages

The SWITCH prints out the following error messages according to error type when you input incorrect commands:

Error message	Description
% Incomplete command.	% User inputs incomplete command.
Error input in the position marked by '^'.	Keyword marked "^" is invalid.
Ambiguous input in the position markedby '^'	Keyword marked with "^" is not clear.



Note

If there is an error message mentioned above, use the help message to solve the problem.

1.1.6 Display information

Display features

Command line interface provides the following display features:

- The help message and prompt message in CLI are displayed in English languages.
- Provide pause function when display message exceeds one screen at a time, you have the following options at this time, as shown in Table 1-1.

Table 1-1 Function keys description for command line message display characteristics

Shortcut key	Description
Press Space or y	Continue to display next screen message
Press Enter	Continue to display next line message
Press any letter key (except y)	Stop the display and command execution

Filtering displayed information

The SWITCH supports a series commands starting with **show**, for checking device configuration, operation and diagnostic information. Generally, these commands can output more information, and then user needs to add filter rules to filter out unnecessary information.

The **show** command on the SWITCH supports three kinds of filter modes:

- | **begin string**: show all lines starting from the assigned string.
- | **exclude string**: show all lines mismatch with the assigned string.
- | **include string**: show all lines only match with the assigned string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-1. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

By default, page-break is enabled.

Configure terminal page-break for the SWITCH as below.

Step	Command	Description
1	Switch#terminal page-break enable	Enable terminal page-break.

1.1.7 Command history

CLI can automatically save history commands. You can use the up cursor key (↑) or down cursor key (↓) to call the history command saved by command line repeatedly at any time.

By default, the system saves the recent 20 history commands in the cache. You can set the number of history commands saved in the system.

Configure the SWITCH as below.

Step	Command	Description
1	Switch# terminal history <i>number</i>	(Optional) configure the number of history commands saved in the system.
2	Switch# terminal time-out <i>period</i>	(Optional) configure the Console terminal timeout period.
3	Switch# history	Show history commands input by the user.
4	Switch# show terminal	Show terminal configurations of the user.

1.1.8 Restoring default value of command line

The default value of command line can be restored by **no** form or **enable | disable** form.

- **no** form: provided in the front of command line to restore the default value, disable some function, and delete some setting, etc.; used to perform some operations opposite to the original command. A command with **no** form is also known as the reverse command.
- **enable | disable** form: provided in the back or center of command line; the **enable** parameter is used to enable a feature or function, while the **disable** parameter is used to disable a feature or function.

For example:

- Use the **description text** command in physical layer interface mode to modify the interface description; use **no description** command to delete interface description and restore the default values.
- Use the **shutdown** command in physical layer interface mode to disable an interface; use the **no shutdown** command to enable an interface.
- Use the **terminal page-break enable** command in privileged EXEC configuration mode to enable terminal page-break; use the **terminal page-break disable** command to disable terminal page-break.



Note

Most configuration commands have default values, which often are restored by **no** form.

1.1.9 Logging command lines

Configure the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# command-log enable	Enable command line logging.

1.2 Accessing device

1.2.1 Introduction

The SWITCH can be configured and managed by the Command Line Interface (CLI) mode or NMS management mode.

The SWITCH CLI mode has a variety of configuration modes:

- Console mode: it must use Console mode in the first configuration.
- Telnet mode: log on through the Console mode, open Telnet service on the Switch, configure the IP address of the VLAN interface, configure the user name and password, and then take remote Telnet configuration.
- SSH mode: before accessing the SWITCH through SSH, you need to log in to the SWITCH and start the SSH service through the Console interface.

When configuring the SWITCH in network management mode, you must first configure the IP address of the VLAN interface in CLI, and then configure the SWITCH through NMS platform.

1.2.2 Accessing through Console interface

Introduction

The Console interface is a command interface used for network device to connect terminal emulation program with PC. Users can take this interface to configure and manage local device. This management method can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the SWITCH through the Console interface when network running out of order.

In the below two conditions, you can only log in to the SWITCH and configure it through the Console port:

- The SWITCH is powered on to start for the first time.
- You cannot access the SWITCH through Telnet.

Accessing device from RJ45 Console interface

If you want to access the SWITCH through PC through RJ45 Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in PC to configure communication parameters as shown in Figure 1-2, and then log in to the SWITCH.

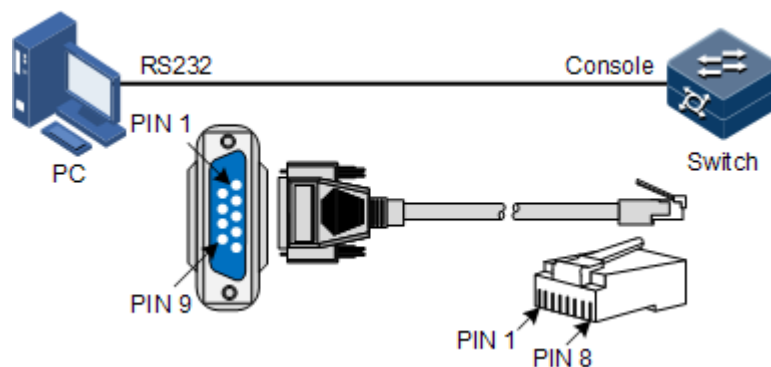


Figure 1-1 Accessing device through PC connected with RJ45 Console interface

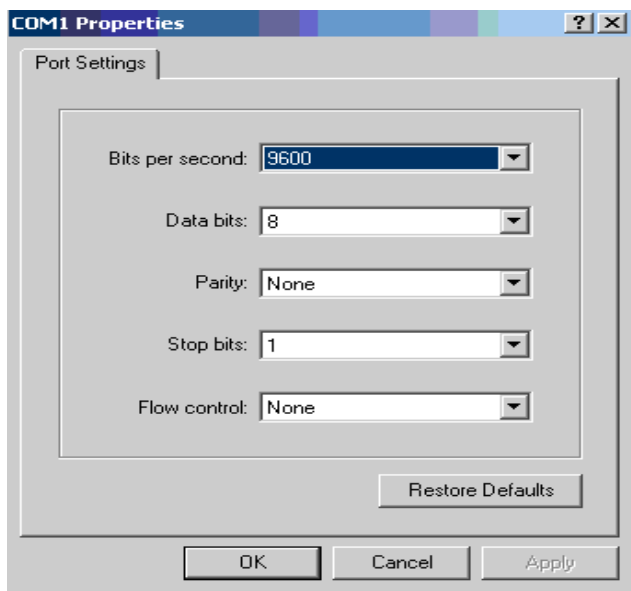


Figure 1-2 Configuring communication parameters in Hyper Terminal

1.2.3 Accessing through Telnet

You can use a PC to log in to the SWITCH remotely through Telnet. You can log in to an SWITCH from PC at first, then Telnet other SWITCH devices on the network. You do not need to connect a PC to each SWITCH.

Telnet service provided by the SWITCH including:

- Telnet Server: run the Telnet client program on a PC to log in to the SWITCH, and take configuration and management. As shown in Figure 1-3, SWITCH is providing Telnet Server service at this time.

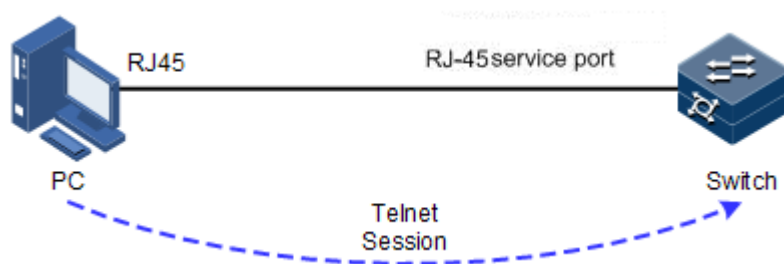


Figure 1-3 Networking with device as Telnet server

Before accessing the SWITCH through Telnet, you need to log in to the SWITCH through the Console interface and start the Telnet service. Take the following configurations on the SWITCH that needs to start Telnet service.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface fastethernet 1/0/1	Enter out-of-band network management interface configuration mode

Step	Command	Description
3	Switch(config-fastethernet1/0/1)# ip address <i>ip-address</i> [<i>ip-mask</i>]	Configure the IP address for the out-of-band network management interface.
4	Switch(config)# telnet-server accept <i>interface-type interface-list</i>	(Optional) configure the interface in support of Telnet function.
5	Switch(config)# telnet-server close terminal-telnet <i>session-number</i>	(Optional) release the specified Telnet connection.
6	Switch(config)# telnet-server max-session <i>session-number</i>	(Optional) configure the maximum number of Telnet sessions supported by the SWITCH. By default, it is 5.

- Telnet Client: when you connect to the SWITCH through the PC terminal emulation program or Telnet client program on a PC, then telnet other SWITCH and configure/manage them. As shown in Figure 1-4, Switch A not only acts as Telnet server but also provides Telnet client service.

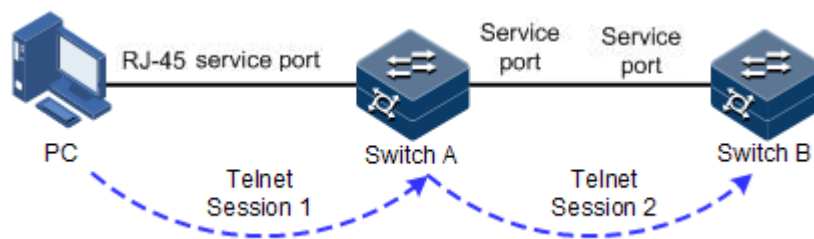


Figure 1-4 Networking with device as Telnet client

Configure Telnet Client device as below.

Step	Command	Description
1	Switch# telnet { <i>ip-address</i> <i>ipv6-address</i> } [port <i>port-id</i>]	Login other devices through Telnet.

1.2.4 Accessing through SSH

Telnet is lack of security authentication and it transports packet by Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP deceive, and routing deceiving.

The traditional Telnet and File Transfer Protocol (FTP) transmits password and data in plaintext cannot satisfy users' security demands. SSH is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provides greater security for remote login and other network services in network environment.

SSH allows data to be exchanged through TCP and it builds up a secure channel over TCP. Besides, SSH supports other service ports besides standard port 22, thus avoiding illegal attacks from the network.


Before accessing the SWITCH through SSH, you must log in to the SWITCH through Console interface and starts up SSH service.

The default configuration to accessing the SWITCH through SSH is as follows.

Function	Default value
SSH server status	Disable
Local SSH key pair length	512 bits
Key renegotiation period	0h
SSH authentication method	password
SSH authentication timeout	600s
Allowable failure times for SSH authentication	20
SSH snooping port number	22
SSH session status	Enable
SSH protocol version	v1 and v2

Configure SSH service for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# generate ssh-key length	Generate local SSHv2 key pair and designate its length. By default, the length is 512 bits.
3	Switch(config)# ssh2 server	Start the SSH server. By default, it is not started. Use the no ssh2 server command to shut down the SSH server. (Optional) configure SSH key renegotiation period.
4	Switch(config)# ssh2 server authentication { password rsa-key }	(Optional) configure SSHv2 authentication mode. By default, it is password.
5	Switch(config)# ssh2 server authentication public-key	(Optional) type the public key of the client to the SWITCH in rsa-key authentication mode.

Step	Command	Description
6	Switch(config)# ssh2 server authentication-timeout <i>period</i>	(Optional) configure the SSHv2 authentication timeout. The Gazelle S3028 refuses to authenticate the client and then closes the connection when the client authentication time exceeds this upper limit. By default, it is 600s.
7	Switch(config)# ssh2 server authentication-retries <i>times</i>	(Optional) configure the allowable failure times for SSHv2 authentication. The SWITCH refuses to authenticate the client and then closes the connection when the number of client authentication failure times exceeds the upper limit. By default, it is 20.
8	Switch(config)# ssh2 server port <i>port-number</i>	(Optional) configure SSHv2 snooping port number. By default, it is 22.  Note When configuring SSHv2 snooping port number, the input parameter cannot take effect until SSH is restarted.
9	Switch(config)# ssh2 server max-session <i>session-number</i>	(Optional) configure the maximum number of SSHv2 sessions.
10	Switch(config)# ssh2 server version { both v1 v2 }	(Optional) configure the SSHv2 protocol version.
11	Switch(config)# ssh access-list { <i>ip access-list number</i> <i>ipv6 access-list number</i> }	(Optional) configure the ACL number.
12	Switch(config)# ssh2 server close session <i>session-number</i>	(Optional) close the specified SSHv2 session.

1.2.5 Managing users

When you start the SWITCH for the first time, connect the PC through Console interface to the SWITCH, input the initial user name and password in HyperTerminal to log in and configure the SWITCH.

If there is no privilege restriction, any remote user can log in to the SWITCH through Telnet or access network by building PPP (Point to Point Protocol) connection when service interfaces are configured with IP address. This is unsafe to the SWITCH and network. Creating user for the SWITCH and setting password and privilege helps to manage the login users and ensures network and device security.

Default configurations of user management are as below.

Function	Default value
Local user information	<ul style="list-style-type: none"> • User name: admin • Password: 123456 • Level: 15
New user privilege	15
New user activation status	Activate
New user service type	N/A
Enable password	N/A
User login authentication mode	local-user
Enable login authentication mode	local-user

Configure login user management for the SWITCH as below.

Step	Command	Description
1	Switch# user name <i>user-name</i> password [cipher simple] <i>password</i>	Create or modify the user name and password.
2	Switch# user <i>user-name</i> privilege <i>privilege-level</i>	Configure login user privilege.
3	Switch# user <i>user-name</i> { allow-exec disallow-exec } <i>first-keyword</i> [<i>second-keyword</i>]	(Optional) configure the priority rule for login user to perform the command line.
4	Switch# user <i>user-name</i> service-type { lan-access ssh telnet web console all }	(Optional) configure the service type supported by the user.
5	Switch# user login { local-radius local-user radius-local [server-no-response] radius-user local-tacacs tacacs-local [server-no-response] tacacs-user }	(Optional) configure authentication mode for user login.
6	Switch# enable login { local-radius local-user radius-local [server-no-response] radius-user local-tacacs tacacs-local [server-no-response] tacacs-user }	(Optional) configure authentication mode of privileged users.
7	Switch# enable password [cipher <i>password</i>]	(Optional) modify the password for entering privileged EXEC mode. Users with the level lower than 11 do not need the password for entering privileged EXEC mode.

**Note**

- Besides the default user admin, you can create up to 9 local users.
- The login password is 8–16 characters, mandatorily including digits, case-sensitive letters, and other special characters.
- A local user with a level lower than 15, unless allowed to execute the command to modify the login password, is not allowed to modify the login password.

1.2.6 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Switch#show user table	Show login user information.
2	Switch#show user active	Show information about users logged in to the SWITCH.
3	Switch#show telnet-server	Show configurations of the Telnet server.
4	Switch#show ssh2 public-key [authentication]	Show the public key used for SSH authentication on the SWITCH and client.
5	Switch#show ssh2 { server session }	Show SSHv2 server or session information.

1.3 Managing files

1.3.1 Managing BootROM files

The BootROM files of the SWITCH include small BootROM and big BootROM.

- The small BootROM is used to boot the SWITCH.
- The big BootROM file is used to boot the SWITCH and finish device initialization. You can upgrade the big BootROM file through File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), or Secure Transfer Protocol (SFTP).

After powering on the SWITCH, run the BootROM files at first, and press **Space** to enter BootROM menu when the prompt "Press space into Bootrom menu..." appears.

**Caution**

We do not recommend doing any operation over the Small BootROM.

After being powered on, the SWITCH runs the BootROM file. When the system prompts "Press Ctrl+B to enter big boot menu", press **Ctrl+B** to enter the big BootROM menu.

In big Boot mode, you can do the following operations.

Operation	Description
t	Update system software to the SWITCH.
m	Update the boot file to the SWITCH.
b	Read system software from the SWITCH, and load it.
s	Specify the sequence of system software to be loaded upon startup.
e	Clear environment variables.
r	Reboot the SWITCH.
p	Configure the BootROM password.
?/h	Show information about system files and help.

Configure the SWITCH as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Switch# download bootstrap { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }[<i>dir</i>]	(Optional) download the big BootROM file through FTP or TFTP.
2	Switch# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.
3	Switch# upload bootstrap { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }[<i>dir</i>]	(Optional) upload the big BootROM file through FTP or TFTP.



Note

The SWITCH does not support upgrading the small BootROM through CLI.

1.3.2 Managing system files

System files are the files needed for system operation (like system startup software and configuration file). These files are usually saved in the memory. The SWITCH manages them by a file system to facilitate user managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the SWITCH supports dual-system. There are 2 sets of system software saved at the memory. These 2 sets of system software are independent. When the SWITCH fails to work due to upgrade failure, you can use another set to boot the SWITCH.

Manage system files for the SWITCH as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Switch# download system-boot { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } { system1.z system2.z }	(Optional) download the system boot file through FTP or TFTP.
2	Switch# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.
3	Switch# upload system-boot { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } { system1.z system2.z }	(Optional) upload the system boot file through FTP or TFTP.

1.3.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios to achieve different service functions. After starting the system, you can configure the SWITCH and save the configuration files. New configurations will take effect in next boot.

The configuration file has a suffix ".cfg", and can be opened by the text book program in Windows system. The contents are in the following format:

- Be saved as Mode+Command format.
- Just keep the non-default parameters to save space (see the command reference manual for default values of configuration parameters).
- Use the command mode for basic frame to organize commands. Put parameters of one mode together to form a section, and the sections are separated by the exclamation mark (!).

The SWITCH starts initialization by reading configuration files from the memory after being powered on. Thus, the configurations in configuration files are called the default configurations. If there is no configuration file in the memory, the SWITCH uses the default parameters for initialization.

The configuration that is currently used by the SWITCH is called the running configuration.

You can modify the running configuration of SWITCH through CLI. The running configuration can be used as initial configuration upon next power-on. You must use the **write** command to save running configurations in the memory and form a configuration file.

Manage configuration files for the SWITCH as below.

Step	Command	Description
1	Switch# download startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) download the startup configuration file through FTP or TFTP.
2	Switch# download backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> } [<i>dir</i>]	(Optional) down the backup configuration file through FTP or TFTP.
3	Switch# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.

Step	Command	Description
4	Switch# upload startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }[<i>dir</i>]	(Optional) upload the startup configuration file through FTP or TFTP.
5	Switch# upload backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }[<i>dir</i>]	(Optional) upload the backup configuration file through FTP or TFTP.
6	Switch# upload command-log { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }[<i>dir</i>]	(Optional) upload the command line logging file and system logs through FTP or TFTP.
7	Switch# upload logging-file { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> }	(Optional) upload the system log file through FTP or TFTP.
8	Switch# write	(Optional) save the running configuration file in the Flash.

1.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show startup-config	Show configurations loaded upon device startup.
2	Switch# show running-config	Show the running configurations.

1.4 Load and upgrade

1.4.1 Introduction

Load

Traditionally, configuration files are loaded through the serial interface, which takes a long time due to low rate and unavailable remote loading. FTP and TFTP loading modes can solve those problems and make operation more convenient.

The SWITCH supports TFTP auto-loading mode.

TFTP auto-loading refers that you can obtain the configuration files from a server and then configure the SWITCH. Auto-loading allows configuration files to contain loading related commands for multiple configurations loading to meet file auto-loading requirements in complex network environment.

The SWITCH provides several methods to confirm configuration file name in TFTP server, such as manually inputting, obtaining through DHCP, and using default name of the configuration file. Besides, you can assign certain naming conventions for configuration files, and then the SWITCH confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

Upgrade

The SWITCH needs to be upgraded if you wish to add new features, optimize functions, or fix bugs in the current software version.

The SWITCH supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

1.4.2 Upgrading system software through BootROM

You need to upgrade system software through BootROM in the following conditions:

- The device is started for the first time.
- A system file is damaged.
- The card is started improperly.

Before upgrading system software through BootROM, you should build a FTP environment, and use the PC as the FTP server and the SWITCH as the client. Basic requirements are as below.

- Configure the FTP server. Ensure that the FTP server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with IP address of the SWITCH.

Upgrade system software through BootROM for the SWITCH as below.

Step	Operation
1	Log in to the SWITCH through serial interface as the administrator, enter Privileged EXEC mode, and reboot the SWITCH with the reboot command. Swi tch# reboot

Step	Operation
2	<p>When the system successfully loads the big BootROM, and it displays " Hit any key to stop autoboot:", press any key to enter =>, and input "@" to download the image file:</p> <pre> 1970-1-1,08:13:22,16842780, tengigabitethernet1/1/28 Link change to Down. 1970-01-01,08:13:22 MIB2 LINK-3- LINK_D:tengigabitethernet1/1/28 Link Down disc.c 1689 all entries resolved start ha -num_cpus 1----- ----- haBoardEvent, BOARD_STANDBY_ACTIVE or BOARD_STANDBY_LEAVE Data smooth start. PCIE1: No link In: serial Out: serial Err: serial Net: eTSEC0: No support for PHY id 1410e20; assuming generic eTSEC0 Hit any key to stop autoboot: 0 => </pre>
3	<p>After the image is downloaded, run it until the following status appears:</p> <pre> Processing /etc/profile... Done []#cd /dev/shm tftp -gr ros 192.168.1.2 chmod +x ros ./ros Please input system partition number for upgrading(1-2):1 </pre>
4	<p>Input "b" to update the Boot software to the SWITCH.</p> <pre> => B Downloading uboot... Speed: 100, full duplex Using eTSEC0 device TFTP from server 07ff621cI4; our IP address is 07ff6040I4 Filename 'u-boot.bin'. Load address: 0x2000000 press y to confirm: y </pre>
5	<p>Input "r" to rapidly execute the big BootROM file. The SWITCH is rebooted and will load the downloaded startup file.</p>

1.4.3 Upgrading system software through CLI

Before upgrading system software through CLI, you should build a FTP/TFTP environment, and use a PC as the FTP/TFTP server and the SWITCH as the client. Basic requirements are as below.

- The SWITCH connects to the FTP/SFTP/TFTP server.
- Configure the FTP/TFTP server, and ensure that the server is available.
- Configure the IP address of the FTP/TFTP server to ensure that SWITCH can access the server.

Upgrade system software through CLI for the SWITCH as below.

Step	Command	Description
1	Switch# download system-boot { ftp ip-address user-name <i>password file-name</i> tftp ip- <i>address file-name</i> } { system1.z system2.z }	Download the system boot file through FTP.
2	Switch# boot sequence	(Optional) configure the sequence for loading system software.
3	Switch# reboot [now]	Reboot the SWITCH, and it will automatically load the downloaded system boot file.

1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show startup-config	Show information about the startup configuration file.
2	Switch# show running-config	Show information about the running configuration file.
3	Switch# show version	Show system version.

1.5 Configuring time management

1.5.1 Configuring time and time zone

To make the SWITCH to work coordinately with other devices, you must configure system time and belonged time zone accurately.

The SWITCH supports 3 system time modes, which are time stamp mode, auxiliary time mode, and default mode from high to low according to timing unit accuracy. You need to

select the most suitable system time mode manually in accordance with actual application environment.

Default configurations of time and time zone are as below.

Function	Default value
Time zone for the system	+08:00
Time zone offset	+08:00
DST status	Disable
System clock display mode	Default


Configure time and time zone for the SWITCH as below.

Step	Command	Description
1	Switch# clock set <i>hour minute second year month day</i>	Configure system time.
2	Switch# clock timezone { + - } <i>hour minute timezone-name</i>	Configure the time zone for the system.
3	Switch# clock display { default utc }	Configure system clock display mode.

1.5.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificial regulation local time system for saving energy. At present, there are nearly 110 countries running DST every summer around the world, but different countries has different stipulations for DST; so you should use local condition when configuring DST.

Configure DST for the SWITCH as below.

Step	Command	Description
1	Switch# clock summer-time enable	Enable DST.
2	Switch# clock summer-time recurring { <i>week</i> <i>last</i> } { <i>fri</i> <i>mon</i> <i>sat</i> <i>sun</i> <i>thu</i> <i>tue</i> <i>wed</i> } <i>month hour minute</i> { <i>week</i> <i>last</i> } { <i>fri</i> <i>mon</i> <i>sat</i> <i>sun</i> <i>thu</i> <i>tue</i> <i>wed</i> } <i>month hour minute offset-mm</i>	Configure calculation period for system DST.  Note Underlined command lines indicate the termination DST.

Note

- When you set system time manually, if the system uses DST, such as DST from 2 a.m. on the second Sunday, April to 2 a.m. on the second Sunday, September

every year, you have to advance the clock one hour faster during this period, set time offset as 60 minutes, and the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. The time setting by manual operation during this period shows failure.

- The summer time in southern hemisphere is opposite to the northern hemisphere, which is from September to April of next year. If you configure the start time later than the end time, the system will suppose that it is in the Southern Hemisphere. That is to say, the summer time is from the start time this year to the ending time of next year.

1.5.3 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305. It is used to perform time synchronization between the distributed time server and clients. NTP transmits data based on UDP, using UDP port 123.

NTP is used to perform time synchronization on all devices with clocks on the network. Therefore, these devices can provide various applications based on the uniformed time. In addition, NTP can ensure a very high accuracy with an error about 10ms.

Devices, which support NTP, can both be synchronized by other clock sources and can synchronize other devices as the clock source.

The SWITCH adopts multiple NTP working modes for time synchronization:

- Server/Client mode

In this mode, the client sends clock synchronization message to different servers. The servers work in server mode automatically after receiving the synchronization message and send response messages. The client receives response messages, performs clock filtering and selection, and is synchronized to the preferred server.

In this mode, the client can be synchronized to the server but the server cannot be synchronized to the client.

- Symmetric peer mode

In this mode, the active equity sends a clock synchronization message to the passive equity. The passive equity works in passive mode automatically after receiving the message and sends the answering message back. By exchanging messages, the two equities build up the symmetric peer mode. The active and passive equities in this mode can synchronize each other.

Default configurations of NTP are as below.

Function	Default value
Whether the SWITCH is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0



Caution

NTP and SNTP are mutually exclusive, so they cannot be currently configured.

Configure NTP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ntp server <i>ip-address</i> [version { <i>v1</i> <i>v2</i> <i>v3</i> }]	(Optional) configure NTP server address for the client working in server/client mode.
3	Switch(config)# ntp peer <i>ip-address</i> [version { <i>v1</i> <i>v2</i> <i>v3</i> }]	(Optional) configure NTP equity address for the SWITCH working in symmetric peer mode.
4	Switch(config)# ntp refclock-master [<i>ip-address</i>] [<i>stratum</i>]	Configure clock of the SWITCH as NTP reference clock source for the SWITCH.



Note

If the SWITCH is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

1.5.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the SWITCH with the time of the SNTP device on the network. The time synchronized by SNTP protocol is Greenwich Mean Time (GMT), which can be translated into the local time according to system settings of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent

Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# ntp server ip-address	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the SWITCH tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.

1.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show clock [summer-time-recurring]	Show configurations of the time zone and DST.
2	Switch# show sntp	Show SNTP configurations.
3	Switch# show ntp status	Show NTP configurations.
4	Switch# show ntp associations [detail]	Show information about NTP connection.

1.6 Configuring interface management

1.6.1 Introduction

Ethernet is a very important LAN networking technology which is flexible, simple and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The SWITCH supports both Ethernet electrical and optical interfaces.

Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices

should use the MDI cable while devices of the same type should use the MDI-X cable. Auto-negotiation mode devices can be connected by the MDI or MDI-X cable.

The Ethernet cable of the SWITCH supports MDI/MDI-X auto-negotiation.

1.6.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Maximum forwarding frame length of interface	2000 Bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable
Time interval of interface dynamic statistics	2s
Interface flow control status	Disable
Interface status	Enable
L2protocol peer stp status	Disable

1.6.3 Configuring basic attributes of interfaces

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and rate) are inconsistent, and then you have to adjust the interface attributes to make the devices at both ends match each other.

The Ethernet physical layer works in three modes as below:

- Half duplex: devices can receive or send messages at a time.
- Full duplex: devices can receive and send messages concurrently.
- Auto-negotiation: devices can automatically choose duplex mode by exchanging information. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode, interface rate, and flow control mode.

Configure the basic attributes of interface for the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#system mtu size</code>	Configure the MTU for all interfaces. MTU is the maximum number of Bytes allowed to pass on the interface (without fragment). When the length of the message to be forwarded exceeds the maximum value, the SWITCH will discard this message automatically.

Step	Command	Description
3	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Switch(config-gigaethernet1/1/1)# duplex { full half }	Configure the duplex mode of the interface.
5	Switch(config-gigaethernet1/1/1)# speed { auto 10 100 1000 10000 }	Configure the interface rate. It depends on specifications of the optical module for the optical interface.
6	Switch(config-gigaethernet1/1/1)# tpid { 8100 9100 88a8 }	(Optional) configure the interface TPID. By default, it is 0x8100.
7	Switch(config-gigaethernet1/1/1)# jumboframe <i>frame-size</i>	(Optional) configure the maximum framelength allowed to pass by the interface.
8	Switch(config-gigaethernet1/1/1)# mdi { across auto normal }	(Optional) configure the MDI/MDIX mode of the electrical interface.
9	Switch(config-gigaethernet1/1/1)# vibration-suppress <i>period</i> <i>second</i>	(Optional) configure the period for suppressing vibration on the interface.

1.6.4 Configuring interface rate statistics

Configure interface rate statistics for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# statistics enable	Enable statistics of the interface rate.
4	Switch(config-gigaethernet1/1/1)# clear interface statistics	Clear statistics of the interface rate.

1.6.5 Configuring flow control on interfaces

IEEE 802.3x is a flow control method for full duplex on the Ethernet data layer. When the client sends request to the server, it will send the PAUSE frame to the server if there is system or network jam. Then, it delays data transmission from the server to the client.

Configure flow control on interfaces for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# flowcontrol { receive send } { off on }	Enable/Disable interface flow control over 802.3x packets. By default, it is disabled.

1.6.6 Enabling/Disabling interfaces

Enable/Disable an interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# shutdown	Disable the current interface. Use the no shutdown command to re-enable the disabled interface.

1.6.7 Configuring L2Protocol Peer STP


To interconnect with the device that sends STP packets with the destination MAC address of 0180.C200.0008, you need to configure L2Protocol Peer STP on the SWITCH. If this function is enabled, the destination MAC address of BPDU, sent through STP, is 0180.C200.0008; otherwise, it is 0180.C200.0000.

Configure L2Protocol Peer STP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# l2protocol peer stp	Enable L2Protocol Peer STP.

1.6.8 Configuring Console interface

Configure the Console interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# console open	(Optional) enable the Console interface. Use this command in non-Console command lines only.  Caution Using the console close command to disable the Console interface causes the SWITCH to be out of control. Use it with care.
3	Switch(config)# login-trap enable	(Optional) enable sending Trap upon user login or exit.

1.6.9 Checking configurations


Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show interface [<i>interface-type interface-number</i>]	Show interface status.
2	Switch# show l2protocol peer stp [<i>interface-type interface-list</i>]	Show status of L2protocol Peer STP on the interface.

1.7 Configuring basic information

Configure basic information for the SWITCH as below.

Step	Command	Description
1	Switch# hostname name	(Optional) configure the device name. By default, the device name is Switch. The system supports changing device name to make users distinguish different devices on the network. Once the device name changes, it can be seen in terminal prompt.

Step	Command	Description
2	Switch# write	<p>Save configurations.</p> <p>Save configurations to the SWITCH after configurations, and the new configurations will overwrite the original configurations.</p> <p>Without saving, the new configurations will be lost after rebooting, and the SWITCH will continue working with the original configurations.</p> <p> Caution</p> <p>Use the erase file-name command to delete the configuration file. This operation cannot be rolled back, so use this command with care.</p>
3	Switch# reboot [now]	<p>(Optional) configure reboot options.</p> <p>When the SWITCH fails, reboot it to try to solve the problem according to actual condition.</p>

Caution

- Rebooting the SWITCH interrupts services, so use the command with care.
- Save configurations before rebooting to avoid loss of configurations.

1.8 Task scheduling

1.8.1 Introduction

When you need to use some commands periodically or at a specified time, configure task scheduling.

The SWITCH supports realizing task scheduling by combining the program list to command lines. You just need to specify the start time of the task, period, and end time in the program list, and then bind the program list to command lines to realize the periodic execution of command lines.

1.8.2 Configuring task scheduling

Configure task scheduling for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# schedule-list <i>list-number</i> start date-time { <i>mm-dd-yyyy hh:mm:ss</i> [every { day week } stop <i>mm-dd-yyyy</i> <i>hh:mm:ss</i>] every <i>days-interval time-</i> <i>interval</i> [stop <i>mm-dd-yyyy hh:mm:ss</i>] }	Create a schedule list, and configure it.
	Switch(config)# schedule-list <i>list-number</i> start date-time <i>mm-dd-yyyy hh:mm:ss</i> every weekday-list { fri mon off-day sta sun thu tue wed working-day <i>weekday-list</i> }	
	Switch(config)# schedule-list <i>list-number</i> start up-time <i>days-after-startup hh:mm:ss</i> [every <i>days-interval time-interval</i> [stop <i>days-after-startup hh:mm:ss</i>]]	
3	Switch(config)# command-string schedule- list <i>list-number</i>	Bind the command line which needs periodical execution and supports the schedule list to the schedule list.

1.8.3 Checking configurations

Use the following command to check configuration results.

No.	Command	Description
1	Switch# show schedule-list [<i>list-</i> <i>number</i>]	Show configurations of the schedule list.

1.9 Watchdog

1.9.1 Introduction

External electromagnetic field interferes with the working of single chip microcomputer, and causes program fleet and dead circulation so that the system cannot work normally.

Considering the real-time monitoring of the running state of single chip microcomputer, a program is specially used to monitor the running status of switch hardware, which is commonly known as the Watchdog.

The SWITCH will be rebooted when it fails due to task suspension or dead circulation, and without feeding the dog within a feeding dog cycle.

The Watchdog function can prevent the system program from dead circulation due to uncertain fault, thus improving stability of the system.

1.9.2 Preparing for configurations

Scenario

By configuring Watchdog, you can prevent the system program from dead circulation due to uncertain fault and thus improve the stability of system.

Prerequisite

N/A

1.9.3 Default configurations of watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable Watchdog.

1.9.4 Configuring Watchdog

Configure Watchdog for the SWITCH as below.

Step	Command	Description
1	Switch# watchdog enable	Enable Watchdog.

1.9.5 Checking configurations

Use the following command to check configuration results.

Step	Command	Description
1	Switch# show watchdog	Show Watchdog status.

1.1 Configuring Banner

1.1.1 Preparing for configurations

Scenario

Banner is a message to display when you log in to or exit the SWITCH, such as the precautions or disclaimer.


You can configure the Banner of the SWITCH as required. In addition, the SWITCH provides the Banner switch. After Banner display is enabled, the configured Banner information appears when you log in to or exit the SWITCH.

After configuring Banner, you should use the **write** command to save configurations. Otherwise, Banner information is lost when the SWITCH is rebooted.

Prerequisite

N/A

1.1.2 Configuring Banner

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# banner login <i>word</i> Press Enter. Enter text message followed by the character ' <i>word</i> ' to finish. User can stop configuration by inputting 'Ctrl+c' <i>message word</i>	Configure the Banner contents. Enter the banner login and <i>word</i> , press Enter , enters the Banner contents, and then end with the <i>word</i> character.  Note The <i>word</i> parameter is a 1-byte character. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical character. We recommend selecting the specified character that will not occur at the <i>message</i> . The message parameter is the Banner contents. Up to 2560 characters are supported.
3	Switch(config)# clear banner login	(Optional) clear contents of the Banner.

1.1.3 Enabling Banner display

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# banner enable	Enable Banner display. By default, Banner display is disabled. Use the banner disable command to disable Banner display.

1.1.4 Checking configurations

No.	Command	Description
1	Switch# show banner login	Show Banner status and contents of the configured Banner.

2 Ethernet

This chapter describes basic principles and configurations of Ethernet, and provides related configuration examples, including the following sections:

- MAC address table
- VLAN
- QinQ
- VLAN mapping
- STP/RSTP
- MSTP
- Loop detection
- Interface protection
- Port mirroring
- L2CP

2.1 MAC address table

2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches the MAC address table for the forwarding interface, implements fast forwarding of packets, and reduces broadcast traffic.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface number
- Interface VLAN ID
- Flag bits

The SWITCH supports showing MAC address information by device, interface, or VLAN.

MAC address forwarding modes

When forwarding packets, based on the information about MAC addresses, the SWITCH adopts following modes:

- **Unicast:** when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the SWITCH will directly forward the packet to the receiving port through the egress interface of the MAC address entry. If the entry is not listed, the SWITCH broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 2-1.

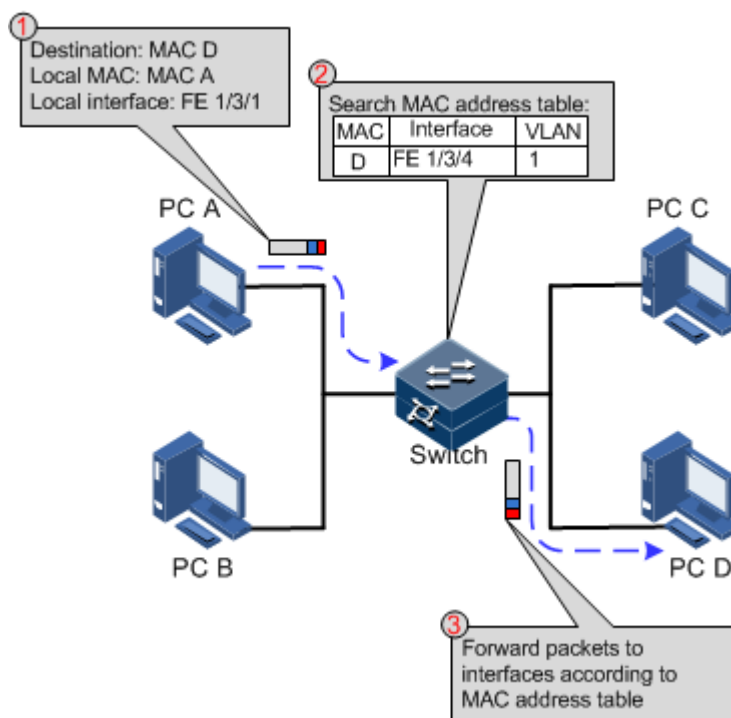


Figure 2-1 Forwarding packets according to the MAC address table

- **Multicast:** when the SWITCH receives a packet of which the destination MAC address is a multicast address, the packet will be broadcasted. If multicast is enabled and storm control over unknown packets, the packet will be sent to the specified Report interface. If no Report interface is specified, the packet will be discarded.
- **Broadcast:** when the SWITCH receives an all-F packet, or the MAC address is not listed in the MAC address table, the SWITCH forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

Classification of MAC addresses

MAC address table is divided into static address entry and dynamic address entry.

- **Static MAC address entry:** also called "permanent address", added and removed by the user manually, not aged with time. For a network with small changes of devices, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is reset.
- **Dynamic MAC address entry:** the SWITCH can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is reset.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the SWITCH. To maximize the use of the MAC address table, the SWITCH uses the aging mechanism to update the MAC address table. For example, when the SWITCH creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the SWITCH will delete the entry.

The SWITCH supports automatical aging of MAC addresses. The aging time ranges from 10s to 1000000s and can be 0. The value 0 indicates no aging.



Note

The aging mechanism takes effect on dynamic MAC addresses.

Policies of forwarding MAC addresses

The MAC address table has two forwarding policies:

When receiving packets on an interface, the SWITCH searches the MAC address table for the interface related to the destination MAC address of packets.

- If successful, it forwards packets on the related interface, records the source MAC addresses of packets, interface number of ingress packets, and VLAN ID in the MAC address table. If packets from other interface are sent to the MAC address, the SWITCH can send them to the related interface.
- If failed, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

MAC address limit

MAC address limit is to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by too large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

MAC address limit improves the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

Configure the static MAC address table in the following situations:

- The static MAC address can be configured for a fixed server, special persons (manager, financial staff, etc.), fixed and important hosts to ensure that all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.
- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.

Configure the aging time of dynamic MAC addresses to avoid saving excessive MAC address entries in the MAC address table and running out of MAC address table resources, and to achieve aging of dynamic MAC addresses.

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

Function	Default value
MAC address learning status	Enable
MAC address aging time	300s
MAC address limit	Unlimited

2.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#mac-address static unicast mac-address vlan vlan-id interface-type interface-number	Configure static unicast MAC addresses.



Note

- The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as static unicast MAC address.
- The maximum number of static unicast MAC addresses supported by the SWITCH is 1024.

2.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#mac-address blackhole mac-address vlan vlan-id	Configure blackhole MAC addresses.

2.1.6 Configuring MAC address learning

Configure MAC address learning for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch#(config) interface <i>interface type interface number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# mac-address learning enable	Enable/Disable MAC address learning.

2.1.7 Configuring MAC address limit

Configure the MAC address limit for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# mac-address threshold <i>threshold-value</i>	Configure interface-based MAC address limit.

2.1.8 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mac-address aging-time { 0 <i>period</i> }	Configure the aging time of MAC addresses.

2.1.9 Enabling inhibition of MAC address drifting

Configure MAC address policies for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mac-address mac- move enable	Enabling inhibition of MAC address drifting.

2.1.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show mac-address static [<i>interface-type interface-number</i> vlan vlan-id]	Show static unicast MAC addresses.
2	Switch# show mac-address blackhole [vlan vlan-id]	Show blackhole MAC addresses.
3	Switch# show mac-address threshold [<i>interface-type interface-number</i> vlan vlan-id]	Show dynamic MAC address limit.
4	Switch# show mac aging-time	Show the aging time of dynamic MAC addresses.
5	Switch# show mac-address learning [<i>interface-type interface-number</i> vlan]	Show status of MAC address learning.
6	Switch# show mac-address count [vlan vlan-id] [<i>interface-type interface-number</i>]	Show the number of MAC address entries.

2.1.11 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear mac-address { all blackhole dynamic static }	Clear MAC addresses.
Switch(config)# clear mac-address dynamic { port-channel <i>channel-number.sub-interface number</i> gigaethernet <i>interface-number</i> tengigaethernet <i>interface-number</i> vlan <i>vlan-id</i> <i>mac-address</i> }	Clear MAC addresses of a specified interface.
Switch(config)# clear mac-address blackhole	Clear blackhole MAC address entries in a specified VLAN.
Switch(config)# search mac-address <i>mac-address</i> { all dynamic static } [<i>interface-type interface-number</i>] [vlan <i>vlan-id</i>]	Search for a MAC address.

2.2 VLAN

2.2.1 Introduction

Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as

virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

Partitioning VLANs

There are multiple ways of partitioning VLANs, such as by interface, by MAC address, and by IP subnet, as shown in Figure 2-2.

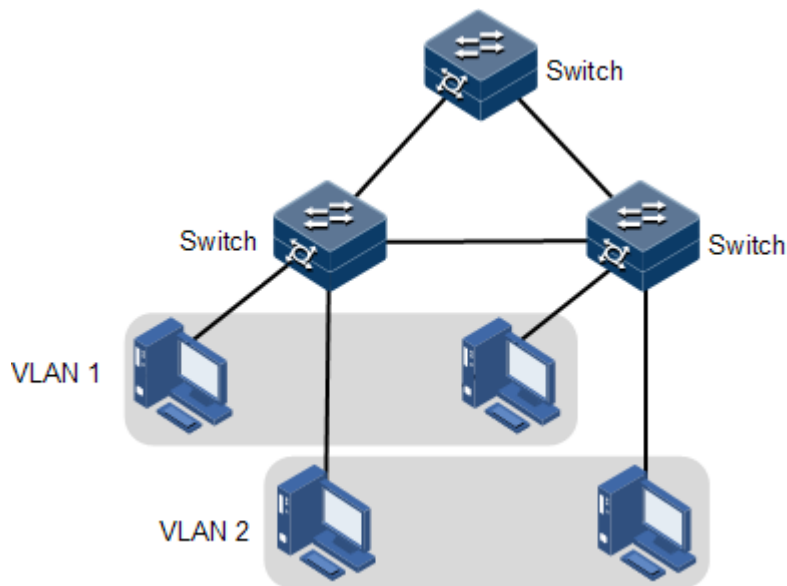


Figure 2-2 Partitioning VLANs

VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitioning improves network security, and reduces broadcast flow and broadcast storm.

The SWITCH complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- Partitioning VLANs by interface

The SWITCH supports VLAN partitioning by interface. The SWITCH has two interface modes: Access mode and Trunk mode. The method of dealing with packet for the two modes shows as below.

Table 2-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untag packets	Tag packets	
Access	Add Access VLAN Tag for packet.	<ul style="list-style-type: none"> • VLAN ID = Access VLAN ID, receive the packet • VLAN ID ≠ Access VLAN ID, discard the packet. 	<ul style="list-style-type: none"> • VLAN ID = Access VLAN ID, remove Tag and transmit the packet. • The VLAN ID list does not include the VLAN ID of the packet, discard the packet.

Interface type	Processing ingress packets		Processing egress packets
	Untag packets	Tag packets	
Trunk	Add Native VLAN Tag.	<ul style="list-style-type: none"> • Receive the packet if the packet VLAN ID is included in the permit passing VLAN ID list. • Discard the packet if the packet VLAN ID is not included in the permit passing VLAN ID list. 	<ul style="list-style-type: none"> • VLAN ID = Native VLAN ID, allow the packet to pass from the interface, remove Tag and transmit the packet. • VLAN ID ≠ Native VLAN ID, allow the packet to pass from the interface, and transmit the packet with Tag.

- Partitioning VLANs by MAC address

This refers to partitioning VLANs by the source MAC address of the packet.

- When an interface receives an Untag packet, it matches the source MAC address of the packet with the VLAN MAC addresses. If they are the same, the match is successful. In this case, the interface adds the VLAN ID specified by VLAN MAC addresses, and forwards the packet. If they are different, the interface continues to match the packet with the IP address-based VLAN and interface-based VLAN in descending order.
- When a Tag packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it; otherwise, the interface discards it.

- Partitioning VLANs by IP subnet

This refers to partitioning VLANs by the source IP subnet of the packet.

- When an interface receives an Untag packet, it determines the VLAN of the packet by the source IP subnet of the packet, and then transmits the packet in the specified VLAN.
- When a Tag packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it; otherwise, the interface discards it.

2.2.2 Preparing for configurations

Scenario

The main function of VLAN is to partition logic network segments. There are 2 typical application modes:

- One kind is that in a small LAN several VLANs are created on a device, the hosts that connect to the device are divided by VLAN. So hosts in the same VLAN can communicate, but hosts between different VLANs cannot communicate. For example, the financial department needs to be separated from other departments and they cannot access each other. Generally, the interface to connect host is in Access mode.
- The other kind is that in bigger LAN or enterprise network multiple devices connect to multiple hosts and the devices are cascaded, and data packets carry VLAN Tag for forwarding. The interfaces in the same VLAN on multiple devices can communicate, but the interfaces in different VLANs cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but

different position, the hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices like router are required if users want to communicate among different VLAN. The cascaded interfaces among devices are set in Trunk mode.

Prerequisite

N/A

2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1 and VLAN 4093
Active status of static VLAN	Suspend
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	All VLANs
Allowable Untag VLAN in Trunk mode	VLAN 1
VLAN mapping table ID	VLAN ID

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# create vlan <i>vlan-list</i> active	Create a VLAN. The command can also be used to create VLANs in batches.
3	Switch(config)# vlan <i>vlan-id</i>	Enter VLAN configuration mode.
4	Switch(config-vlan1)# name <i>vlan-name</i>	(Optional) configure the VLAN name.
5	Switch(config-vlan1)# state { active suspend }	Configure VLAN in active or suspend status.



Note

- The VLAN created by the **vlan** *vlan-id* command is in active status.
- All configurations of VLAN do not take until the VLAN is activated.

2.2.5 Configuring interface mode

Configure interface mode for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaetherne1/1/1)# switchport mode { access trunk }	Configure the interface to Access or Trunk mode.

2.2.6 Configuring VLAN on Access interface

Configure VLAN on the Access interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaetherne1/1/1)# switchport mode access Switch(config- gigaetherne1/1/1)# switchport access vlan <i>vlan-id</i>	Configure the interface to Access mode, and add the Access interface to the VLAN.
4	Switch(config- gigaetherne1/1/1)# switchport access egress-allowed vlan { all [add remove] <i>vlan-list</i> }	(Optional) configure the VLAN allowed to pass by the Access interface.



Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN permitted by the Access interface, the forwarded packets do not carry VLAN Tag.
- When setting the Access VLAN, the system creates and activates a VLAN automatically if you have not created and activated a VLAN in advance.
- If you delete or suspend the Access VLAN manually, the system will automatically set the interface Access VLAN as default VLAN.
- When configuring interface Access VLAN as non-default Access VLAN, default Access VLAN 1 is the VLAN allowed by the Access the egress interface, you can

delete Access VLAN 1 from allowed VLAN list of Access the egress interface by deleting this VLAN.

- If the configured Access VLAN is not default VLAN and there is no default VLAN in the allowed VLAN list of the Access interface, the interface does not allow default VLAN packets to pass.
- The allowed VLAN list of the Access interface is only effective to static VLANs, and ineffective to cluster VLAN, GVRP dynamic VLAN, etc.

2.2.7 Configuring VLAN on Trunk interface

Configure VLAN on the Trunk interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)#switchport mode trunk	Configure the interface to Trunk mode.
4	Switch(config-gigaetherne t1/1/1)#switchport trunk native vlan vlan-id	Configure the Native VLAN of the interface.
5	Switch(config-gigaetherne t1/1/1)#switchport trunk allowed vlan { all [add remove] vlan-list }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Switch(config-gigaetherne t1/1/1t)#switchport trunk untagged vlan { all [add remove] vlan-list }	(Optional) configure VLANs from which the Trunk interface can remove Tag.



Note

- The interface allows Native VLAN packets to pass regardless of configuration in the VLAN list and Untagged VLAN list allowed by the Trunk interface and, the forwarded packets do not carry VLAN Tag.
- The system will create and activate the VLAN if no VLAN is created and activated in advance when setting the Native VLAN.
- The system set the interface Trunk Native VLAN as default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk Untagged VLAN, the VLAN Tag is removed from the packets at the egress interface; otherwise the packets are not modified.
- If the configured Native VLAN is not default VLAN, and there is no default VLAN in Trunk interface allowed VLAN list, the interface will not allow default VLAN packets to pass.
- When setting Trunk Untagged VLAN list, the system automatically adds all Untagged VLAN into the VLAN allowed by the Trunk interface.
- The VLAN list and Untagged VLAN list allowed by the Trunk interface are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN, etc.

2.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show vlan [<i>vlan-list</i> static]	Show VLAN configurations.
2	Switch# show switchport <i>interface-type interface-number</i>	Show VLAN configurations on the interface.

2.3 QinQ

2.3.1 Introduction

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension to 802.1Q defined in IEEE 802.1ad standard.

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet takes double VLAN Tag to transmit through backbone network (public network) of the carrier. On the public network, packets are transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VLAN Tag is transmitted as data in packets.

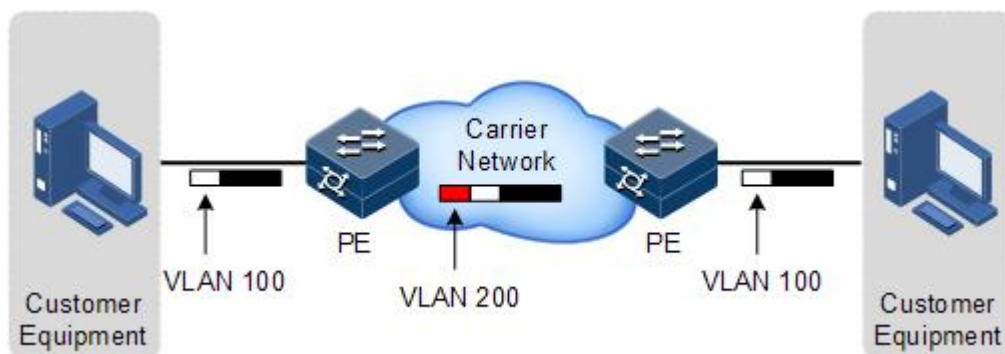


Figure 2-3 Principle of basic QinQ

Typical networking of basic QinQ is shown as Figure 2-3, the SWITCH is the PE.

The packet transmitted to the switch from user device, and the VLAN ID of packet tag is 100. The packet will be printed outer tag with VLAN 200 when passing the user side interface on the PE device and then enter the PE network.

The VLAN 200 packet is transmitted to the PE on the other end of the carrier, and then the other Switch will remove the outer tag VLAN 200 and send it to the user device. So the packet returns to the status that it carries VLAN 100 Tag only.

This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is realized by combination of interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner Tag packets.

Selective QinQ makes structure of the carrier network more flexible. You can classify different terminal users on the access device interface by VLAN Tag and then, encapsulate different outer Tags for users in different classes. On the public network, you can configure QoS policy according to outer Tag and configure data transmission priority flexibly to make users in different classes receive corresponding services.

2.3.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the SWITCH are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to layout Private VLAN ID freely to make the user device data at both ends of carrier network take transparent transmission without conflicting with VLAN ID in service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID in the user network which are divided by adding different outer VLAN Tag for voice, video, and data services etc. Then packets are forwarded to different services through different flows, and inner and outer VLAN mapping is implemented.

Prerequisite

- Connect interfaces and configure interface physical parameters to make the physical status Up.
- Create VLANs.

2.3.3 Default configurations of QinQ

Default configurations of QinQ are as below.

Function	Default value
Outer VLAN Tag TPID	0x8100
Basic QinQ status	Disable
Selective QinQ status	Disable

2.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)#switchport qinq default-cvlan <i>vlan-id</i>	Enable basic QinQ on the interface.
4	Switch(config-gigaetherne t1/1/1)#switchport reject-frame { tagged untagged }	Configure the types of packets disallowed to be forwarded.



Note

- To use basic QinQ functions on an interface, configure its attributes first by configuring it to the Access or Trunk interface and configuring the default VLAN.
- When basic QinQ is enabled on the interface, all packets are processed as Untagged packets. If you configure the Untagged packets to be discarded, Tagged packets are discarded as well.

2.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface gigaethernet1/1/1	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)#switchport qinq default-cvlan <i>vlan-id</i>	Enable basic QinQ on the interface.
4	Switch(config-gigaetherne t1/1/1)#switchport vlan-mapping cvlan <i>custom-vlan-list [cos cos-value] add-outer</i> <i>outer-vlan-id</i>	(Optional) configure selective QinQ, and add the outer VLAN ID based on inner VLAN.
5	Switch(config-gigaetherne t1/1/1)#switchport vlan-mapping-miss discard	Configure the interface to discard Tagged packets that fail to match selective QinQ or VLAN mapping rules.

Step	Command	Description
6	Switch(config-gigaetherne1/1/1) switchport vlan-mapping both { cvlan <i>vlan-id</i> untagged inner <i>vlan-id</i> priority-tagged } add-outer <i>vlan-id</i> {remove translate }	(Optional) configure bidirectional selective QinQ.



Note

To configure selective QinQ, configure basic QinQ in advance.

2.3.6 Configuring network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# switchport mode trunk	Configure interface trunk mode, permit double Tag packet to pass.

2.3.7 Configuring TPID

Configure TPID on the network side interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# mls double-tagging tpid <i>tpid</i>	Configure the TPID of the outer VLAN Tag on the interface.

2.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show dot1q-tunnel	Show configurations of basic QinQ.

No.	Command	Description
2	Switch# show switchport vlan-mapping both interface <i>interface-number</i>	Show configurations of selective QinQ.

2.4 VLAN mapping

2.4.1 Introduction

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-4 shows the principle of VLAN mapping.

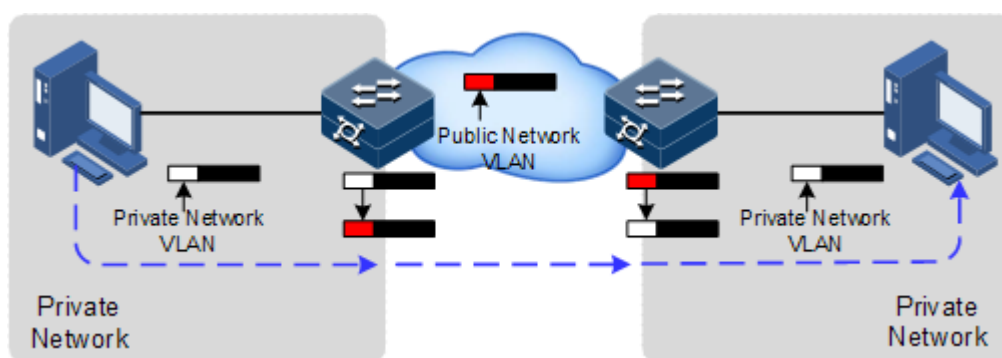


Figure 2-4 Principle of VLAN mapping

After receiving a VLAN Tag contained in a user private network packet, the SWITCH matches the packet according to configured VLAN mapping rules. If successful, it maps the packet according to configured VLAN mapping rules.

By supporting 1:1 VLAN mapping, the SWITCH replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rule.

2.4.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the carrier's VLAN mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

- A user service needs to be mapped to a carrier's VLAN ID.

- Multiple user services need to be mapped to a carrier's VLAN ID.

Prerequisite

- Connect the interface and configure its physical parameters to make it Up at the physical layer.
- Create VLANs.

2.4.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

2.4.4 Configuring 1:1 VLAN mapping

Configure 1:1 VLAN mapping for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# switchport vlan-mapping ingress <i>outer-vlan-id</i> translate <i>outer-new-vlan-id</i>	Configure the VLAN mapping rule based on outer VLAN Tag in the ingress direction of the interface, translating the outer VLAN Tag only.
4	Switch(config-gigaethernet1/1/1)# switchport vlan-mapping egress <i>outer-vlan-id</i> translate <i>outer-new-vlan-id</i>	Configure the VLAN mapping rule based on outer VLAN Tag in the egress direction of the interface, translating the outer VLAN Tag only.
5	Switch(config-gigaethernet1/1/1)# switchport vlan-mapping egress outer { all <i>outer-vlan-id</i> } { inner <i>inner-vlan-id</i> outer <i>outer-vlan-id</i> } { translate <i>vlan-id</i> remove tagged unchanged } { inner outer } { translate <i>vlan-id</i> remove tagged }]	Configure the VLAN mapping rule based on outer VLAN Tag and inner VLAN Tag in the ingress direction of the interface, translating both the outer VLAN Tag and inner VLAN Tag.
6	Switch(config-gigaethernet1/1/1)# switchport vlan-mapping ingress outer { all <i>outer-vlan-id</i> } inner { all <i>inner-vlan-id</i> } translate outer <i>outer-new-vlan-id</i>	Configure the VLAN mapping rule based on outer VLAN Tag and inner VLAN Tag in the egress direction of the interface, translating both the outer VLAN Tag and inner VLAN Tag.

2.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show switchport interface <i>interface-type interface-number</i>	Show configurations of VLAN mapping.

2.5 STP/RSTP

2.5.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 2-5.

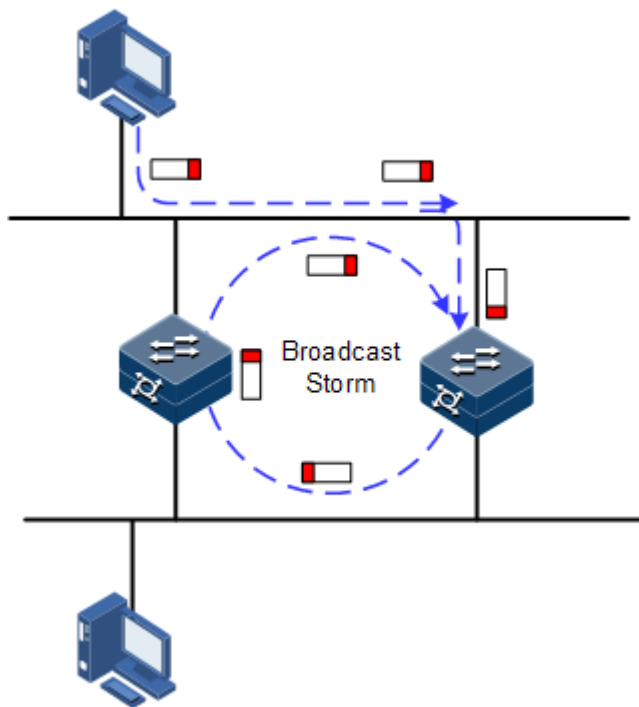


Figure 2-5 Network storm due to loopback

Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in LAN.

The SWITCH running STP can process Bridge Protocol Data Unit (BPDU) packet with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the SWITCH logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an SWITCH as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-6 shows loop networking running STP.

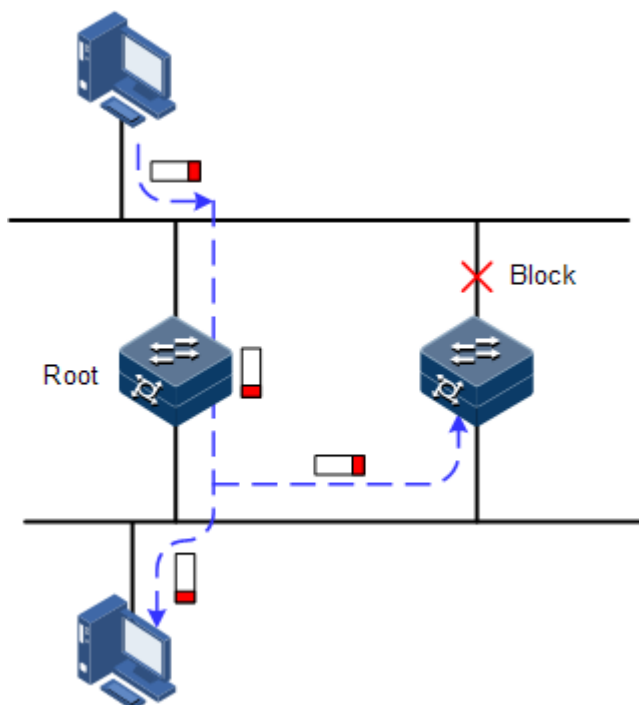


Figure 2-6 Loop networking with STP

Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergence speed.

RSTP

For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridge connection LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads the below problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- Waste of bandwidth since a link does not carry any flow after it is blocked.

- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-7, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

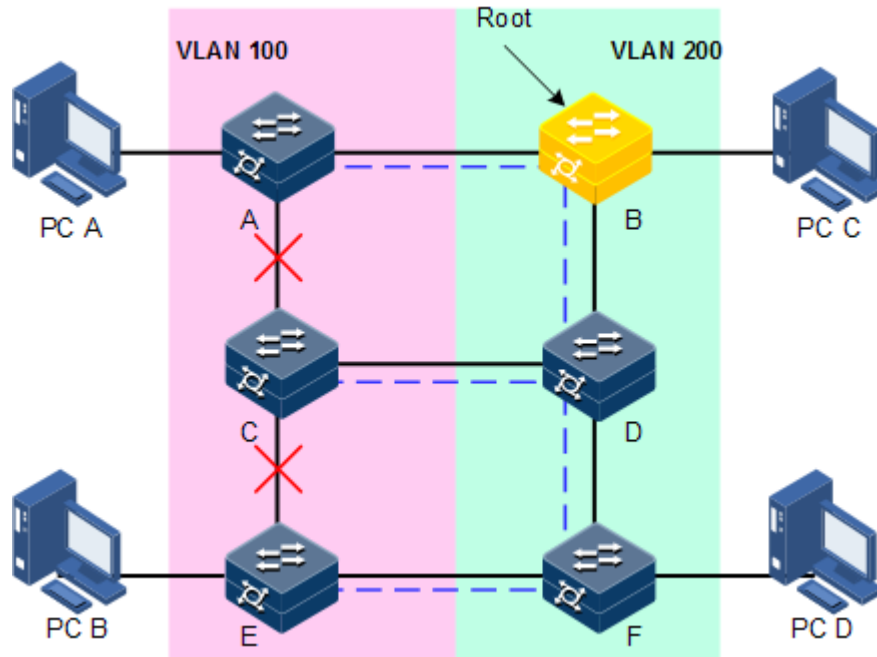


Figure 2-7 VLAN packet forward failure due to RSTP

2.5.2 Preparation for configuration

Networking situation

In a big LAN, multiple devices are concatenated for accessing each other among hosts. They need to be enabled with STP to avoid loop among them, MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame. STP calculation can block one interface in a broken loop and ensure that there is only one path from data flow to the destination host, which is also the best path.

Preconditions

N/A

2.5.3 Default configurations of STP

Default configurations of STP are as below.

Function	Default value
Global STP status	Disable
Interface STP status	Enable
STP priority of device	32768

Function	Default value
STP priority of interface	128
Path cost of interface	0
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s

2.5.4 Enabling STP

Configure STP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree enable	Enable global STP.
3	Switch(config)# spanning-tree mode { stp rstp mstp }	Configure spanning tree mode.
4	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config- gigaethernet1/1/1)# spanning-tree enable	Enable interface STP.

2.5.5 Configuring STP parameters

Configure STP parameters for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree priority <i>priority-value</i>	(Optional) configure device priorities.
3	Switch(config)# spanning-tree root { primary secondary }	(Optional) configure the SWITCH as the root or backup device.
4	Switch(config)# interface <i>interface-type interface-number</i> Switch(config- gigaethernet1/1/1)# spanning-tree priority <i>priority-value</i>	(Optional) configure interface priorities on the SWITCH.
5	Switch(config- gigaethernet1/1/1)# spanning-tree extern-path-cost <i>cost-value</i> Switch(config- gigaethernet1/1/1)# exit	(Optional) configure the path cost of interfaces on the SWITCH.

Step	Command	Description
6	Switch(config)# spanning-tree hello-time <i>value</i>	(Optional) configure the value of Hello Time.
7	Switch(config)# spanning-tree transit-limit <i>value</i>	(Optional) configure the maximum transmission rate of the interface
8	Switch(config)# spanning-tree forward-delay <i>value</i>	(Optional) configure forward delay.
9	Switch(config)# spanning-tree max-age <i>value</i>	(Optional) configure the maximum age.

2.5.6 (Optional) configuring RSTP edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device through the network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the SWITCH are set in auto-detection attribute.

Configure the edge interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# spanning-tree edged-port { auto force-true force-false }	Configure attributes of the RSTP edge interface.

2.5.7 (Optional) configuring RSTP link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# spanning-tree link-type { auto point-to-point shared }	Configure link type for interface.

2.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show spanning-tree	Show basic configurations of STP.
2	Switch# show spanning-tree <i>interface-type interface-list</i> [detail]	Show STP configuration on the interface.

2.6 MSTP

2.6.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP realizes fast convergence and distributes different VLAN flow following its own path to provide an excellent load sharing mechanism.

MSTP divides a switch network into multiple domains, called MST domain. Each MST domain contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST domain as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST domain.

Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The domain root is a local concept, which is relative to an instance in a domain. As shown in Figure 2-8, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

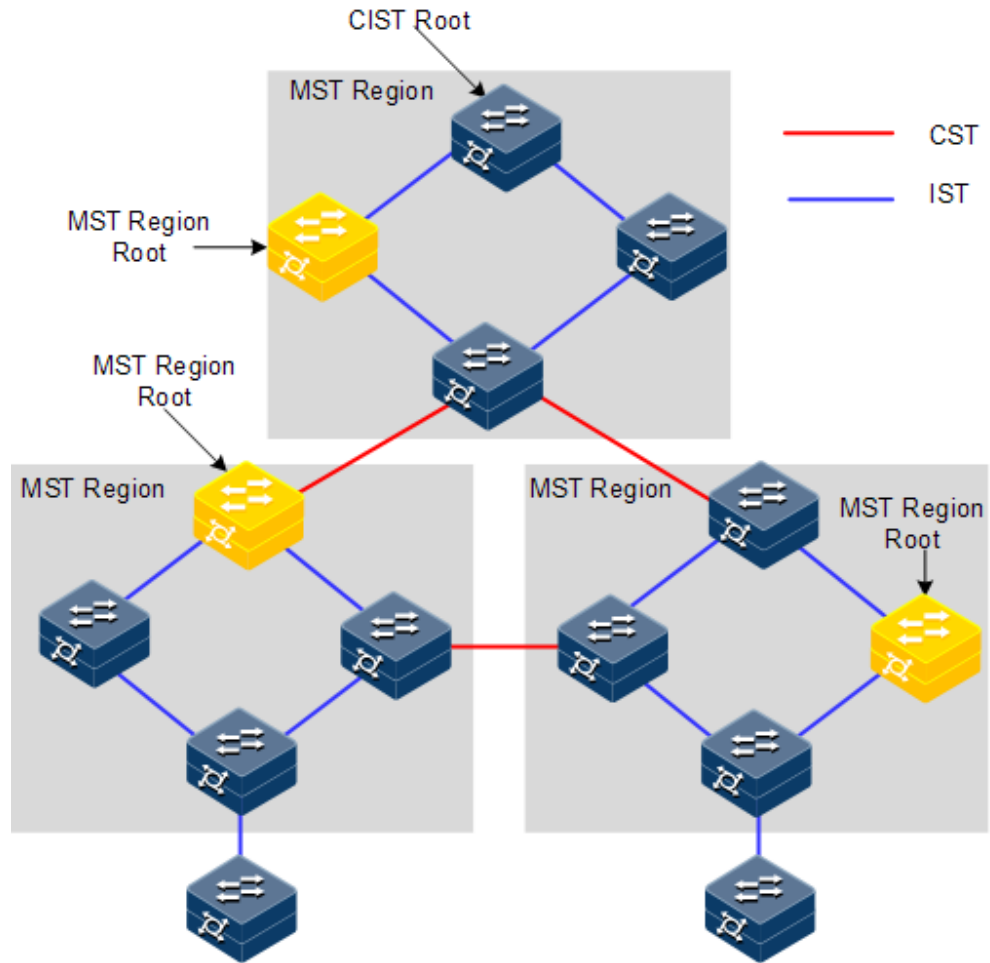


Figure 2-8 Basic concepts of the MSTI network

There can be different MST instance in each MST domain, which associates VLAN and MSTI by setting VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 2-9.

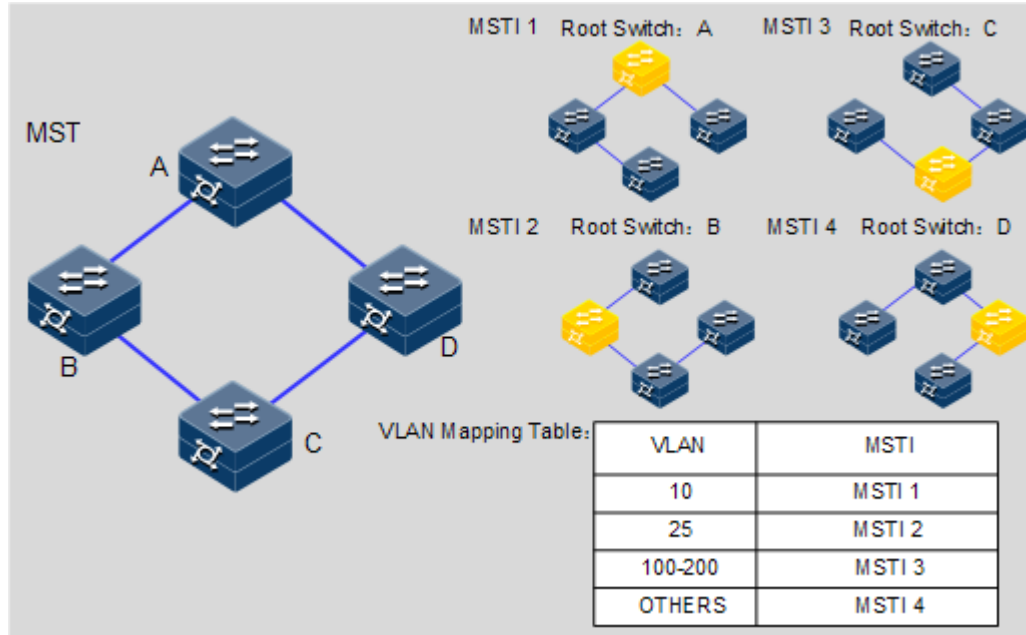


Figure 2-9 MSTI concepts



Note

Each VLAN can map to one MSTI; that is to say, data of one VLAN can only be transmitted in one MSTI but one MSTI may correspond to several VLANs.

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load sharing, similar RSTP interface status switching as well as binding multiple VLAN to one MST instance to reduce resource occupancy rate. In addition, devices running MSTP on the network are also compatible with the devices running STP and RSTP.

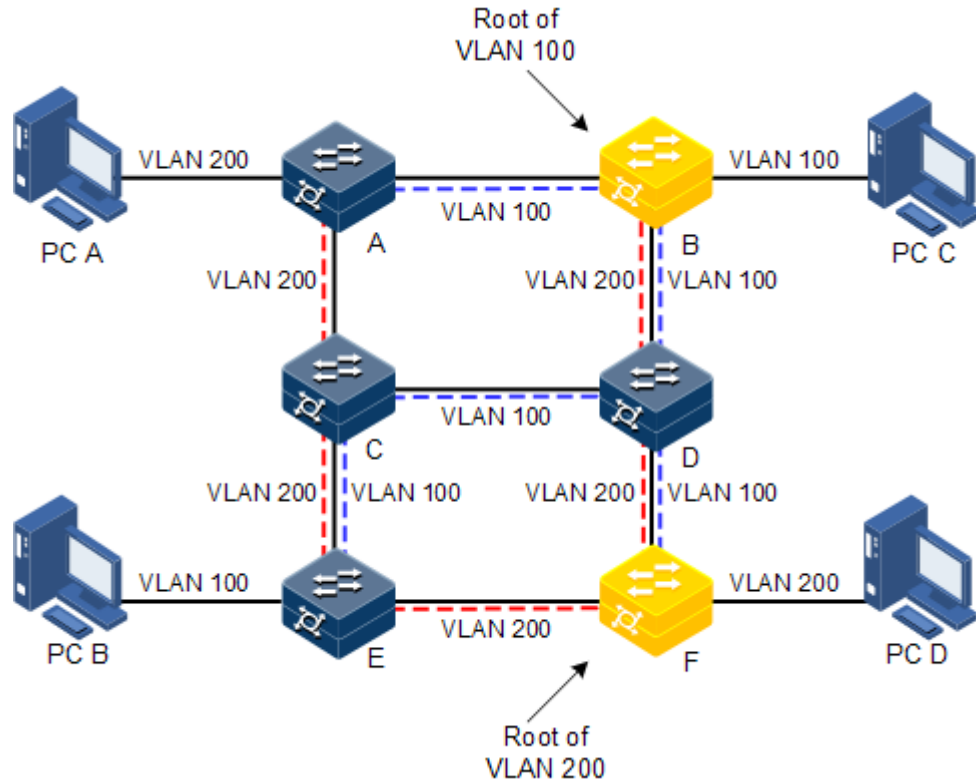


Figure 2-10 Networking of multiple spanning trees instances in MST domain

Apply MSTP to the network as shown in Figure 2-10. After calculation, there are two spanning trees generated at last (two MST instances):

- MSTI 1 takes B as the root switch, forwarding packet of VLAN 100.
- MSTI 2 takes F as the root switch, forwarding packet of VLAN 200.

In this case, all VLANs can communicate internally, different VLAN packets are forwarded in different paths to share loading.

2.6.2 Preparation for configuration

Scenario

In a big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, avoiding loop and realizing load sharing. MSTP can select different and unique forwarding paths for each one or a group of VLANs.

Prerequisite

N/A

2.6.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum numbers of hops in the MST domain	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST domain	0

2.6.4 Enabling MSTP

Enable MSTP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree mode mstp	Configure spanning tree for MSTP.
3	Switch(config)# spanning-tree enable	Enable global STP.
4	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config-gigaethernet1/1/1)# spanning-tree enable	Enable interface STP.

2.6.5 Configuring MST domain and its maximum number of hops

You can set domain information for the SWITCH when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can set current device in a specific MST domain through following configuration.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count once it is forwarded passing a device; the SWITCH discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation and then restrict MST domain scale.

Configure MSTP domain and its maximum number of hops for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree region-configuration	Enter MST domain configuration mode.
3	Switch(config-region)# name name	Configure MST domain name.
4	Switch(config-region)# revision-level level-value	Set revision level for MST domain.
5	Switch(config-region)# instance instance-id vlan vlan-list Switch(config-region)# exit	Set mapping relationship from MST domain VLAN to instance.
6	Switch(config)# spanning-tree max-hops hops-value	Configure the maximum number of hops for MST domain.



Note

Only when the configured device is the domain root can the configured maximum number of hops be used as the maximum number of hops for MST domain; other non-domain root cannot be configured this item.

2.6.6 Configuring root bridge/backup bridge

Two methods for MSTP root selection are as below:

- To configure device priority and calculated by STP to confirm STP root bridge or backup bridge.
- To assign MSTP root directly by a command.

When the root bridge has a fault or powered off, the backup bridge can replace of the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the smallest MAC address as the new root bridge.



Note

We recommend not modifying the priority of any device on the network if you directly assign the root bridge; otherwise, the assigned root bridge or backup bridge may be invalid.

Configure root bridge or backup bridge for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree [instance instance-id] root { primary secondary }	Set the SWITCH as the root bridge or backup bridge of a STP instance.



- You can confirm the effective instance of root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as root bridge or backup bridge of CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.
- The roots in device instances are mutually independent; namely, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in a spanning tree instance, a device cannot be used as the root bridge and backup bridge concurrently.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, you had better assign one root bridge and several backup bridges for a spanning tree.

2.6.7 Configuring interface priority and system priority

Whether the interface is selected as the root interface depends on interface priority. Under the identical condition, the interface with smaller priority will be selected as the root interface. An interface may have different priorities and play different roles in different instances.

The Bridge ID decides whether the SWITCH can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the SWITCH as the root. If priorities of two SWITCH devices are identical, the SWITCH with smaller MAC address will be selected as the root.

Similar to configuring root and backup root, priority is mutually independent in different instances. You can confirm priority instance through the **instance** *instance-id* parameter. Configure bridge priority for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

Configure interface priority and system priority for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i> Switch(config-gigaethernet1/1/1)# exit	Configure interface priority for a STP instance.
4	Switch(config)# spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i>	Configure system priority for a STP instance.



The value of priorities must be multiples of 4096, such as 0, 4096, and 8192. It is 32768 by default.

2.6.8 Configuring network diameter for switch network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to CIST, and invalid to MSTI instance. No matter how many nodes in a path in one domain, it is considered as just one node. Actually, network diameter should be defined as the domain number in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum number of hops of MST domain is used to measure the domain scale, while the network diameter is a parameter to measure the whole network scale. The bigger the network diameter is, the bigger the network scale is.

Similar to the maximum number of hops of MST domain, only when the SWITCH is configured as the CIST root device can this configuration take effect. MSTP will automatically set the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#spanning-tree bridge-diameter <i>bridge-diameter-value</i></code>	Configure the network diameter for the switching network.

2.6.9 Configuring inner path cost for interface

When selecting the root interface and designated interface, the smaller the interface path cost is, the easier it is to be selected as the root interface or designated interface. Inner path costs of interface are independently mutually in different instances. You can configure inner path cost for instance through the **instance** *instance-id* parameter. Configure inner path cost of interface for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure the inner path cost for the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Switch(config-gigaetherne1/1/1)# spanning-tree [instance <i>instance-id</i>] inter-path-cost <i>cost-value</i>	Configure the inner path cost on the interface.

2.6.10 Configuring external path cost on interface

The external path cost is the cost from the device to the CIST root, which is equal in the same domain.

Configure the external path cost for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# spanning-tree extern-path-cost <i>cost-value</i>	Configure the external path cost on interface.

2.6.11 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Configure maximum transmission rate on the interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree transit-limit <i>value</i>	Configure the maximum transmission rate on the interface.

2.6.12 Configuring MSTP timer

- Hello Time: the SWITCH sends the interval of bridge configuration information (BPDU) regularly to check whether there is failure in detection link of the SWITCH. The SWITCH sends hello packets to other devices around in Hello Time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network condition. Reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.

- **Forward Delay:** the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay according to actual condition; namely, reduce it when network topology changes infrequently and increase it under opposite conditions.
- **Max Age:** the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The SWITCH will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. Over short age may cause frequent recalculation of the spanning tree, while over greater age value will make STP not adapt to network topology change timely.

All devices in the whole switching network adopt the three time parameters on CIST root device, so only the root device configuration is valid.

Configure the MSTP timer for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree hello-time <i>value</i>	Set Hello Time.
3	Switch(config)# spanning-tree forward-delay <i>value</i>	Set Forward Delay.
4	Switch(config)# spanning-tree max-age <i>value</i>	Set Max Age.

2.6.13 Configuring edge interface

The edge interface indicates the interface neither directly connects to any devices nor indirectly connects to any device via network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the SWITCH are set in auto-detection attribute.

Configure the edge interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Switch(config-gigaetherne1/1/1)# spanning-tree edged-port { auto force-true force-false }	Configure attributes of the RSTP edge interface.

2.6.14 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDU packets nor process received BPDU packets.

Configure BPDU filtering for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree edged-port bpdu-filter enable interface-type interface-list	Enable BPDU filtering on the edge interface.

2.6.15 Configuring BPDU Guard

Generally, on a switch, interfaces are directly connected with terminals (such as a PC) or file servers are set to an edge interfaces. Therefore, these interfaces can be moved quickly.

In normal status, these edge interfaces will not receive BPDU packets. If somebody attacks the switch by forging the BPDU packet, the device will set these edge interfaces to non-edge interfaces when these edge interfaces receive the forged BPDU packet and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this attack. After BPDU Guard is enabled, edge interfaces can avoid attack from forged BPDU packets.

After BPDU Guard is enabled, the device will shut down the edge interfaces if they receive BPDUs and notify the NMS of the case. The blocked edge interface is restored only by the administrator through the CLI.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# spanning-tree bpduguard enable	Enable BPDU Guard.
3	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Switch(config-gigaetherne1/1/1)# no spanning-tree bpduguard shutdown port	Manually restore interfaces that are shut down by BPDU Guard.



Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU packet.

2.6.16 Configuring STP/RSTP/MSTP mode switching

When STP is enabled, three spanning tree modes are supported as below:

- STP compatible mode: the SWITCH does not implement fast switching from the replacement interface to the root interface and fast forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.
- RSTP mode: the SWITCH implements fast switching from the replacement interface to the root interface and fast forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.
- MSTP mode: the SWITCH sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of domain.

Configure the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#spanning-tree mode { stp rstp mstp }</code>	Configure spanning tree mode.

2.6.17 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Switch(config-gigaetherne1/1/1)# spanning-tree link-type { auto point-to-point shared }	Configure link type for interface.

2.6.18 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which influences network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDU packets with higher priority, the network may become unstable for the continuous election. Generally, priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. So the downlink interface cannot receive the packets higher than bridge priority unless under someone attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# spanning-tree rootguard enable	Enable/Disable root interface protection.

2.6.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant link in the topology if link backup is required. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

The spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

Loopguard is used to keep the original interface status when it cannot receive packet in a period.



Note

Loopguard and link backup are mutually exclusive; namely, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# spanning-tree loopguard enable	Configure interface loopguard attributes.

2.6.20 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show spanning-tree	Show basic configurations of STP.
2	Switch# show spanning-tree [instance <i>instance-id</i>] <i>interface-type interface-</i> <i>list</i> [detail]	Show configurations of spanning tree on the interface.
3	Switch# show spanning-tree region-operation	Show operation information about the MST domain.
4	Switch(config-region)# show spanning-tree region- configuration	Show configurations of MST domain.

2.6.21 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config-gigaethernet1/1/1)# spanning-tree clear statistics	Clear statistics of spanning tree on the interface.

2.7 Loop detection

2.7.1 Introduction

Loop detection can address the influence on network caused by a loopback, providing the self-detection, fault-tolerance and robustness.

During loop detection, an interface enabled with loop detection periodically sends loop detection packets (Hello packets). Under normal conditions, the edge interface should not receive any loop detection packets because the loop detection is applied to the edge interface.

However, if the edge interface receives a loop detection packet, it is believed that a loop occurs on the network. There are two conditions that an edge interface receives a loop detection packet: receiving a loop detection packet from itself or receiving a loop detection packet from other devices, which can be told by comparing the MAC address of the device and the MAC address carried in the packet.

Loop types

Common loop types are self-loop and internal loop.

As shown in Figure 2-11, Switch B and Switch C connect the user network.

- Self-loop: user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop on Fastethernet 1/3/2 on Switch B.
- Internal loop: the loop forming on different Ethernet interfaces of the same device. Fastethernet 1/3/1 and Fastethernet 1/3/3 on Switch C forms an internal loop with the user network A.

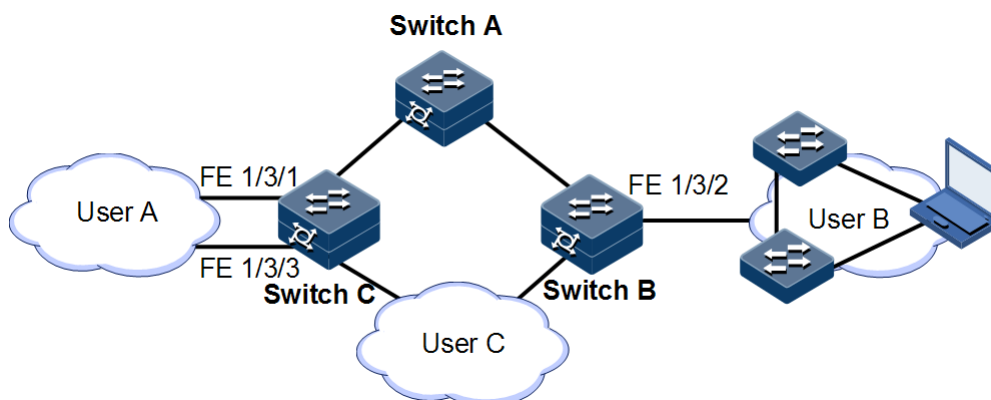


Figure 2-11 Loop detection networking

Principle for processing loops

The SWITCH processes loops as below:

- If the device sending the loop detection packet is not the one receiving the packet, process the device with the larger MAC address to eliminate the loop (external loop).
- If the device sending the loop detection packet is the one receiving the packet but the interface sending the packet and the interface receiving the packet are different, process the interface with the larger interface ID to eliminate the loop (internal loop).
- If the interface sending the packet and the interface receiving the packet are the same, process the interface to eliminate the loop (self-loop).

In Figure 2-11, assume that both Switch B and Switch C connect user network interfaces enabled with loop detection. The system processes loops for the three loop types as below:

- Self-loop: the interface sending the packet and the interface receiving the packet on Switch B are the same, the configured loop detection action will be taken to eliminate the loop on Fastethernet 1/3/2.
- Internal loop: Switch C will receive the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface number, namely, Fastethernet 1/3/3.

Action for processing loops

The action for processing loops is the method for the SWITCH to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

- Discarding: block the interface and send Trap.
- Trap-only: send Trap only.
- Shutdown: shut down the interface and send Trap.

Loop detection modes

The loop detection modes consist of port mode and VLAN mode:

- Port mode: when a loop occurs, the system blocks the interface and sends Trap in the loopback processing mode of discarding, or shuts down the physical interface and sends Trap information in the loopback processing mode of shutdown.
- VLAN mode: when a loop occurs,
 - In the loopback processing mode of discarding, when a loop occurs on one or more of VLANs to which the interface belongs, the system blocks the VLANs with loop and leaves other VLANs to normally receive or send packets.
 - In the loopback processing mode of shutdown, the system shuts down the physical interface and sends Trap information.

If the loop detection processing mode is Trap-only in the previous two modes, the SWITCH sends Trap only.

Loop restoration

After an interface is blocked or shut down, you can configure it, such as no automatic restoration and automatic restoration after a specified period.

- If an interface is configured as automatic restoration after a specified period, the system will start loop detection after the period. If the loop disappears, the interface will be restored; otherwise, it will be kept in blocking or shutdown status.
- If an interface is configured as no automatic restoration, namely, the automatic restoration time is infinite; it will not be automatically restored. However, you can use the **no loopback-detection discarding** command to manually restore the interface blocked or shut down upon loop detection.

2.7.2 Preparing for configurations

Scenario

On the network, hosts or Layer 2 devices connected to access devices may form a loopback intentionally or involuntarily. Enable loop detection on downlink interfaces of all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loopback is detected on an interface, the interface will be blocked.

Prerequisite

Loopback interface, interface backup, STP, G.8032, and RRPS interfere with each other. We do not recommend configuring two or more of them concurrently.

2.7.3 Default configurations of loop detection

Default configurations of loop detection are as below.

Function	Default value
Loop detection status	Disable
Automatic recovery time for the blocked interface	5 multiples of the period for sending packets
Mode for processing detected loops	Block (discard-vlan)
Loop detection period	<ul style="list-style-type: none"> Based on interface: 1s Based on interface+VLAN: 5s
Loop detection mode	0 (printing log information aperiodically)

2.7.4 Configuring loop detection



Note

- Loop detection and STP are exclusive, so only one can be enabled at one time.
- Loop detection cannot be concurrently enabled on both two directly-connected devices.

Configure loop detection based on interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)#loopback-detection [pkt-vlan { untag <i>vlan-id</i> }] [hello-time <i>second</i>] [restore-time <i>second</i>] [action { block trap-only shutdown }] [log-interval <i>log-interval-value</i>]	<p>Enable loop detection on the interface.</p> <p>(Optional) configure the VLAN for sending packets.</p> <p>(Optional) configure the time for automatically recover the blocked interface due to loop detection and the mode for processing loops</p> <p>(Optional) configure the logging period.</p>
4	Switch(config-gigaetherne t1/1/1)#loopback-detection manual restore	Manually restore the interface blocked due to loop detection.

Configure loop detection based on interface+VLAN for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)# loopback-detection detect- vlanlist <i>vlan-id</i> [hello- time <i>second</i>] [restore-time <i>second</i>] [action { shutdown discard-vlan trap- only }] [log-interval <i>log- interval-value</i>]	Enable loop detection on the interface. Configure the VLAN list for loop detection. (Optional) configure the period for sending Hello packets. (Optional) configure the time for automatically recover the blocked interface due to loop detection and the mode for processing loops (Optional) configure the logging period.
4	Switch(config-gigaetherne t1/1/1)# loopback- detection manual restore	Manually restore the interface blocked due to loop detection.

2.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show loopback-detection [<i>interface-type interface- number</i>] [detail]	Show configurations and status of loop detection.

2.7.6 Maintenance

Maintain the SWITCH by below commands.

Command	Description
Switch(config-gigaetherne t1/1/1)# clear loopback- detection statistic	Clear statistics of loop detection.

2.8 Interface protection

2.8.1 Introduction

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2/Layer 3 data in the interface protection group.

This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface protection, interfaces in an interface protection group cannot transmit packets to each other. Interfaces in and out of the interface protection group can communicate with each other. So do interfaces out of the interface protection group.

2.8.2 Preparing for configurations

Scenario

The interface protection function can realize mutual isolation of interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

Prerequisite

N/A

2.8.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.8.4 Configuring interface protection



Caution

Interface protection is unrelated with the VLAN to which the interface belongs.

Configure interface protection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# switchport protect	Enable interface protection.

2.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show switchport protect	Show interface protection configuration.

2.9 Port mirroring

2.9.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source interface to the destination interface, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on an interface through this function and analyze the relevant network conditions.

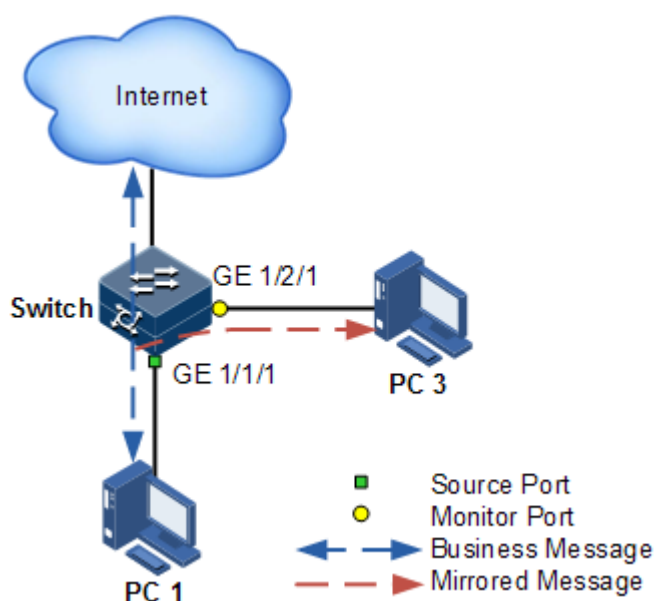


Figure 2-12 Port mirroring principle

The basic principle of port mirroring is shown in Figure 2-12. PC 1 connects to the external network via the GigabitEthernet 1/1/1; PC 3 is the monitor PC, connecting the external network through GigabitEthernet 1/2/1.

When monitoring packets from the PC 1, you need to assign GigabitEthernet 1/1/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GigabitEthernet 1/2/1 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the switch, the switch will forward and copy them to monitor port (GigabitEthernet 1/2/1). The monitor device connected to mirror the monitor port can receive and analyze these mirrored packets.

The SWITCH supports data stream mirroring on the ingress port and egress port. The packets on ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

2.9.2 Preparing for configurations

Scenario

Port mirroring is used to monitor the type and flow of network data regularly for network administrator.

Port mirroring copies the port flow monitored to a monitor port or CPU to obtain the ingress/egress port failure or abnormal flow of data for analysis, discovers the root cause, and solves them timely.

Prerequisite

N/A

2.9.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

Function	Default value
Port mirroring status	Disable
Mirroring the source interface	N/A
Monitor interface	Gigaethernet 1/1/1

2.9.4 Configuring port mirroring on local port

Configure local port mirroring for the SWITCH as below.

Step	Configure	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mirror-group <i>group-id</i>	Create a port mirroring group.
3	Switch(config)# interface <i>interface-type interface-number</i> Switch(config-gigaethernet1/1/1)# portswitch	Enter Layer 2 physical interface configuration mode.
4	Switch(config-gigaethernet1/1/1)# mirror-group <i>group-id</i> monitor-port	Configure the monitor port for mirroring.
5	Switch(config-gigaethernet1/1/1)# mirror-group <i>group-id</i> source-port { ingress egress }	Configure the mirroring port of port mirroring, and designate the mirroring rule for port mirroring. Port mirroring supports mirroring packets in both the ingress and egress directions of the port.

Step	Configure	Description
6	Switch(config- gigaetherne1/1/1)# exit Switch(config)# mirror-group <i>group-id</i> source-cpu [ingress egress]	Configure mirroring packets to CPU or specified monitor port.

2.9.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show mirror-group [<i>group-id</i>]	Show configurations of port mirroring.

2.10 L2CP

2.10.1 Introduction

Metro Ethernet Forum (MEF) introduces service concepts, such as EPL, EVPL, EP-LAN, and EVP-LAN. Different service types have different processing modes for Layer 2 Control Protocol (L2CP) packets.

MEF6.1 defines processing modes for L2CP as below.

- **Discard:** discard the packet, by applying the configured L2CP profile on the ingress interface of the SWITCH, to complete configuring processing mode.
- **Peer:** send packets to the CPU in the same way as the discard action.
- **Tunnel:** send packets to the MAN. It is more complex than discard and peer mode, requiring cooperating profile at network side interface and carrier side interface tunnel terminal to allow packets to pass through the carrier network.

2.10.2 Preparing for configurations

Scenario

On the access device of MAN, you can configure profile on user network interface according to services from the carrier to configure L2CP of the user network.

Prerequisite

N/A

2.10.3 Default configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Applying the profile on the interface	Disable
Interface tunnel terminal status	Disable
Specified multicast destination MAC address	0x0100.0ccd.cdd0
Description of the L2CP profile	N/A

2.10.4 Configuring global L2CP

Configure global L2CP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# l2cp-process tunnel destination-address mac-address	(Optional) configure the destination MAC address for transparently transmitted packets.

2.10.5 Configuring L2CP profile

Configure the L2CP profile for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# l2cp-process profile profile-number	Create and enter the L2CP profile.
3	Switch(config-l2cp-profile)# name string	(Optional) add profile description.
4	Switch(config-l2cp-profile)# l2cp-process protocol { oam stp dot1x lacp lldp cdp vtp pvst e1mi udld pagp all } action { tunnel drop peer }	(Optional) configure the mode for processing L2CP packets.
5	Switch(config-l2cp-profile)# tunnel vlan vlan-id	(Optional) configure the specified VLAN for transparent transmission.
6	Switch(config-l2cp-profile)# tunnel interface-type interface-number	(Optional) configure the specified egress interface for transparent transmission.
7	Switch(config-l2cp-profile)# tunnel tunnel-type mac	(Optional) configure the type of the tunnel for transparent transmission.

2.10.6 Configuring L2CP profile on interface

Configure the L2CP profile on interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# l2cp-process profile <i>profile-number</i>	Apply the L2CP profile on the interface.

2.10.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Switch# show l2cp-process profile [<i>profile-number</i>]	Show information about the created L2CP profile.
2	Switch# show l2cp-process [<i>interface-type interface-number</i>]	Show configurations of L2CP on the interface.
3	Switch# show l2cp-process tunnel statistics [<i>interface-type interface-number</i>]	Show statistics of L2CP packets on the interface.

2.10.8 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear l2cp-process tunnel statistic [<i>interface-type interface-number</i>]	Clear statistics of L2CP packets on the interface.

3 Ring network protection

This chapter describes ring network protection, and provides related configuration examples, including the following sections:

- G.8032
- **Ошибка! Источник ссылки не найден.**

3.1 G.8032

3.1.1 Introduction

G.8032 is an APS protocol over ITU-T G.8032 recommendation. It is specially used in Ethernet ring link protocol. Generally, G.8032 can avoid broadcast storm caused by data loopback. When Ethernet has loop or device malfunction, G.8032 can switch the link to backup link and ensure service restore quickly.

G.8032 takes the control VLAN in ring network to transmit ring network control information and meanwhile, combining with the topology feature of ring network to discover network fault quickly and enable backup link to restore service fast.

3.1.2 Preparing for configurations

Scenario

With the development from Ethernet to the telecom-grade network, voice and video multicast services bring forth higher requirements on Ethernet redundant protection and fault-restore time. The fault-restore convergent time of current STP system is in second level that is far away to meet requirement. G.8032 can blocks a loop to avoid broadcast storm by defining different roles in the ring under normal situations. G.8032 can switch the service link to the backup link if the ring link or node fails, thus eliminating loops, conducting fault Automatic Protection Switching (APS) and automatic fault restoration. In addition, the APS time is shorter than 50ms. It supports the single ring, intersecting ring, and tangent rings networking modes.

G.8032 supports fault detection based on physical interface status, which helps obtain link fault and implement quick switching, available to neighbor devices.

Prerequisite

- Connect interface and configure physical parameters for it, the interface is Up at physical layer.
- Create VLANs.
- Add interfaces into VLANs.

3.1.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

Function	Default value
Protocol VLAN	1
Protection ring	Revertive mode
Ring WTR timer	5min
Version of the ring protocol	2
Guard timer	500ms
Ring HOLDOFF timer	0
G.8032 fault information reported to network management system	Disable
Sub-ring virtual path mode in intersecting node	with
Ring Propagate switch in intersecting node	Disable

3.1.4 Creating G.8032 ring


Create a G.8032 ring for the SWITCH as below.




Caution

- Only one device can be configured as the RPL (Ring Protection Link) Owner in a ring, and one device as the RPL Neighbour, other devices can only be configured as ring forwarding nodes.
- A tangent ring can be taken as two independent rings in fact, and its configurations are identical to common single rings. The intersecting ring has a master ring and a sub-ring; for its configurations, see section 3.1.5 (Optional) creating G.8032 sub-ring.

Step	Command	Description
1	swi tch# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Switch(config)#ethernet ring- protection ring-id east { interface-type interface- number port-channel port- channel-number } west { interface-type interface- number port-channel port- channel-number } [node-type rpl-owner rpl { east west }] [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]</pre>	<p>Create a ring and configure the node as the RPL Owner.</p> <p> Note The east-bound and western-bound interface cannot be identical.</p>
	<pre>Switch(config)#ethernet ring- protection ring-id east { interface-type interface- number port-channel port- channel-number } west { interface-type interface- number port-channel port- channel-number } node-type rpl-neighbour rpl { east west } [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]</pre>	<p>Create a ring and configure node as RPL Neighbour.</p>
	<pre>Switch(config)#ethernet ring- protection ring-id east { interface-type interface- number port-channel port- channel-number } west { interface-type interface- number port-channel port- channel-number } [not- revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]</pre>	<p>Create a ring and configure node as ring forwarding node.</p>
3	<pre>Switch(config)#ethernet ring- protection ring-id name string</pre>	<p>(Optional) configure the ring name. The length of name cannot exceed 32 characters.</p>
4	<pre>Switch(config)#ethernet ring- protection ring-id version { 1 2 }</pre>	<p>(Optional) configure protocol version. All nodes in one ring must be consistent. Version 1 differentiates rings through protocol VLAN, so different rings need to be configured with different protocol VLANs. So does version 2.</p>


Step	Command	Description
5	Switch(config)# ethernet ring-protection ring-id guard-time guard-time	(Optional) after configured with the Guard timer, the faulty node does not process APS protocol packets during restoration time. In some big ring network, restoring node fault immediately may receive fault notice from neighbor nodes and cause link Down. Configuring the Guard timer of the ring can solve this problem.
6	Switch(config)# ethernet ring-protection ring-id wtr-time wtr-time	(Optional) configure the WTR timer of the ring. In revertive mode, wait the WTR timer to expire to switch back current link when the current link restores from a fault.
7	Switch(config)# ethernet ring-protection ring-id holdoff-time holdoff-time	(Optional) the system delays reporting the fault when the current link becomes faults after configuring the HOLDOFF timer of the ring; namely, traffic will switch to the protection link after a delayed time. This can avoid current link switching frequently.  Note If the HOLDOFF timer is set over greater, the performance of 50ms switching will be affected. Thus it is set to 0 by default.
8	Switch(config)# ethernet ring-protection trap enable	(Optional) enable G.8032 fault information to be reported to NMS.

3.1.5 (Optional) creating G.8032 sub-ring

Caution

- Only the intersecting ring network contains the master ring and sub-ring.
- Configurations of a master ring are identical to configurations of a single ring or tangent ring. For details, see section 3.1.4 Creating G.8032 ring.
- Configure the master ring before configuring the sub-ring; otherwise, the sub-ring cannot find the interface of the master ring and the virtual path of the sub-ring cannot be established.
- The sub-ring ID must be greater than the ID of the master ring.
- Configurations of a Non-intersecting node in a sub-ring are identical to configurations of a single ring or tangent ring. For details, see section 3.1.4 Creating G.8032 ring for details.

Create a G.8032 sub-ring for SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet ring-protection ring-id { east west } { interface-type interface-number port-channel port-channel-number } node-type rpl-owner [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]	<p>Create sub-ring and configure node as RPL Owner on intersecting node.</p> <p>A protection ring changes to non-revertive mode if configured with the not-revertive parameter. Traffic switches back to the current link from protection link after the fault of the current link is cleared; however, traffic does not switch in non-revertive mode.</p> <p>By default, the protection ring is in revertive mode.</p> <p> Note</p> <p>The link between two intersecting nodes in intersecting rings belongs to the master ring, so either east-bound or wester-bound interface can be configured for sub-ring.</p>
	Switch(config)# ethernet ring-protection ring-id { east west } { interface-type interface-number port-channel port-channel-number } node-type rpl-neighbour [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]	Create a sub-ring, and configure the node as the RPL Neighbour on intersecting nodes.
	Switch(config)# ethernet ring-protection ring-id { east west } { interface-type interface-number port-channel port-channel-number } [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan-list]	Create a sub-ring, and configure the node as ring forwarding node on intersecting nodes.

Step	Command	Description
3	Switch(config)# ethernet ring-protection ring-id raps-vc { with without }	<p>(Optional) configure sub-ring virtual path mode on the intersecting node. Protocol packets transmitted in the sub-ring are different from that transmitted on the master ring, including with mode and without mode:</p> <ul style="list-style-type: none"> • with: the primary ring provides access for sub-ring APS packet; the intersecting node in the sub-ring will transmit sub-ring APS packets to the primary ring to use primary ring to complete the communications among sub-ring intersecting nodes. • without: the sub-ring APS packets on cross nodes need to be ended and cannot be transmitted to the primary ring. This mode requires the sub-ring not to block sub-ring protocol VLANs (to ensure sub-ring packets to pass through Owner). <p>By default, sub-ring virtual path is configured with the with parameter. Configuration mode of two intersecting nodes must be consistent.</p>
4	Switch(config)# ethernet ring-protection ring-id propagate enable	<p>Enable the ring Propagate switch on intersecting nodes.</p> <p>Sub-ring data needs to be forwarded by the master ring, so the sub-ring MAC address table also exists on the master ring device. When the sub-ring has fault, the Propagate switch notifies the master ring of refreshing the MAC address table in time and thus avoids flow loss.</p> <p>By default, the Propagate switch is disabled. Use the ethernet ring-protection ring-id propagate disable command to disable this function.</p>

3.1.6 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet ring-protection ring-id force-switch { east west }	Configure FS of ring flow to east or west. FS can be configured on multiple interfaces of multiple ring nodes.

Step	Command	Description
3	Switch(config)# ethernet ring-protection <i>ring-id</i> manual-switch { east west }	Configure MS of traffic on the ring to east or west. MS has a lower priority than FS or APS upon fault of the current link. MS can be configured on only one interface of a ring node.
4	Switch(config)# clear ethernet ring-protection <i>ring-id</i> { command statistics }	Clear switch control command, including force-switch and manual-switch , WTR timer, and WTB timer.



Note

By default, traffic will switch to the protection link when the current link fails. Thus G.8032 is needed in some special conditions.

3.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ethernet ring-protection	Show G.8032 ring configuration.
2	Switch# show ethernet ring-protection status	Show G.8032 ring status information.
3	Switch# show ethernet ring-protection statistics	Show G.8032 ring statistics.

3.1.8 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear ethernet ring-protection <i>ring-id</i> statistics	Clear protection ring statistics.

4 IP services

This chapter describes basic principle and configuration of routing features, and provides the related configuration examples, including the following sections:

- IP basis
- Loopback interface
- ARP
- NDP
- Static route
- Configuring OSPF

4.1 IP basis

4.1.1 Introduction

The IP interface is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices.

4.1.2 Preparing for configurations

Scenario

Configure the IP address of each VLAN interface and loopback interface.

Prerequisite

Configure VLAN associated with interface and activate it.

4.1.3 Default configurations of the Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Function	Default value
Management VLAN TPID	0x8100

Function	Default value
Management VLAN inner VLAN	1
Management VLAN CoS	0
IP address of IP interface 0	192.168.0.1

4.1.4 Configuring IPv4 address of VLAN interface

Configure the IPv4 address of the VLAN interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Switch(config-vlan1)# ip address <i>ip-address</i> [<i>ip-mask</i>] [sub]	Configure the IP address of the VLAN interface. Use the no ip address <i>ip-address</i> command to delete configuration of the IP address.



Note

Up to 255 IP interfaces can be configured, and they range from 0 to 254.

4.1.5 Configuring IPv6 address of VLAN interface

Configure the IPv6 address of the VLAN interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface vlan <i>vlan-id</i>	Enter Layer 3 interface configuration mode.
3	Switch(config-vlan1)# ipv6 address <i>ipv6-address/prefix-length</i> [sub]	Configure the IPv6 address of the VLAN interface.

4.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip interface brief	Show configurations of the IP address of the IP interface.

No.	Command	Description
2	Switch# show ipv6 interface brief	Show configurations of the IPv6 address of the IP interface.

4.2 Loopback interface

4.2.1 Introduction

The loopback interface is a virtual interface and can be classified into two types:

- Loopback interface automatically created by the system: the IP address is fixed to 127.0.0.1. This type of interfaces receives packets that sent to the device. It does not broadcast packets through routing protocols.
- Loopback interface created by users: without affecting physical interface configurations, configure a local interface with a specified IP address, and make the interface Up permanently so that packets can be broadcasted through routing protocols.

Loopback interface status is free from physical interface status (Up/Down). As long as the SWITCH is operating normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

4.2.2 Preparing for configurations

Scenario

Use the IP address of the loopback interface to log in through Telnet so that the Telnet operation does not become Down due to change of physical status. The loopback interface ID is also used as the router ID of dynamic routing protocols, such as OSPF, to uniquely identify a device.

Prerequisite

N/A

4.2.3 Default configurations of the loopback interface

N/A

4.2.4 Configuring IP address of the loopback interface

Configure the IP address of the loopback interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface loopback <i>lb-number</i>	Enter loopback interface configuration mode.

Step	Command	Description
3	Switch(config-loopback)# ip address <i>ip-address</i> [<i>ip-mask</i>]	Configure the IP address of the loopback interface.

4.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show interface loopback	Show loopback interface configurations.

4.3 ARP

4.3.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and set mapping relationship between IP address and MAC address.

ARP address mapping table includes the following two types:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
 - Static ARP address entry needs to be added/deleted manually.
 - No aging to static ARP address.
- Dynamic entry: MAC address automatically learned through ARP.
 - This dynamic entry is automatically generated by switch. You can adjust partial parameters of it manually.
 - The dynamic ARP address entry will be aged after the aging time if not used.

The SWITCH supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the SWITCH learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.
- learn-reply-only mode: in this mode, the SWITCH learns ARP response packets with corresponding ARP request only sent by itself. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address

mapping entry. In this way, network load is heavier but some network attacks based on ARP request packets can be prevented.

4.3.2 Preparing for configurations

Scenario

The mapping of IP address and MAC address is saved in the ARP address mapping table.

Generally, ARP address mapping table is dynamically maintained by the SWITCH. The SWITCH searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the SWITCH manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

4.3.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Dynamic ARP entry learning mode	Learn-reply-only

4.3.4 Configuring static ARP entries



Caution

- The IP address in static ARP entry must belong to the IP network segment of Layer 3 interface on the switch.
- The static ARP entry needs to be added and deleted manually.

Configure static ARP entries for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# arp <i>ip-address</i> <i>mac-address</i>	Configure static ARP entry.

4.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# arp learning enable	Enable dynamic ARP learning on the interface.
3	Switch(config)# arp mode { learn-all learn-reply-only }	Configure the aging time of dynamic ARP entries.
4	Switch(config)# arp aging-time <i>time</i>	Enter Layer 3 interface configuration mode.
5	Switch(config)# arp max-learning-num <i>number</i>	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.
6	Switch(config)# gratuitous-arp-learning enable	(Optional) enable gratuitous ARP learning on the interface.

4.3.6 Configuring local proxy ARP

Configure local proxy ARP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type primary-interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# arp local-proxy enable	Configure local proxy ARP on the interface.

4.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show arp [<i>ip-address</i> interface <i>interface-type interface-number</i> static]	Show information about entries in the ARP address table.
2	Switch# show arp local-proxy [<i>interface-type interface-number</i>]	Show the status of local proxy ARP and ARP buffer.

4.3.8 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)#clear arp	Clear all entries in the ARP address table.

4.4 NDP

4.4.1 Introduction

Neighbor Discovery Protocol (NDP) is a neighbor discovery mechanism used on IPv6 devices in the same link. It is used to discover neighbors, obtain MAC addresses of neighbors, and maintain neighbor information.

NDP obtains data link layer addresses of neighbor devices in the same link, namely, MAC address, through the Neighbor Solicitation (NS) message and Neighbor Advertisement (NA) message.

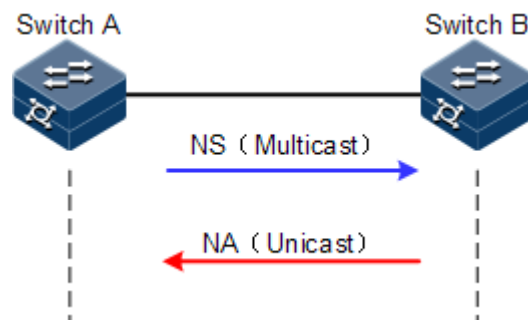


Figure 4-1 Principle of NDP address resolution

As shown in Figure 4-1, take Switch A for example. Switch A needs to obtain the data link layer address of Switch B, and the detailed procedure is as below:

- Step 2 Switch A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.
- Step 3 After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.
- Step 4 After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

4.4.2 Preparing for configurations

Scenario

IPv6 NDP not only implements IPv4 ARP, ICMP redirection, and ICMP device discovery, but also supports detecting whether the neighbor is reachable.

Prerequisite

- Connect related interfaces and configure physical parameters of them to make the physical layer Up.
- Configure the IPv6 address of the Layer 3 interface.

4.4.3 Default configurations of NDP

Default configurations of NDP are as below.

Function	Default value
Times of sending NS messages for detecting duplicated addresses	1
Maximum number of NDPs allowed to learn	512

4.4.4 Configuring static neighbor entries

To resolve the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Configure static neighbor entries for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ipv6 neighbor <i>ipv6-address mac-address</i>	configure static neighbor entries

4.4.5 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.

Step	Command	Description
3	Switch(config-vlan1)# ipv6 nd dad attempts <i>value</i>	Configure times of sending NS messages for detecting duplicated addresses.



Note

When the SWITCH obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

4.4.6 Configuring maximum number of NDPs allowed to learn on Layer 3 interface

Configure the maximum number of NDPs allowed to learn on the Layer 3 interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Switch(config-vlan1)# ipv6 neighbors max-learning-number <i>number</i>	Configure the maximum number of NDPs allowed to learn on the Layer 3 interface.

4.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ipv6 neighbors	Show all NDP neighbor information.
2	Switch# show ipv6 neighbors <i>ipv6-address</i>	Show neighbor information about a specified IPv6 address.
3	Switch# show ipv6 neighbors ip <i>if-number</i>	Show neighbor information about a specified layer 3 interface.
4	Switch# show ipv6 neighbors static	Show information about IPv6 static neighbor.
5	Switch# show ipv6 interface prefix [ip <i>if-number</i>]	Show prefix information about the IPv6 address.
6	Switch# show ipv6 interface nd [ip <i>if-number</i>]	Show ND information configured on the interface.

4.4.8 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)#clear ipv6 neighbors	Clear all IPv6 neighbor information.

4.5 Static route

4.5.1 Introduction

A route is required for communication among different devices in one VLAN, or different VLANs. The route is to transmit packets through network to destination, which adopts routing table for forwarding packets.

The SWITCH supports default route and static route only but dynamic route.

Default route

The default route is a special route that can be used only when there is no matched item in the routing table. The default route appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show default route configuration by using the **show ip route** command. If the SWITCH has not been configured with default route and the destination IP of the packet is not in the routing table, the SWITCH will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static route

The static route is the route configured manually, thus bring low requirements on the system. It is available to simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

4.5.2 Preparing for configurations

Scenario

Configure the static route for simple network topology manually to build an intercommunication network.

Prerequisite

Configure the IP address for the VLAN interface correctly.

4.5.3 Configuring static route

Configure static route for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip route <i>ip-address</i> { <i>masklength</i> <i>ip-mask</i> } <i>next-hop-ip-address</i> [distance <i>distance-value</i>] [description <i>word</i>] [tag <i>route-tag-value</i>]	Configure the static route.
3	Switch(config)# ip route static distance <i>value</i>	(Optional) configure the default IPv4 management distance.

4.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Switch# show ip route [detail]	Show information about IPv4 routes.

4.6 Configuring OSPF

4.6.1 Configuring OSPF basic functions

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# network <i>ip-address wild-card-mask</i> area <i>area-id</i>	Configure network segments included in the OSPF area.



Note

- If you manually configure the *router-id* parameter through the optional parameters in the **router ospf** *process-id* [**router-id** *router-id*] command, the OSPF process will select the *router-id* parameter first. Otherwise, the parameter is selected automatically.
- If the OSPF process is configured or selects the *router-id* parameter, after being modified, the *router-id* parameter takes effect after the OSPF process is rebooted.

4.6.2 Configuring OSPF route properties

Configuring OSPF cost of interface

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf cost <i>cost</i>	Configure the OSPF cost of the physical interface.

Configuring reference bandwidth

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# reference-bandwidth <i>bandwidth</i>	Configure the reference bandwidth reference of the link.



Note

- After the routing cost is manually configured through the **ip ospf cost** command, the manually-configured routing cost takes effect.
- If the routing cost is not configured manually but the link bandwidth reference value is configured, the routing cost is automatically configured based on the link bandwidth reference value. The formula is: $\text{cost} = \text{link bandwidth reference value (bit/s)} / \text{link bandwidth}$. If the cost value is greater than 65535, it is set to 65535. If no link bandwidth reference value is configured, it is set to 100 Mbit/s by default.

Configuring OSPF administration distance

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# distance <i>administrative-distance</i>	Configure the OSPF administration distance. By default, it is set to 110.

Step	Command	Description
4	Switch(config-router-ospf)# distance ospf { intra-area inter-area external } <i>distance</i>	Configure the administration distance of OSPF specified route. By default, it is set to 0. However, it takes 110 as the standard.

Configuring compatibility with RFC 1583

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Start an OSPF process, and enter OSPF configuration mode.
3	Switch(config-router-ospf)# compatible rfc1583	Configure compatibility with RFC 1583. By default, OSPF is compatible with RFC 1583.

4.6.3 Configuring OSPF network

Configuring type of OSPF network

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf network { broadcast non-broadcast ptmp ptp }	Configure the network type of the physical interface. By default, it is broadcast.

Configuring DR election priority

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf priority <i>priority</i>	Configure the DR election priority on the interface. By default, it is set to 1.

Configuring OSPF NBMA network neighbor

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf network non-broadcast Switch(config-gigaethernet1/1/1)# exit	Configure the network type of the interface to NBMA, and exit interface configuration mode.
4	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Switch(config-router-ospf)# neighbor <i>ip-address</i> [priority <i>priority</i>]	Configure the NBMA neighbor and its priority. By default, no NBMA neighbor is configured and the priority is set to 0 when you configure the NBMA neighbor.



Caution

Priorities configured by the **neighbour** and **ip ospf priority** *priority* commands are different:

- The priority configured by the **neighbor** command indicates that whether the neighbor has the right to vote. If you set the priority to 0 when configuring the neighbor, the local router believes that the neighbor has no right to vote and will not send Hello packets to the neighbor. This method helps reduce the number of Hello packets transmitted through the network during DR and BDR election processes. However, if the local router is a DR or BDR, it will send the Hello packet to the neighbor, whose priority is set to 0, to establish the neighboring relationship.
- The priority configured by the **ip ospf priority** *priority* command is used for actual DR election.

4.6.4 Optimizing OSPF network

Configuring OSPF packet timer

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.

Step	Command	Description
3	Switch(config-gigabitEthernet1/1/1)# ip ospf dead-interval <i>seconds</i>	Configure the OSPF neighbor dead interval. By default, it is 4 times of Hello packet delivery interval. If no Hello packet delivery interval is configured, it is set to 40s for P2P and Broadcast interfaces and 120s for P2MP and NBMA interfaces by default.
4	Switch(config-gigabitEthernet1/1/1)# ip ospf hello-interval <i>seconds</i>	Configure the OSPF Hello packet delivery interval. By default, it is set to 10s for P2P and Broadcast interfaces and 30s for P2MP and NBMA interfaces
5	Switch(config-gigabitEthernet1/1/1)# ip ospf poll-interval <i>seconds</i>	Configure the OSPF Poll timer interval. By default, it is set to 120s.
6	Switch(config-gigabitEthernet1/1/1)# ip ospf retransmit-interval <i>seconds</i>	Configure the LSA retransmission interval on the IP interface. By default, it is set to 5s.
7	Switch(config-gigabitEthernet1/1/1)# ip ospf transmit-delay <i>seconds</i>	Configure the LSA retransmission delay on the IP interface. By default, it is set to 1s.

Caution

- When the dead-interval is not manually configured, after hello-interval is configured, dead-interval and poll-interval is changed to 4 times of hello-interval.
- When the dead-interval is manually configured, after hello-interval is configured, no effect is brought to the dead-interval and poll-interval. No matter whether you configure the poll interval or not, the poll-interval changes with the dead-interval. Therefore, we recommend configuring these 3 values in the following order: hello-interval, dead-interval, and poll-interval.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, it needs to re-calculate the shortest path. If the network changes frequently and it needs to calculate the shortest path immediately, it will occupy a great amount of system resources and affect efficiency of the router. By adjusting the SPF calculation interval, you can prevent some effects brought by frequent network changes.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	Switch(config-router-ospf)# timers spf <i>delay-time hold-time</i>	Configure the calculation delay and interval of the OSPF route. By default, the calculation delay is set to 2s and calculation interval is set to 3s.

Configuring OSPF passive interface

To make some OSPF routing information not obtained by some router in the network, you can set the interface to an OSPF passive interface to disable the interface to send OSPF packets.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf passive-interface enable	Enable passive interface on the OSPF interface. By default, it is disabled.

Configuring MTU ignorance

By default, the value of MTU domain in the DD packet is the MTU value of the interface, which sends the DD packet. Default MTU values may vary on devices. In addition, if the MTU value of the DD packet is greater than the one of the interface, the DD packet will be discarded. To ensure receiving the DD packet properly, enable MTU ignorance to set the MTU value to 0. Therefore, all devices can receive the DD packet.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf mtu- ignore enable	Enable MTU ignorance on the IP interface. By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF Hello packet.

4.6.5 Configuring OSPF authentication mode

Configuring OSPF area authentication mode

All routers in an area need to be configured with the identical area authentication mode (non-authentication, simple authentication, or MD5 authentication). The OSPF area has no authentication password but adopts the interface authentication password. If no interface authentication password is configured, the empty password will be used for authentication.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# area <i>area-id</i> authentication { md5 simple }	Configure the area authentication mode. By default, it is set to non-authentication.

Configuring OSPF interface authentication mode

Packet authentication prioritizes selecting the interface authentication mode. If the interface authentication mode is set to non-authentication mode, the area authentication mode will be selected. OSPF interfaces cannot establish the neighbor relationship unless the authentication mode and authentication password are identical.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip ospf authentication { md5 simple }	Configure the interface authentication mode. By default, it is set to non-authentication. It means adopting the area authentication mode.
4	Switch(config-gigaethernet1/1/1)# ip ospf authentication-key { simple [0 7] <i>password</i> md5 { [<i>key-id</i> [0 7] <i>password</i>] keychain <i>keychain-name</i> } }	Configure the authentication password of the interface.

4.6.6 Configuring Stub area

For the non-backbone area at the edge of Autonomous System (AS), you can configure the **stub** command on all routers in the area to configure the area to a Stub area. In this case, Type5 LSA, which is used to describe external routes of the AS cannot be flooded in the Stub area. This facilitates reducing the routing table size.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	Switch(config-router-ospf)# area <i>area-id</i> stub [no-summary]	Configure the area to a Stub area. The no-summary parameter is used to disable the ABR to send Summary LSA to the Stub area. It means that it is a Totally Stub area and the ABR is available for the Stub only. By default, no area is set to the Stub area.
4	Switch(config-router-ospf)# area <i>area-id</i> default-cost <i>cost</i>	Configure the default route cost of the Stub area. This command is available for the ABR in the Stub area only. By default, it is set to 1.

Caution

- All routers in the Stub area must be configured with the Stub property through the **area area-id stub** command.
- To set an area to a Totally Stub area, all routers in the area must be configured by the **area area-id stub** command. In addition, all ABRs in the area must be configured by the **area area-id stub no-summary** command.
- The backbone area cannot be set to the Stub area.
- ASBR should not be in the Stub area. It means that routers besides the AS cannot be transmitted in the Stub area.

4.6.7 Controlling OSPF routing information

Configuring OSPF redistributed routes

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# redistribute { static connected rip isis ospf bgp } [metric <i>metric</i>] [metric-type { 1 2)] [tag <i>tag-value</i>] [route-map <i>map-name</i>] Switch(config-router-ospf)# redistribute ospf [<i>process-id</i>] [vrf <i>vrf-</i> <i>name</i>] [metric <i>metric</i>] [metric-type { 1 2] [tag <i>tag-value</i>] [route- map <i>map-name</i>]	Configure OSPF route redistribution polity. By default, no external route is redistributed. When an external route is redistributed: <ul style="list-style-type: none"> • When the directly-connected and static route is redistributed, the metric is set to 1 by default. When other routes are redistributed, take the original metric of the external route as the metric of the LSA. • If no Metric-type is specified, the Metric-type is set to Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	Switch(config-router-ospf)# redistribute limit <i>limit-number</i>	Configure the threshold of redistributed OSPF external routes. By default, no threshold is set.

Configuring inter-area route aggregation

If there are sequent network segments in the area, you can configure route aggregation on the ABR to aggregate these network segments to a network segment. When sending routing information, the ABR generates Type3 LSA by taking the network segment as the unit.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# area <i>area-id</i> range <i>ip-address ip-mask</i> [not-advertise]	Configure the inter-area route aggregation. By default, no inter-area route aggregation is configured. When you configure the aggregated route, the cost is set to the maximum Metric of the LSA by default. In addition, the aggregated route is redistributed.

Aggregating redistributed external routes

After the external route is redistributed, configure route aggregation on the ASBR. The SWITCH just puts the aggregated route on the ASE LSA. This helps reduces the number of LSAs in the LSDB.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# summary-address <i>ip-address ip-mask</i> [not-advertise] [metric <i>metric</i>]	Aggregate external routes. By default, external routes are not aggregated. When external aggregates are aggregated, the Metric is set to the maximum Metric of the LSA by default.

Redistributing default route

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# default-information originate [always] [metric <i>metric</i>] [type { 1 2 }]	Redistribute the default route. By default, no default route is generated. When the default LSA is generated, if the always key word is specified, the default Metric is set to 1. If the always key word is not specified, the Metric is set to 10.

4.6.8 Configuring OSPF routing policy

Configuring OSPF receiving policy

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip prefix-list <i>list-name</i> [index number] { permit deny } <i>ip-address mask-length</i> [greater-equal <i>ge-length</i>] [less-equal <i>le-length</i>]	Configure the IP prefix-list. You can use the no ip prefix-list <i>list-name</i> [index number] command to delete the configuration.
3	Switch(config)# rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address source-ip-mask</i> any }	Configure the IP ACL rule. At present, the SWITCH just supports matching the address prefix information about the route by specifying the destination IP address and subnet mask.
4	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Switch(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } in	Configure the OSPF filtering policy for receiving the OSPF inter-area routes, intra-area routes, and AS external routes.



Note

- Before configuring OSPF receiving policy, ensure that the IP ACL used by the OSPF receiving policy has been created.
- When the SWITCH performs filtering based on IP ACL, if the ACL mode is set to permit, all routes, which match with the ACL, can pass. Others are filtered.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- If the configured IP prefix-list does not exist, do not filter received routes.

Configuring OSPF distributing policy

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip prefix-list <i>list-name</i> [index number] { permit deny } <i>ip-address mask-length</i> [greater-equal <i>ge-length</i>] [less-equal <i>le-length</i>]	Configure the IP prefix-list. You can use the no ip prefix-list <i>list-name</i> [index number] command to delete the configuration.
3	Switch(config)# rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address source-ip-mask</i> any }	Configure the IP ACL rule. At present, the SWITCH just supports matching the address prefix information about the route by specifying the destination IP address and subnet mask.

Step	Command	Description
4	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Switch(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out	Configure the filtering policy that the OSPF releases 5 types of LSAs to the AS.
6	Switch(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out [static connected rip isis bgp]	Configure the OSPF distributing policy.
	Switch(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out ospf <i>process-id</i> [vrf <i>vrf-</i> <i>name</i>]	



Note

- Before configuring OSPF global distributing policy, ensure that the IP ACL used by the OSPF global distributing policy has been created.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- After global distributing policy is configured, routes cannot be redistributed to the local LSDB unless it passes the global distributing policy. After protocol distributing policy is configured, the route can be redistributed through the protocol distributing policy.
- After protocol distributing policy is configured, the redistributed protocol route can be redistributed to the local LSDB through the protocol distributing policy. If global distributing policy is also configured, the route must be redistributed through the global distributing policy.

Configuring Type3 LSA filtering policy

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip prefix-list <i>list-name</i> [index <i>number</i>] { permit deny } <i>ip-</i> <i>address mask-length</i> [greater-equal <i>ge-</i> <i>length</i>] [less-equal <i>le-length</i>]	Configure the IP prefix-list. You can use the no ip prefix-list <i>list-name</i> [index <i>number</i>] command to delete the configuration.
3	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
4	Switch(config-router-ospf)# area <i>area-id</i> filter prefix-list <i>list-name</i> { in out }	Configure Type3 LSA filtering policy in the area.

**Note**

If the configured filtering policy does not exist, it believes that the command fails to configure the filtering policy and no filtering operation is performed on received routes.

4.6.9 Configuring BFD for OSPF

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enter OSPF configuration mode.
3	Switch((config-router-ospf))# bfd all-interfaces	Enable global BFD. By default, it is disabled.
4	Switch(config-router-ospf)# exit	Enter global configuration mode.
5	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
6	Switch(config-gigaethernet1/1/1)# ip ospf bfd	Enable BFD on the interface. By default, it is disabled.

**Note**

- If global BFD is enabled through the **bfd all-interfaces** command, no matter what BFD configurations are set on the interface, BFD is enabled.
- If global BFD is disabled, BFD configurations on the interface take effect.

4.6.10 Configuring OSPF for MPLS-TE

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Switch(config-router-ospf)# capability opaque	Enable OSPF opaque LSA. By default, it is disabled.
4	Switch(config-router-ospf)# mpls traffic-eng area <i>area-id</i>	Enable TE in the OSPF area. By default, it is disabled.
5	Switch(config-router-ospf)# mpls traffic-eng router-id <i>router-id</i>	Configure the Router ID of the MPLS-TE router.

4.6.11 Checking configurations

No.	Command	Description
1	Switch# show ip ospf [<i>process-id</i>]	Show basic information about OSPF.
2	Switch# show ip ospf [<i>process-id</i>] interface [<i>interface-type interface-number</i>]	Show information about OSPF interfaces.
3	Switch# show ip ospf [<i>process-id</i>] neighbor [<i>interface-type interface-number</i>] [<i>neighbor-id</i>]	Show information about OSPF neighbors.
4	Switch# show ip ospf [<i>process-id</i>] route	Show routing information about OSPF.
5	Switch# show ip ospf [<i>process-id</i>] database [max-age self-originate]	Show information and statistics of OSPF link status database.
	Switch# show ip ospf [<i>process-id</i>] database [router network summary asbr-summary external] [<i>linkstate-id</i>] [adv-router ip- address self-originate]	
	Switch# show ip ospf [<i>process-id</i>] database statistics	
6	Switch# show ip ospf [<i>process-id</i>] border- routers	Show information about routers at edges of the area and AS.
7	Switch# show ip ospf [<i>process-id</i>] neighbor statistics	Show OSPF statistics or OSPF neighbor statistics.
8	Switch# show ip ospf [<i>process-id</i>] summay- address	Show information about OSPF ASBR external route aggregation.
9	Switch# show cspf tedb [detail]	Show information about the TEDB database.

4.6.12 Maintenance

Command	Description
Rasiecom# clear ip ospf [<i>process-id</i>] process [graceful]	Restart the OSPF process.

5 DHCP

This chapter describes basic principle and configuration procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Relay
- DHCP Server
- DHCP Client
- DHCP Snooping
- DHCP Options

5.1 DHCP Relay

5.1.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same network segment, instead of different network segments. As a result, a DHCP server is configured for all network segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

Figure 5-1 shows the principle of DHCP Relay.

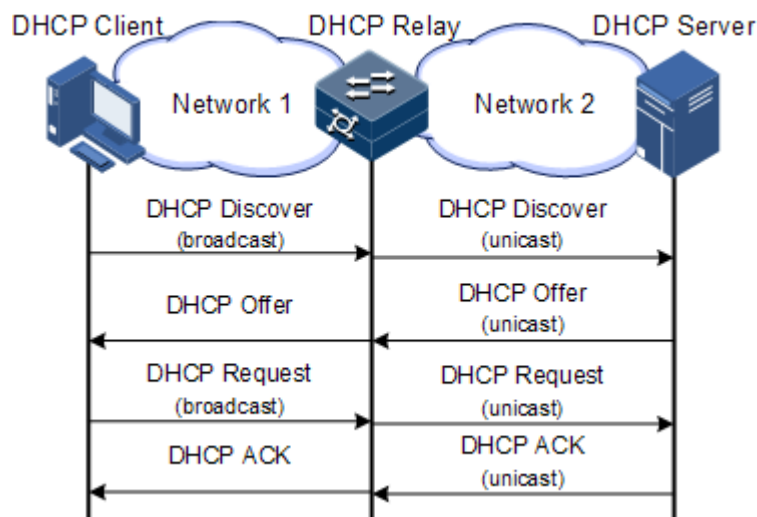


Figure 5-1 Principle of DHCP Relay

- Step 1 The DHCP client sends a request packet to the DHCP server.
- Step 2 After receiving the packet, the DHCP relay device process the packet in a certain way, and then sends it to the DHCP server on the specified network segment.
- Step 3 The DHCP server sends acknowledgement packet to the DHCP client through the DHCP relay device according to the information contained in the request packet. In this way, the configuration of the DHCP client is dynamically configured.

5.1.2 Preparing for configurations

Scenario

When the SWITCH works as a DHCP v4 relay, the DHCP v 4 client can communicate with the DHCP server in a different segment through the relay to obtain the IP address. In this case, DHCP clients in different network segment can share the same DHCP server and thus obtain the IP address to save coast and facilitate centralized management.

Prerequisite

DHCP v4 Client or Server is disabled.

5.1.3 Configuring DHCP v4 Relay

Configure global DHCP v4 Relay for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip dhcp relay	Enable DHCP Relay on the interface. By default, it is disabled.

5.1.4 Configuring destination IP address for DHCP v4 Relay

Configure the destination IP address for DHCP v4 Relay for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter Layer 3 interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# ip dhcp relay target-ip <i>ip-address</i>	Configure the destination IP address for DHCP v4 Relay.

5.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip dhcp relay	Show configurations of DHCP Relay.

5.2 DHCP Server

5.2.1 Introduction

DHCP works in client/server mode, so a specified server assigns network addresses and transmits configured parameters to hosts on the network. The specified server is called the DHCP server.

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than the number of IP addresses, which make it unable to assign a fixed IP address for each host, and restrict the number of users connected to network simultaneously.
- A large number of users must obtain their own IP address dynamically through DHCP service.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

The SWITCH can work as the DHCP server to assign dynamic IP addresses for clients, as shown in Figure 5-2.

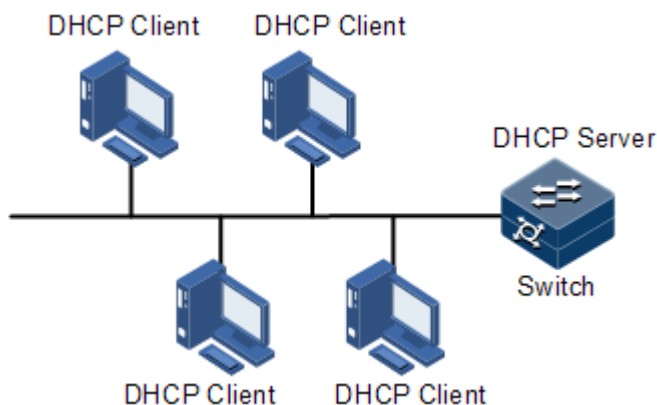


Figure 5-2 DHCP Server networking

After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the leased period. You can specify the duration of the leased period.

5.2.2 Preparing for configurations

Scenario

When the SWITCH works as the DHCP v4 server, DHCP v4 clients can apply IP addresses from it.

Prerequisite

- DHCP v4 Client is disabled.
- The working mode of the DHCP server is common.

5.2.3 Configuring IPv4 address pool

Configure the IPv4 address pool for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip dhcp server pool <i>pool-name</i>	Create an IPv4 address pool, and enter address pool mode.
3	Switch(config-pool)# address <i>start-ip-address end-ip-address mask</i> { <i>mask</i> <i>mask-length</i> }	Configure the range of IPv4 addresses.
4	Switch(config-pool)# lease expired { <i>minute</i> <i>infinite</i> }	Configure the leased period of the IPv4 address pool.
5	Switch(config-pool)# dns-server <i>ip-address</i> [secondary]	(Optional) configure the DNS server of the IPv4 address pool.
6	Switch(config-pool)# gateway <i>ip-address</i>	(Optional) configure the default gateway of the IPv4 address pool.

Step	Command	Description
7	Switch(config-pool)# option 60 <i>vendor-string</i>	(Optional) configure information carried by Option 60.
8	Switch(config-pool)# tftp-server <i>ip-address</i>	(Optional) configure the TFTP server of the IPv4 address pool.
9	Switch(config-pool)# trap server-ip <i>ip-address</i>	(Optional) configure the Trap server of the IPv4 address pool.

5.2.4 Configuring DHCP Server on interface

Configure DHCP Server on the interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip dhcp server	Enable DHCP v4 Server on the interface.

5.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch(config)# show ip dhcp server	Show configurations of DHCP Server.
2	Switch(config)# show ip dhcp server lease	Show the assigned IPv4 address and client information.
3	Switch(config)# show ip dhcp server statistics	Show statistics of packets of the DHCP server.
4	Switch(config)# show ip dhcp static-bind	Show information about DHCP static binding.

5.3 DHCP Client

5.3.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assign IP address configurations dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol,

and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of notebooks and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies configuration to the server (including IP address, Subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address, etc.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or Notebook), as shown in Figure 5-2.

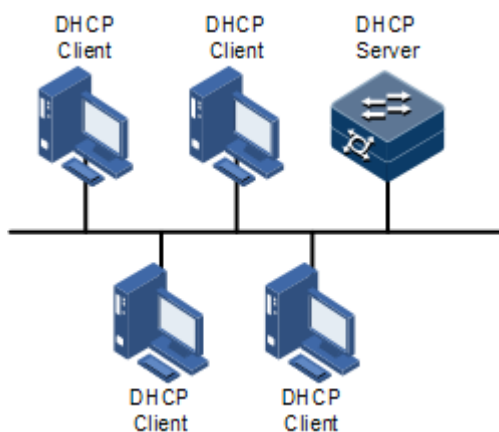


Figure 5-3 DHCP typical networking

DHCP technology ensures rational allocation, avoid waste and improve the utilization rate of IP addresses in the entire network.

Figure 5-4 shows structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

0	7	15	23	31
OP	Hardware type		Hardware length	Hops
Transaction ID				
Seconds			Flags	
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Figure 5-4 Structure of DHCP packet

Table 5-1 describes fields of DHCP packets.

Table 5-1 Fields of DHCP packet

Field	Length	Description
OP	1	Packet type <ul style="list-style-type: none"> • 1: a request packet • 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client.
Hardware length	1	Hardware address size of a DHCP client.
Hops	1	DHCP hops number passed from DHCP packet. This field increases 1 every time DHCP request packet passes a DHCP hop.
Transaction ID	4	The client chooses a number at random when starting a request, used to mark process of address request.
Seconds	2	Passing time for the DHCP client after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is the broadcast reply flag, used to mark whether the DHCP server replies packets in unicast or broadcast mode. <ul style="list-style-type: none"> • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	DHCP client IP address, only filled when the client is in bound, updated or re-bind status, used to reply ARP request.
Your (client) IP address	4	IP address of the client distributed by DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP hop after the DHCP client sends request packets.
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Name of the startup configuration file of the DHCP client and path assigned by the DHCP server
Options	Modifiable	A modifiable option field, including packet type, available leased period, Domain Name System (DNS) server IP address, Windows Internet Name Server (WINS) IP address, etc. information.

The SWITCH can be used as DHCP client to get IP address from the DHCP server for future management, as shown in Figure 5-5.

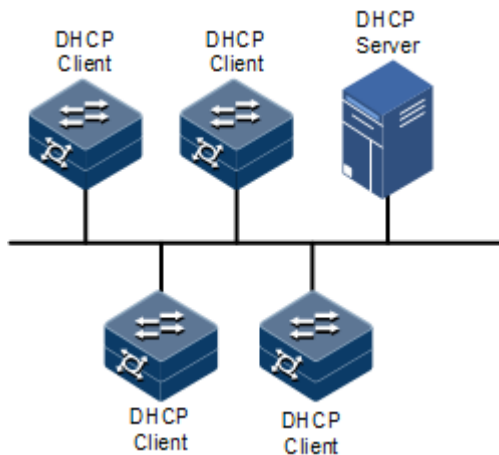


Figure 5-5 DHCP Client networking

5.3.2 Preparing for configurations

Scenario

As a DHCP client, the SWITCH obtains its IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to relet IP address for continuous use. The DHCP client can release the IP address if it does not want to use the IP address before expiration.

We recommend setting the number of DHCP relay devices smaller than 4 if the DHCP client needs to obtain IP address from the DHCP server through multiple DHCP relay devices.

Prerequisite

- Create a VLAN and add Layer 3 interface to it.
- DHCP Snooping is disabled.

5.3.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	Switch
class-id	Switch-ROS
client-id	Switch-SYSMAC-IF0

5.3.4 Configuring DHCP Client

Only interface IP 0 on the SWITCH supports DHCP Client.

When applying for an IP address, the DHCP client needs to create a VLAN firstly, and add the interface with the IP address to the VLAN. Meanwhile configure DHCP server; otherwise the interface will fail to obtain IP address through DHCP.


For interface IP 0, the IP addresses obtained through DHCP and configured manually can overwrite each other.



Note

- If the SWITCH is enabled with DHCP Server or DHCP Relay, DHCP Client cannot be enabled. Vice versa.
- By default, the SWITCH is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the SWITCH obtains the IP address from the DHCP server through DHCP previously, it will restart the application process for IP address if you use the **ip address dhcp** command to modify the IP address of the DHCP server.

Configure DHCP Client for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface vlan 1	Enter VLAN interface configuration mode.
3	Switch(config-vlan1)# ip dhcp client { class-id class-id client-id client-id hostname hostname }	(Optional) configure DHCP client information, including the type identifier, client identifier, and host name.  Caution After the IP address is obtained through DHCP, client information cannot be modified.
4	Switch(config-vlan1)# ip address dhcp [server-ip ip-address]	Configure the DHCP client to obtain IP address through DHCP.
5	Switch(config-vlan)# ip dhcp client renew	(Optional) relet the IP address. If the interface of the DHCP client has obtained an IP address through DHCP, the IP address will automatically be renewed when the lease period expires.
6	Switch(config-ip)# no ip address dhcp	(Optional) release the IP address.

5.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip dhcp client	Show configurations of DHCP Client.

5.4 DHCP Snooping

5.4.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Make the DHCP client obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown in Figure 5-6, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits to set an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards the reply packets from the DHCP server.

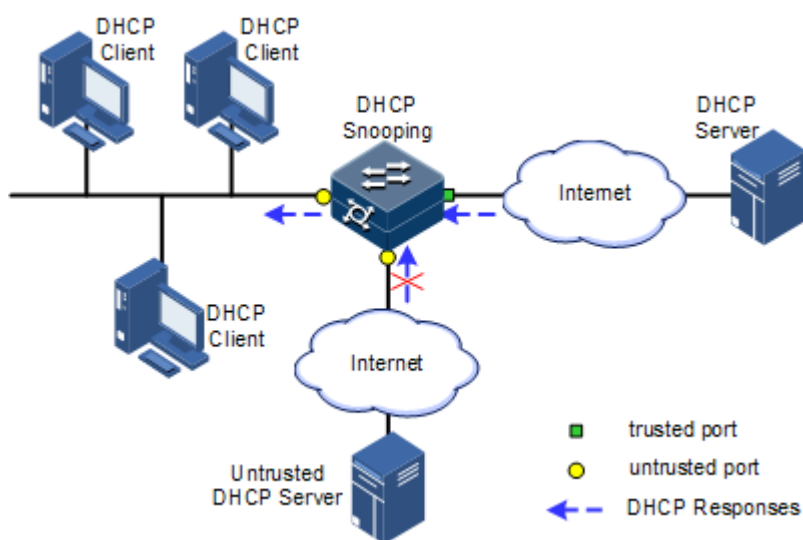


Figure 5-6 DHCP Snooping networking

- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface, etc. Then implement following by the record information:

- ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
- IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
- VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option field to locate DHCP clients and control client security and accounting.

If the SWITCH configures DHCP Snooping to support Option function:

- When the SWITCH receives a DHCP request packet, it processes packets according to Option field included or not and filling mode as well as processing policy configured by user, then forwards the processed packet to DHCP server.
- When the SWITCH receives a DHCP reply packet, it deletes the field and forward to DHCP client if the packet does not contain Option field; it then forwards packets directly if the packet does not contain Option field.

5.4.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, used to make DHCP client obtain its IP address from a legal DHCP server and record mapping between IP address and MAC address of a DHCP client.

The Option field of a DHCP packet records location of a DHCP client. The administrator can locate a DHCP client through the Option field and control client security and accounting. The device configured with DHCP Snooping and Option can perform related process according to Option field status in the packet.

Prerequisite

N/A

5.4.3 Default configurations of DHCP Snooping

Default configurations of DHCP Snooping are as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trust/untrust status	Untrust
DHCP Snooping in support of Option 82	Disable

5.4.4 Configuring DHCP Snooping

Generally, ensure that the SWITCH interface connected to DHCP server is in trust state, while the interface connected to user is in distrust state.

If enabling DHCP Snooping without configuring DHCP Snooping supporting Option function, the SWITCH will do nothing to Option fields in the packets. For packets without Option fields, the SWITCH still does not do insertion operation.

By default, DHCP Snooping of all interfaces is enabled, but only when global DHCP Snooping is enabled, interface DHCP Snooping can take effect.

Configure DHCP Snooping for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip dhcp snooping	Enable global DHCP Snooping.
3	Switch(config)# ip dhcp snooping interface-type interface-number	(Optional) enable interface DHCP Snooping.
4	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
5	Switch(config-gigaetherne t1/1/1)#ip dhcp snooping trust	Configure the trusted interface of DHCP Snooping.
6	Switch(config-gigaetherne t1/1/1)#ip dhcp snooping information option vlan-list vlan-list	(Optional) configure the lists of VLANs that support Option 82 through DHCP Relay.
7	Switch(config-gigaetherne t1/1/1)#exit Switch(config)# ip dhcp snooping option option-id	(Optional) configure DHCP Snooping to support user-defined Option fields.
8	Switch(config)# ip dhcp snooping option client-id	(Optional) configure DHCP Snooping to support Option 61 field.
9	Switch(config)# ip dhcp snooping information option	(Optional) configure DHCP Snooping to support Option 82 field.

5.4.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Switch# show ip dhcp snooping	Show configurations of DHCP Snooping.
2	Switch# show ip dhcp snooping binding	Show configurations of the DHCP Snooping binding table.

5.5 DHCP Options

5.5.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to realize address dynamical distribution to provide abundant network configurations for client. DHCP protocol has 255 kinds of options, the final option is 255. Table 5-2 lists frequently used DHCP options.

Table 5-2 Common DHCP options

Options	Description
3	Router option, to assign gateway for DHCP client
6	DNS server option, to assign DNS server address distributed by the DHCP client
18	IPv6-based DHCP client flag option, to assign interface information for DHCP client
51	IP address lease option
53	DHCP packet type, to mark type for DHCP packets
55	Request parameter list option. Client uses this optical to indicate network configuration parameters need to obtain from server. The content of this option is values corresponding to client requested parameters.
61	DHCP client flag option, to assign device information for DHCP clients.
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP clients.
67	Startup file name, to assign startup file name distributed by DHCP clients.
82	DHCP client flag option, user-defined, mainly used to mark position of DHCP client, including Circuit ID and remote ID.
150	TFTP server address, to assign TFTP server address distributed by DHCP clients.
184	DHCP reserved option, at present Option184 is used to carry information required by voice calling. Through Option184 it can distribute IP address for DHCP client with voice function and meanwhile provide voice calling related information.
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients arrive the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

Option 82 can include at most 255 sub-options. If defined field Option 82, at least one sub-option must be defined. The SWITCH supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains interface number, interface VLAN, and the additional information about DHCP client request packet.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP snooping device) of the SWITCH, or user-defined string of DHCP client request packets.

5.5.2 Preparing for configurations

Scenario

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients reach the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting.

Prerequisite

N/A

5.5.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	Switch-mac
circuit-id in interface configuration mode	N/A

5.5.4 Configuring DHCP Option field

Configure DHCP Option field for the SWITCH as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip dhcp information option attach-string <i>attach-string</i>	(Optional) configure additional information for Option 82 field.
	Switch(config)# interface <i>interface-type interface-number</i> Switch(config-gigaethernet1/1/1)# ip dhcp information option circuit-id <i>circuit-id</i> [prefix-mode]	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
	Switch(config)# ip dhcp information option { attach-string circuit-id format circuit-id hex } <i>string</i>	(Optional) configure the attached string in Option 82 of DHCP packets.

Step	Command	Description
	Switch(config)# ip dhcp information option circuit-id mac-format <i>string</i>	(Optional) configure the format of the MAC address in the variable of Circuit ID in Option 82 of DHCP packets.
	Switch(config-gigaethernet1/1/1)# exit Switch(config)# ip dhcp information option remote-id { client-mac client-mac-string hostname switch-mac switch-mac-string string <i>string</i> }	(Optional) configure remote ID sub-option information for Option 82 field.
3	Switch(config)# ipv4 dhcp option <i>option-id</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) create user-defined Option field information.
	Switch(config)# interface gigaethernet1/1/1 Switch(config-gigaethernet1/1/1)# ipv4 dhcp option <i>option-id</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) create user-defined Option field information on the interface.
4	Switch(config-gigaethernet1/1/1)# exit Switch(config)# ipv4 dhcp option client-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) configure Option 61 field information.
	Switch(config-gigaethernet1/1/1)# ipv4 dhcp option client-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	(Optional) configure Option61 field information on the interface.

5.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip dhcp information option	Show configurations of DHCP Option fields.

6 QoS

This chapter describes basic principle and configuration of QoS and provides related configuration examples, including the following sections:

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic classification and traffic policy
- Configuring rate limiting

6.1 Introduction

Users bring forward different service quality demands for network applications, then the network should distribute and schedule resources for different network applications according to user demands. Quality of Service (QoS) can ensure service in real time and integrity when network is overloaded or congested and guarantee that the whole network runs efficiently.

QoS is composed of a group of flow management technologies:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

6.1.1 Service model

QoS technical service models:

- Best-effort Service
- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without being allowed in advance and notifying the network. For Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP and E-mail, which is implemented by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements.

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket; otherwise, it discards the packets or remarks IP precedence, DSCP, EXP, etc. CAR can not only control the flows, but also mark and remark the packets.
- Queue technology: the queue technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

6.1.2 Priority trust

Priority trust refers that the SWITCH uses priority of packets for classification and performs QoS management.

The SWITCH supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- Type of Service (ToS) priority

6.1.3 Traffic classification

Traffic classification refers to recognizing packets of certain types according to configured rules, conducting different QoS policies for packets matching with different rules. It is the prerequisite of differentiated services.

The SWITCH supports traffic classification by IP priority, DSCP priority, and CoS priority over IP packets, as well as traffic classification by Access Control List (ACL) rule and VLAN ID. Figure 6-1 shows the principle of traffic classification.

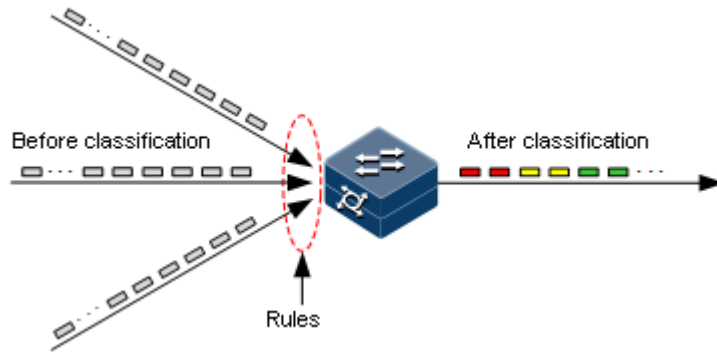


Figure 6-1 Traffic classification

IP priority and DSCP priority

Figure 6-2 shows the structure of the IP packet head. The head contains an 8-bit ToS field. Defined by RFC 1122, IP priority (IP Precedence) uses the highest 3 bits (0–3) with value range of 0–7; RFC2474 defines ToS field again, and applies the first 6 bits (0–5) to DSCP priority with value range 0–63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 6-3 shows the structure of two priority types.

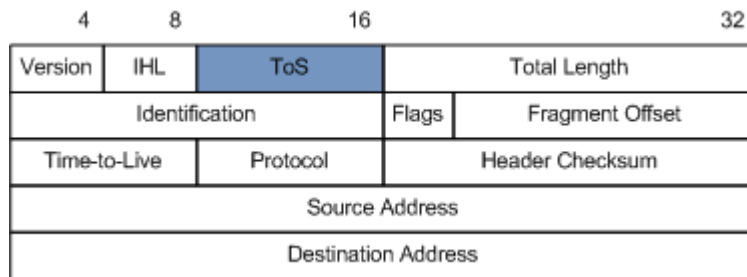


Figure 6-2 Structure of IP packet head

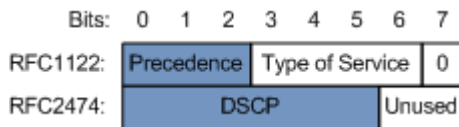


Figure 6-3 Structure of packets with IP priority and DSCP priority

CoS priority

The format of Ethernet packets is modified to make VLAN packets based on IEEE 802.1Q. IEEE 802.1Q adds 4-Byte 802.1Q tag between the source address field and protocol type field, as shown in Figure 6-4. The tag includes a field of 2-Byte TPID (Tag Protocol Identifier, value being 0x8100) and a field of 2-Byte Tag Control Information (TCI).

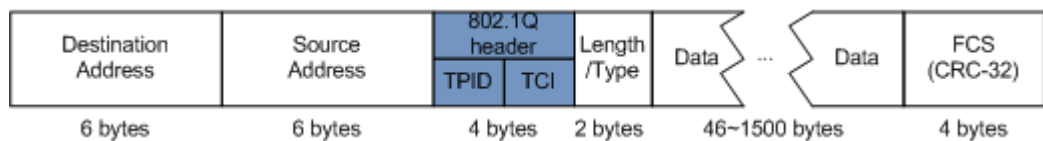


Figure 6-4 Structure of VLAN packets

The CoS priority is included in the first 3 bits of the TCI field, ranging from 0 to 7, as shown in Figure 6-5. It is used when QoS needs to be guaranteed on the Layer 2 network.

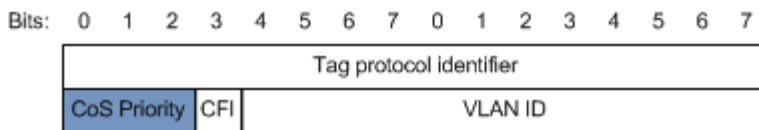


Figure 6-5 Structure of packets with CoS priority

6.1.4 Traffic policy

After classifying packets, the SWITCH needs to take different actions for different packets. The binding of traffic classification and an action forms a traffic policy.

Rate limiting

Rate limiting refers to controlling network traffic, monitoring the rate of traffic entering the network, and discarding overflow part, so it controls ingress traffic in a reasonable range, thus protecting network resources and carrier interests.

The SWITCH supports rate limiting based on traffic policy in the ingress direction on the interface.

The SWITCH supports using token bucket for rate limiting, including single-token bucket and dual-token bucket.

Re-direction

Re-direction refers to re-directing packets to a specified interface, instead of forwarding packets according to the mapping between the original destination address and interface, thus implementing policy routing.

The SWITCH supports re-directing packets to the specified interface for forwarding in the ingress direction of an interface.

Re-mark

Re-mark refers to setting some priority fields in packet again and then classifying packets by user-defined standard. Besides, downstream nodes on the network can provide differentiated QoS service according to re-mark information.

The SWITCH supports remarking packets by the following priority fields:

- IP priority of IP packets
- DSCP priority
- CoS priority

Traffic statistics

Traffic statistics is used to take statistics of data packets of a specified service flow, namely, the number of packets and Bytes matching traffic classification that pass the network or are discarded.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

6.1.5 Priority mapping

Priority mapping refers when the SWITCH receives packets, it sends them in queues with different local priorities in accordance with mapping from external priority to local priority, thus scheduling packets in the egress direction of packets.

The SWITCH supports priority mapping based on DSCP priority or CoS priority.

Table 6-1 lists the default mapping of local priority, DSCP, and CoS. The Traffic-Class field of IPv6 packets is corresponding to the DSCP domain of IPv4 packets. The mapping from DSCP to local priority is also applicable to IPv6 packets, and you can use the first 6 bits of the Traffic-Class field.

Table 6-1 Default mapping of local priority, DSCP, and CoS

Local priority	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal function assigned by the SWITCH, namely, the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the SWITCH supports 8 queues. Local priority and interface queue is in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 6-2.

Table 6-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

6.1.6 Congestion management

Queue scheduling is necessary when there is intermittent congestion on the network or delay sensitive services require higher QoS service than non-sensitive services.

Queue scheduling adopts different schedule algorithms to transmit packets in queues. The SWITCH supports Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR and SP+DRR algorithm. Each algorithm solves specific network traffic problems, and has different influences on distribution, delay, and jitter of bandwidth resource.

- SP: schedule packets strictly according to queue priority order. Queues with low priority cannot be scheduled until queues with higher priority finishes schedule, as shown in Figure 6-6.

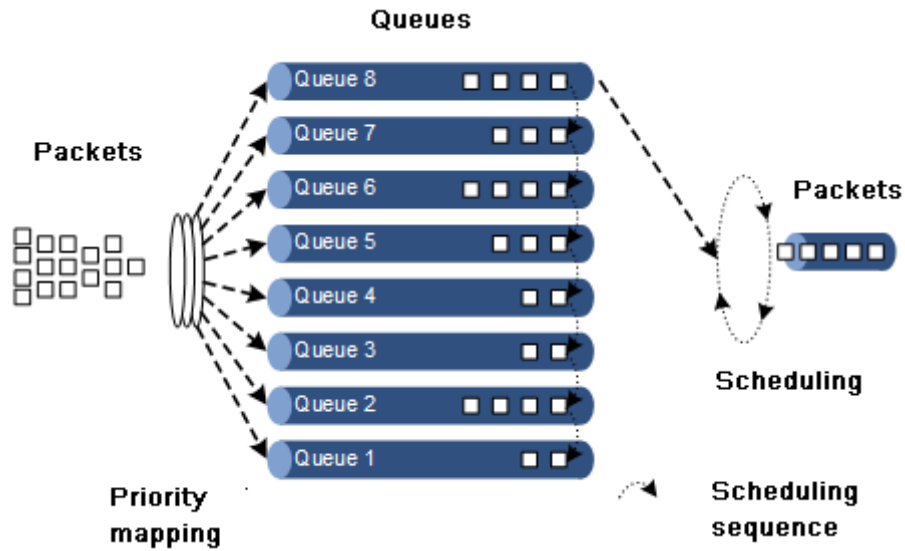


Figure 6-6 SP scheduling

- WRR: on the basis of round scheduling each queue according to queue priority, schedule packets in various queues according to weight of each queue, as shown in Figure 6-7.

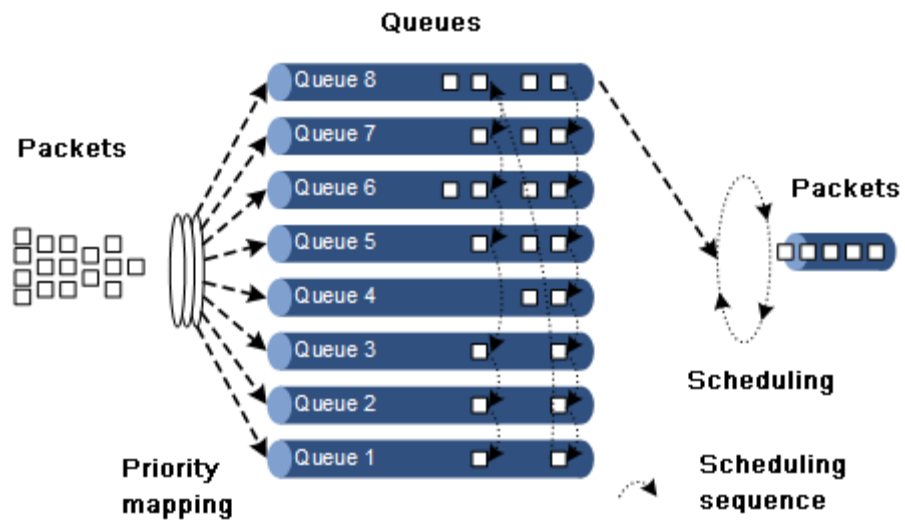


Figure 6-7 WRR scheduling

- DRR: on the basis of circular schedule each queue according to queue priority, schedule packets in each queue according to weight of each queue. Besides, the SWITCH lends the redundant bandwidth of a queue in one schedule to other queues in the later schedule, and the queue borrowing the bandwidth will return it back, as shown in Figure 6-8.

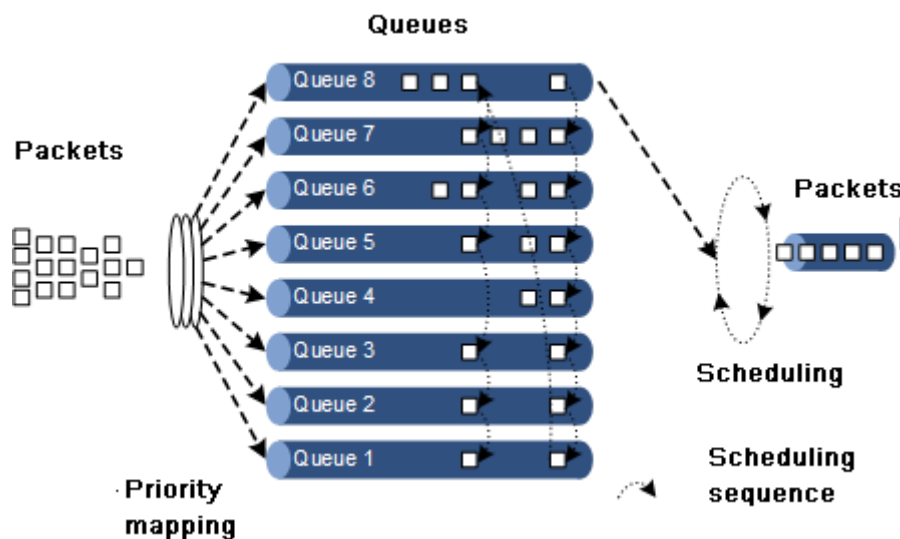


Figure 6-8 DRR scheduling

- SP+WRR: schedule queues on interfaces into two groups, you can assign some queues to conduct SP schedule and other queues to conduct WRR schedule.
- SP+DRR: schedule queues on interfaces into two groups, you can assign some queues to conduct SP schedule and other queues to perform DRR schedule.

6.1.7 Congestion avoidance

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or when network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating CoS. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

RED

The Random Early Detection (RED) technology discards packets randomly and makes multiple TCP connection not reduce transport speed simultaneously to avoid TCP global synchronization.

The RED algorithm set a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

WRED

The Weighted Random Early Detection (WRED) technology also discards packets randomly to avoid TCP global synchronization. However, the random drop parameter generated by WRED technology is based on the priority. WRED differentiates drop policies through the color of packets. This helps ensure that high-priority packets have a smaller packet drop probability.

The SWITCH supports WRED congestion avoidance but only supports the queue scheduling in the egress interface.

6.1.8 Rate limiting

The SWITCH supports rate limiting based on traffic policy, based on interface, based on VLAN, and based on interface+VLAN. Similar to rate limiting based on traffic policy, the SWITCH discards the exceeding traffic.

6.2 Configuring priority

6.2.1 Preparing for configurations

Scenario

You can choose to trust the priority carried by packets from an upstream device, or process packets with untrusted priority through traffic classification and traffic policy. After being configured to priority trust mode, the SWITCH processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the SWITCH will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping relationship between IP priority/DSCP priority and local priority; while VLAN packets need to be configured with mapping relationship between CoS priority and local priority.

Prerequisite

N/A

6.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable
Interface trust priority type	Trust CoS priority
Mapping from CoS to local priority	See Table 6-3.
Mapping from DSCP to local priority	See Table 6-4.

Function	Default value
Mapping from ToS to local priority and color	See Table 6-5.
Interface priority	0

Table 6-3 Default mapping from CoS to local priority

CoS	0	1	2	3	4	5	6	7
Local	0	1	2	3	4	5	6	7

Table 6-4 Default mapping from DSCP to local priority

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Local	0	1	2	3	4	5	6	7

Table 6-5 Default mapping from ToS to local priority and color

DSCP	0	1	2	3	4	5	6	7
Local	0	1	2	3	4	5	6	7

6.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaetherne1/1/1)# mls qos trust { cos dscp port-priority }	Configure types of priorities trusted by interface. CoS priority exists in the head of 802.1q packets. When you use it, the interface type must be Trunk Tunnel.
4	Switch(config- gigaetherne1/1/1)# mls qos priority <i>portpri-value</i>	Configure the interface priority.

6.2.4 Configuring mapping from CoS to local priority

Configure mapping from CoS to local priority and color for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos mapping cos-to-local-priority <i>profile-id</i>	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.
3	Switch(cos-to-pri)# cos <i>cos-value</i> to local-priority <i>localpri-value</i> [color { green red yellow }]	(Optional) modify the profile of mapping from CoS to local priority and color.
4	Switch(cos-to-pri)# exit Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config-gigaethernet1/1/1)# mls qos cos-to-local-priority <i>profile-id</i>	Apply the profile of mapping from CoS to local priority and color on the interface.

6.2.5 Configuring mapping from DSCP to local priority and color

Configure mapping from DSCP to local priority and color for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos mapping dscp-to-local-priority <i>profile-id</i>	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	Switch(dscp-to-pri)# dscp <i>dscp-value</i> to local-priority <i>localpri-value</i> [color { green red yellow }]	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	Switch(dscp-to-pri)# exit Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config-gigaethernet1/1/1)# mls qos dscp-to-local-priority <i>profile-id</i>	Apply the profile of mapping from DSCP to local priority and color on the interface.

6.2.6 Configuring DSCP mutation

Configure DSCP mutation for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos mapping dscp-mutation <i>profile-id</i>	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.
3	Switch(dscp-mutation)# dscp <i>dscp-value</i> to new-dscp <i>newdscp-value</i>	(Optional) modify the DSCP mutation profile.
4	Switch(dscp-mutation)# exit Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config-gigaethernet1/1/1)# mls qos dscp-mutation <i>profile-id</i>	Apply the DSCP mutation profile on the interface.

6.2.7 Configuring CoS remarking

Configure CoS remarking for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos mapping cos-remark <i>profile-id</i>	Create a CoS remarking profile, and enter cos-remark configuration mode.
3	Switch(cos-remark)# local-priority <i>localpri-value</i> to cos <i>newcos-value</i>	Modify the CoS remarking profile.
4	Switch(dscp-mutation)# exit Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Switch(config-gigaethernet1/1/1)# mls qos cos-remark <i>profile-id</i>	Apply the DSCP remark profile on the interface.

6.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show mls qos sred profile [<i>profile-list</i>]	Show global QoS status and status of the SRED profile.
2	Switch# show mls qos interface [<i>interface-type interface-number</i>]	Show QoS priority, trust mode, and scheduling mode on the interface.
3	Switch# show mls qos mapping cos-to-local-priority [default <i>profile-id</i>]	Show information about mapping from CoS to local priority and color profile.

No.	Command	Description
4	Switch# show mls qos mapping dscp-to-local-priority [default <i>profile-id</i>]	Show information about mapping from DSCP to local priority and color profile.
5	Switch# show mls qos dscp-mutation port-list <i>port-list</i>	Show application of the DSCP mutation profile
6	Switch# show mls qos mapping cos-remark [<i>profile-id</i>]	Show information about the CoS remarking profile.

6.3 Configuring congestion management

6.3.1 Preparing for configurations

Scenario

When a network is congested, you need to balance delay and delay jitter of various packets. Packets of key services (such as video and voice) can be preferentially processed while packets of common services (such as E-mail) with identical priority can be fairly processed. Packets with different priorities can be processed according to its weight value. You can configure queue scheduling in this situation. Choose a schedule algorithm according to service condition and customer requirements.

Prerequisite

Enable global QoS.

6.3.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	<ul style="list-style-type: none"> • WRR weight for scheduling 8 queues is 1. • DRR weight for scheduling 8 queues is 81.

6.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# mls qos queue scheduler sp	Configure queue scheduling mode as SP on the interface.

6.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# mls qos queue scheduler wrr <i>weigh1 weight2 weight3...weight8</i>	Configure queue scheduling mode as WRR on the interface and the weight for each queue.

6.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interfac <i>e interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# mls qos queue scheduler drr <i>weigh1 weight2 weight3...weight8</i>	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

6.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# mls qos queue <i>queue-id</i> shaping cir <i>minband cbs minburst pir</i> <i>maxband [pbs maxburst]</i>	(Optional) configure queue bandwidth guarantee on the interface and set burst size.

6.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show mls qos queue interface <i>interface-type interface-number</i>	Show the weight of queues on the interface.
2	Switch# show mls qos queue statistics interface <i>interface-type interface-number</i>	Show statistics of queues on the interface.
3	Switch# show mls qos queue shaping <i>interface-type interface-list</i>	Show queue shaping on the interface.

6.4 Configuring congestion avoidance

6.4.1 Preparing for configurations

Scenario

To avoid network congestion and solve the problem of TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The SWITCH conducts congestion avoidance based on WRED.

Prerequisite

Enable global QoS.

6.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

6.4.3 Configuring WRED

Configure WRED for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos sred profile profile-id	Create a WRED profile, and enter WRED configuration mode.
3	Switch(sred)# sred [color { red yellow }] start-drop-threshold start-drop value drop-probability drop probability value	Modify the WRED profile.

6.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show mls qos sred profile [profile-list]	Show information about the WRED profile.

6.5 Configuring traffic classification and traffic policy

6.5.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from an upstream device by priorities or ACL rule.

A traffic classification rule will not take effect until it is bound to a traffic policy. Apply traffic policy according to current network loading conditions and period. Usually, the SWITCH limits the rate of transmitting packets according to configured rate when packets enter the network, and re-marks priority according to service feature of packets.

Prerequisite

Enable global QoS.

6.5.2 Default configurations of traffic classification and traffic policy

Default configurations of traffic classification and traffic policy are as below.

Function	Default value
Traffic policy status	Disable
Traffic policy statistics status	Disable

6.5.3 Creating traffic classification

Create traffic classification for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# class-map <i>class-map-name</i> [match-all match-any]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Switch(config-cmap)# description <i>string</i>	(Optional) describe traffic classification.

6.5.4 Configuring traffic classification rules

Configure traffic classification rules for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# class-map <i>class-map-name</i> [match-all match-any]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Switch(config-cmap)# match access-list { <i>access-list</i> <i>name</i> }	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be permit .
4	Switch(config-cmap)# match cos <i>cos-value</i>	(Optional) configure traffic classification based on CoS priority of packets.
5	Switch(config-cmap)# match inner-vlan <i>inner-vlan-value</i>	(Optional) configure traffic classification based on inner VLAN of packets.
6	Switch(config-cmap)# match vlan <i>vlan-value</i>	(Optional) configure traffic classification based on VLANs of packets.
7	Switch(config-cmap)# match dscp <i>dscp-value</i>	(Optional) configure traffic classification based on DSCP priority rule.




Note

- Traffic classification rules must be created for traffic classification; namely, the **match** parameter must be configured.
- For traffic classification quoted by traffic policy, do not modify traffic classification rule; namely, do not modify the **match** parameter of traffic classification.

6.5.5 Creating rate limit rule and shapping rule

When user needs to take rate limit to packets based on traffic policy, please create token bucket and set rate limit and shaping rule to token bucket as well as quote this rule to traffic classification bound to traffic policy.

Create rate limiting rules and shaping rule for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# mls qos policer-profile <i>policer-name</i> [single]	Create a traffic policer profile, and enter traffic-policer configuration mode.
3	Switch(traffic-policer)# cir <i>cir</i> cbs <i>cbs</i>	(Optional) configure flow mode token bucket parameters.  Note Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.
4	Switch(traffic-policer)# cir <i>cir</i> cbs <i>cbs</i> ebs <i>ebs</i>	(Optional) configure RFC2697 mode token bucket parameters.
5	Switch(traffic-policer)# cir <i>cir</i> cbs <i>cbs</i> pir <i>pir</i> pbs <i>pbs</i>	(Optional) configure RFC2698 mode token bucket parameters.
6	Switch(traffic-policer)# cir <i>cir</i> cbs <i>cbs</i> eir <i>eir</i> ebs <i>ebs</i> [coupling]	(Optional) configure RFC4115 mode or MEF token bucket parameters.
7	Switch(traffic-policer)# drop-color red	(Optional) configure the token bucket to discard red packets.
8	Switch(traffic-policer)# recolor { green-recolor red red-recolor green }	(Optional) configure packet recoloring.
9	Switch(traffic-policer)# set-cos { green <i>cos</i> red <i>cos</i> }	(Optional) configure the mapping from packets color to CoS.
10	Switch(traffic-policer)# set-dscp { green <i>green-value</i> red <i>red-value</i> }	(Optional) configure the mapping from packets color to DSCP.
11	Switch(traffic-policer)# set-pri { green <i>green-value</i> red <i>red-value</i> }	(Optional) configure the mapping from packets color to local priority.

6.5.6 Creating traffic policy

Create traffic policy for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# policy-map <i>policy-map-name</i>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Switch(config-pmap)# description <i>string</i>	(Optional) configure description of traffic policy.


6.5.7 Defining traffic policy mapping



Note

Define one or more defined traffic classifications to one traffic policy.

Define traffic policy mapping for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# policy-map <i>policy-map-name</i>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Switch(config-pmap)# class-map <i>class-map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification.  Note At least one rule is required for traffic classification to bind traffic policy, otherwise the binding will fail.

6.5.8 Defining traffic policy operation





Note

Define different operations to different flows in policy.

Define a traffic policy operation for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# policy-map <i>policy-map-name</i>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Switch(config-pmap)# class-map <i>class-map-name</i>	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification.  Note At least one rule is necessary for traffic classification to bind traffic policy, otherwise the binding will fail.
4	Switch(config-pmap-c)# police <i>policer-name</i>	(Optional) apply token bucket on traffic policy and take rate limiting and shaping.  Note The token bucket needs to be created in advance and be configured with rate limiting and shaping rule; otherwise, the operation will fail.
6	Switch(config-pmap-c)# redirect-to port <i>port-id</i>	(Optional) configure re-direct rule under traffic classification, forwarding classified packets from assigned interface.
7	Switch(config-pmap-c)# set { cos <i>cos-value</i> dscp <i>dscp-value</i> local-priority <i>value</i> }	(Optional) configure re-mark rule under traffic classification, modify packet CoS priority, local priority, inner VLAN, DSCP priority, IP priority, and VLAN ID.
8	Switch(config-pmap-c)# copy-to-mirror	(Optional) configure flow mirror to monitor interface.
9	Switch(config-pmap-c)# statistics enable	(Optional) configure flow statistic rule under traffic classification, statistic packets for matched traffic classification.

6.5.9 Applying traffic policy to interfaces

Apply traffic policy to the interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# service-policy ingress <i>policy-map-name</i>	Apply the configured traffic policy to the ingress direction of the interface.

6.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show service-policy statistics interface <i>interface-type interface-number</i> { egress ingress } [class-map <i>class-map-name</i>]	Show traffic policy status and the statistics of the applied policy.
2	Switch# show class-map [<i>class-map-name</i>]	Show information about traffic classification.
3	Switch# show policy-map [<i>policy-map-name</i>]	Show information about traffic policy.
4	Switch# show policy-map [<i>policy-map-name</i>] [class <i>class-map-name</i>]	Show information about traffic classification in traffic policy.
5	Switch# show mls qos policer [<i>policer-name</i>]	Show information about the assigned token bucket (rate limiting and shaping).

6.6 Configuring rate limiting

6.6.1 Preparing for configurations

Scenario

When the network is congested, you wish to restrict burst flow on an interface or VLAN to make packets transmitted in a well-proportioned rate to remove network congestion. In this case, you need to configure rate limiting.

Prerequisite

N/A

6.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.

Step	Command	Description
3	Switch(config-gigaethernet1/1/1)# rate-limit { egress ingress } cir <i>cir-value</i> cbs <i>cbs-value</i>	Configure rate limiting based on interface.



Note

- By default, no interface-based rate limiting is configured.
- Adopt the drop processing mode for packets on the ingress interface if they exceed the configured rate limit.
- When you configure the rate limit and burst for an interface, the burst value should not be much greater if the configured rate limit is smaller than 256 Kbit/s. Otherwise, packets may be inconsecutive.
- When the rate limit is too small, we recommend that the burst value is 4 times greater than then rate limit. If packets are inconsecutive, reduce the burst value or increase the rate limit.
- Packets discarded due to rate limiting on the egress interface are included in statistics of packet loss of the ingress interface.

6.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show rate-limit interface Switch# show rate-limit interface <i>interface-type interface-number</i> [ingress egress]	Show configurations of rate limiting on interfaces.

7 Multicast

This chapter describes basic principle and configuration of multicast and provides related configuration examples, including the following sections:

- Introduction
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP MVR
- IGMP filtering
- PIM-SM

7.1 Introduction

7.1.1 Multicast

With the continuous development of Internet, more and more various interactive data, voice, and video emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services come up with higher requirements for network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During transmission of packets on the network, multicast can save network resources and improve information security.

Comparison among unicast, broadcast and multicast

Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information for them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become an important bottleneck, and unicast will not be conducive to large-scale information transmission.

- **Broadcast:** the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the network segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.
- **Multicast:** when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 7-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

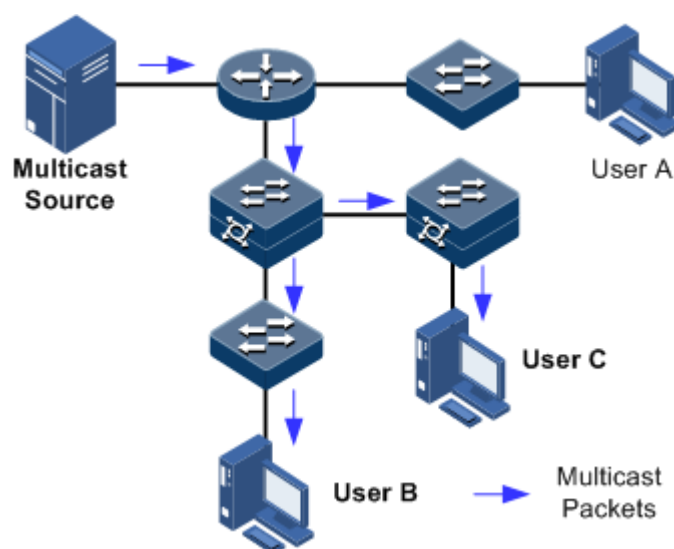


Figure 7-1 Multicast transmission networking

In summary, the unicast is for sparse network users and broadcast is for dense network users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

Compared with unicast and broadcast, multicast has the following advantages:

- **Improve efficiency:** reduce network traffic, relieve server and CPU load.
- **Optimize performance:** reduce redundant traffic and guarantee information security.
- **Support distributed applications:** solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- **Multimedia and streaming media,** such as, network television, network radio, and real-time video/audio conferencing

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing, financial applications (stock)
- Any other "point-to-multipoint" applications

Basic concept in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal network segment connecting with users.

- Router interface

A router interface refers to the interface toward multicast router between a multicast router and a host. The SWITCH receives multicast packets from this interface.

- Member interface

Known as the receiving interface, a member interface is the interface towards the host between multicast router and the host. The SWITCH sends multicast packets from this interface.

Figure 7-2 shows basic concepts in multicast.

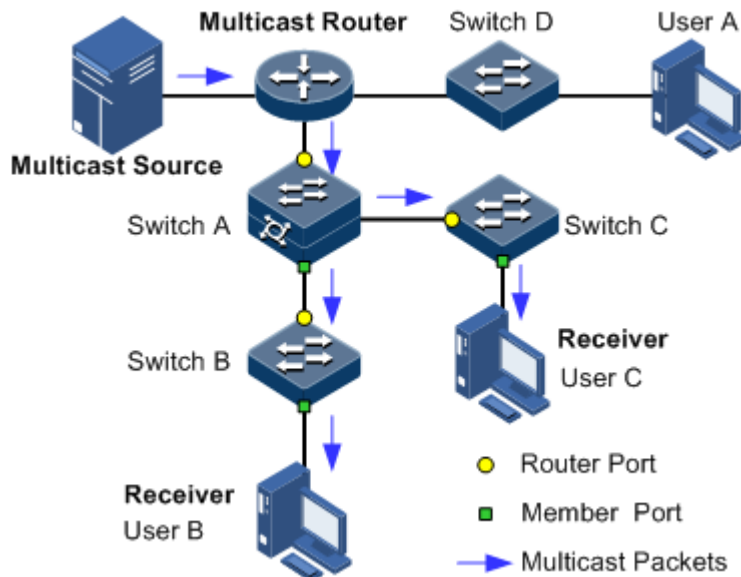


Figure 7-2 Basic concepts in multicast

Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.



Note

The multicast address is the destination address instead of the source address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 7-3 shows mapping between the IP multicast address and MAC address.

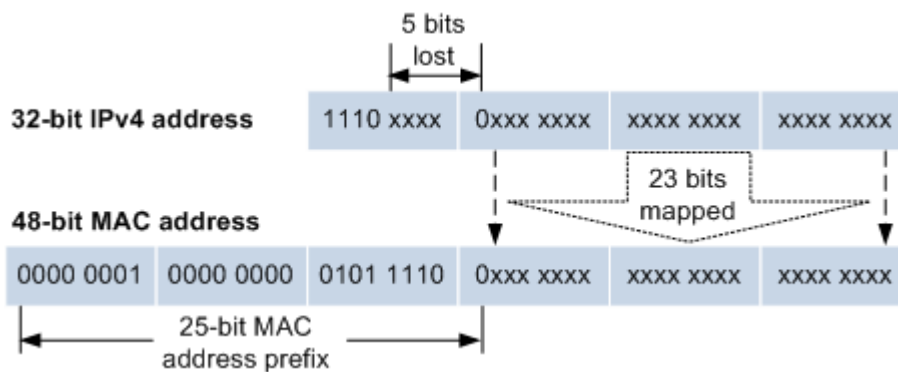


Figure 7-3 Mapping between IPv4 multicast address and multicast MAC address

The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the SWITCH may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the SWITCH.

Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 7-4 shows operating of IGMP and Layer 2 multicast features.

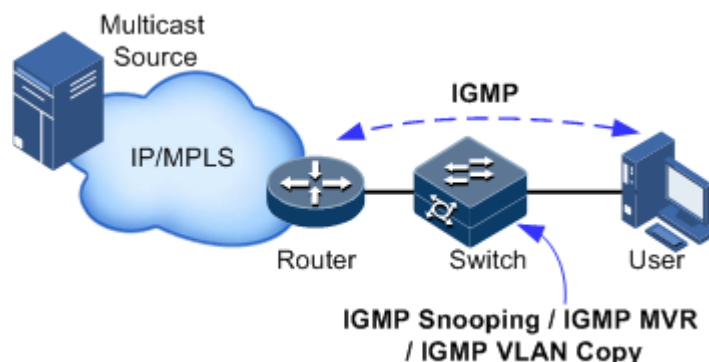


Figure 7-4 Operating of IGMP and Layer 2 multicast features

IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically decides which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected network segment. The multicast data will be forwarded to the network segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the elder version. Currently the most widely used version is IGMPv2, while the Leave packet does not IGMPv1.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The SWITCH supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping
- IGMP Multicast VLAN Registration (MVR)
- IGMP filtering



Note

- IGMP Snooping and IGMP MVR can be enabled concurrently. Multicast VLAN copy and IGMP Snooping, or Multicast VLAN copy and IGMP MVR cannot be enabled concurrently.
- The SWITCH supports both IGMPv1 and IGMPv2.

7.2 Basic functions of Layer 2 multicast

7.2.1 Introduction

Basic functions of Layer 2 multicast are as below:

- Assign the multicast router interface.
- Enable immediate leaving.
- Set multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the SWITCH enabled with IGMP Snooping or IGMP MVR.



Note

Configurations of basic function take effect on IGMP Snooping or IGMP MVR.

The concepts related to IGMP basic functions are as below.

Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or set manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the IGMP Snooping aging time. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast forwarding entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding entry will be updated when an IGMP Report packet is received.

Immediate leaving

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast forwarding entry immediately, but wait until the entry is aged after sending Leave packets. Enable this function to delete the corresponding multicast forwarding entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.



Note

Only IGMP v2/v3 version supports immediate leaving.

IGMP ring network forwarding

On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.

Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.

IGMP ring network forwarding can be applied to the RRPS ring, STP/RSTP/MSTP ring, and G.8032 ring, etc.

7.2.2 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the SWITCH enabled with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

7.2.3 Default configurations of Layer 2 multicast basic functions

Default configurations of Layer 2 multicast basic functions are as below.

Function	Default value
IGMP immediate leaving status	Disable
Multicast forwarding entry aging time	300s
Interface IGMP ring network forwarding status	Disable

7.2.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# igmp mrouter vlan <i>vlan-id</i> <i>interface-type</i> <i>interface-number</i>	(Optional) configure multicast route interface.
3	Switch(config)# igmp immediate-leave <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-list</i>	(Optional) configure immediate leaving.
4	Switch(config)# igmp ring <i>interface-type</i> <i>interface-number-list</i>	(Optional) enable IGMP ring network forwarding on the interface.

7.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show igmp mrouter	Show configurations of the multicast route interface.

No.	Command	Description
2	Switch# show igmp immediate-leave [<i>interface-type interface-number</i>]	Show configuration of immediate leaving on Layer 2 multicast.
3	Switch# show igmp statistics [<i>interface-type interface-number</i>]	Show Layer 2 multicast statistics.

7.2.6 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear igmp statistics [<i>interface-type interface-number</i>]	Clear statistics of Layer 2 multicast IGMP.
Switch(config)# no igmp member <i>interface-type interface-number</i>	Delete a specified multicast forwarding entry.

7.3 IGMP Snooping

7.3.1 Introduction

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the SWITCH to monitor IGMP session between the host and multicast router. When monitoring a group of IGMP Report from host, the SWITCH will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the SWITCH will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the SWITCH will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the SWITCH effectively.

IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.



Note

Currently, the SWITCH supports up to 1024 Layer 2 multicast entries.

7.3.2 Preparing for configurations

Scenario

As shown in Figure 7-5, multiple hosts belonging to a VLAN receive data from the multicast source. Enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

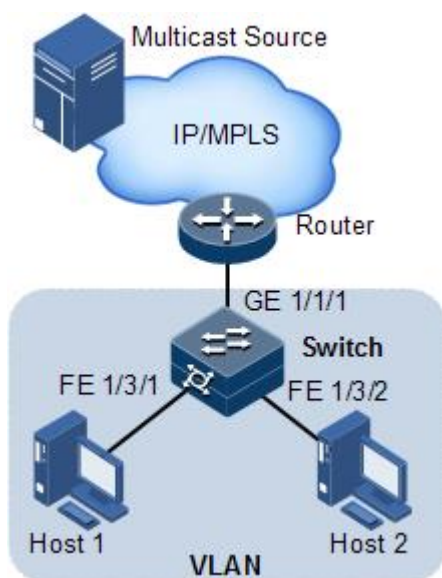


Figure 7-5 IGMP Snooping networking

Prerequisite

- Disable multicast VLAN copy on the SWITCH.
- Create a VLAN, and add related interfaces to the VLAN.

7.3.3 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable

7.3.4 Configuring IGMP Snooping

Configure IGMP Snooping for the SWITCH as below.

Step	Command	Description
1	switch# confi	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# igmp snooping	Enable global IGMP Snooping.
3	Switch(config)# igmp snooping member time-out { <i>seconds</i> infinite }	(Optional) configure the aging time of IGMP members.

7.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show igmp snooping [<i>vlan vlan-list</i>]	Show configurations of IGMP Snooping.
2	Switch# show igmp snooping member [<i>interface-type interface-number</i> vlan vlan-id]	Show information about multicast group members of IGMP Snooping.
3	Switch# show igmp snooping vlan <i>vlan-id</i>	Show configurations of IGMP Snooping in the specified VLAN.

7.4 IGMP MVR

7.4.1 Introduction

IGMP Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

IGMP MVR adds member interfaces belonging to different user VLAN in switch to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated which also increases the security.

Both IGMP MVR and IGMP Snooping can achieve Layer 2 multicast, but the difference is: multicast VLAN in IGMP Snooping is the same with user VLAN, while multicast VLAN in IGMP MVR can be different with user VLAN.



Note

One switch can configure up to 10 multicast VLAN, at least one multicast VLAN and group addresses. The supported maximum number of multicast groups is 1024.

7.4.2 Preparing for configurations

Scenario

As shown in Figure 7-6, multiple users receive data from the multicast source. These users and the multicast router belong to different VLAN. Enable IGMP MVR on Switch A, and configure multicast VLAN. In this way, users in different VLAN can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

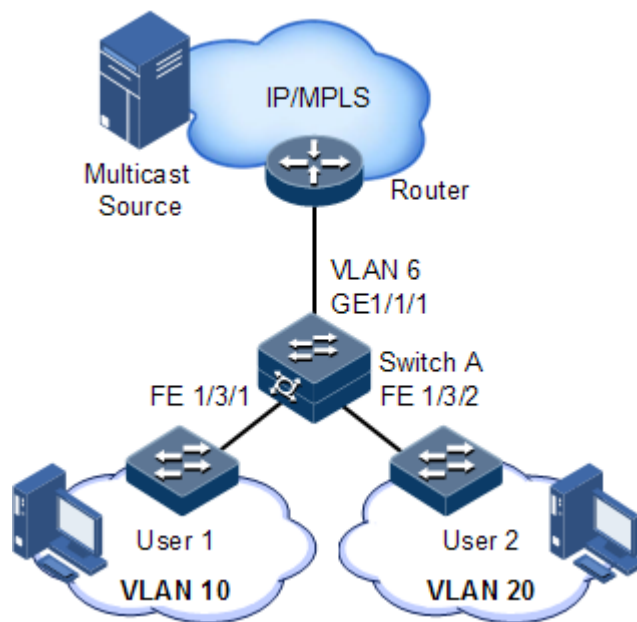


Figure 7-6 IGMP MVR networking

Prerequisite

- Disable multicast VLAN copy.
- Create VLANs and add related interfaces to VLANs.


7.4.3 Default configurations of IGMP MVR

Default configurations of MVR are as below.

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

7.4.4 Configuring IGMP MVR

Configure IGMP MVR for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# igmp mvr	Enable global IGMP MVR.
3	Switch(config)# igmp mvr mcast-vlan vlan-id group { start-ip-address [end-ip-address] any }	Configure group address set for multicast VLAN.  Note After IGMP MVR is enabled, you need to configure multicast VLAN and bind group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.

7.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show igmp mvr [<i>interface-type interface-number</i>]	Show configurations of IGMP MVR.
2	Switch# show igmp mvr member [<i>interface-type interface-number</i> user-vlan <i>vlan-id</i>]	Show information about multicast group members of IGMP MVR.
3	Switch# show igmp mvr vlan-group [mcast-vlan <i>vlan-id</i>]	Show multicast VLAN and its group address set.

7.5 IGMP filtering

7.5.1 Introduction

To control user access, you can set IGMP filtering. IGMP filtering contains the range of accessible multicast groups passing filtering rules and the maximum number of groups.

- IGMP filter profile

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

Configure IGMP Profile filter profile to control the interface. One IGMP Profile can be set one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filter profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and does not allow receiving this group of multicast data.

IGMP filter profile can be configured on an interface or interface+VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

The maximum allowed adding number of multicast groups and the maximum group number rule can be set on an interface or interface+VLAN.

The maximum group number rule sets the actions for reaching the maximum number of multicast group users added, which can be no longer allowing user adding groups, or covering the original adding group.



Note

IGMP filtering is generally used with IGMP Snooping/IGMP MVR/multicast VLAN copy.

7.5.2 Preparing for configurations

Scenario

The different users in the same multicast group receive different multicast requirements and permissions, allow configuring filter rule on switch which connects multicast router and user host to restrict multicast users. It also can set the maximum number of multicast group allowed user joining. IGMP Proxy is generally used with IGMP Snooping or IGMP MVR.

Prerequisite

Create VLANs and add interfaces to the corresponding VLANs.

7.5.3 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filter profile Profile	N/A
IGMP filter profile action	Refuse
IGMP filtering under interface	No maximum group limit, the largest group action is drop, no application filter profile
IGMP filtering under interface+VLAN	No maximum group limit, the largest group action is drop, no application filter profile

7.5.4 Enabling global IGMP filtering

Enable global IGMP filtering for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode
2	Switch(config)# igmp filter	Enable global IGMP filtering



Note

When configuring IGMP filter profile or the maximum group number, use the **igmp filter** command to enable global IGMP filtering.

7.5.5 Configuring IGMP filter profile

IGMP filter profile can be used to interface or interface+VLAN.

Configure IGMP filter profile for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode
2	Switch(config)# igmp filter profile <i>profile-number</i>	Create IGMP Profile and enter Profile configuration mode.
3	Switch(config-igmp-profile)#{ permit deny }	Configure IGMP Profile action.
4	Switch(config-igmp-profile)# range <i>range-id start-ip-address [end-ip-address]</i>	Configure to control IP multicast address access and range.
5	Switch(config-igmp-profile)# exit Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
6	Switch(config-gigaethernet1/1/1)# igmp filter profile <i>profile-number [vlan vlan-list]</i>	Configure IGMP Profile filter profile to physical interface or interface+VLAN.
	Switch(config-aggregator)# igmp filter profile <i>profile-number [vlan vlan-list]</i>	Configure IGMP Profile filter profile to LAG interface or interface+VLAN.



Note

Perform the command of **igmp filter profile** *profile-number* in interface configuration mode to make the created IGMP Profile apply to the specified interface. One IGMP Profile can be applied to multiple interfaces, but each interface can have only one IGMP Profile.

7.5.6 Configuring maximum number of multicast groups

You can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configure the maximum number of multicast groups for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Switch(config-gigabitEthernet1/1/1)# igmp filter max-groups <i>group-number</i> [vlan <i>vlan-list</i>]	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	Switch(config-aggregator)# igmp filter max-groups <i>group-number</i> [vlan <i>vlan-list</i>]	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
4	Switch(config-gigabitEthernet1/1/1)# igmp filter max-groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action over maximum number of multicast groups in physical interface or interface+VLAN.
	Switch(config-aggregator)# igmp filter max-groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action over maximum number of multicast groups in LAG interface or interface+VLAN.

7.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show igmp filter [interface <i>interface-type interface-number</i> [vlan <i>vlan-id</i>]]	Show configurations of IGMP filtering.
2	Switch# show igmp filter profile [<i>profile-number</i>]	Show information about the IGMP profile.

7.6 PIM-SM

7.6.1 Introduction

Protocol Independent Multicast-Dense Mode (PIM-DM) is a dense-mode multicast route protocol and fits for a network with a wide distribution of group members, wide range, and large scale. PIM-SM is independent of any unicast routing protocol, so it is called the protocol independent multicast routing protocol.

Figure 7-7 shows the function and location of PIM-SM in the multicast network.

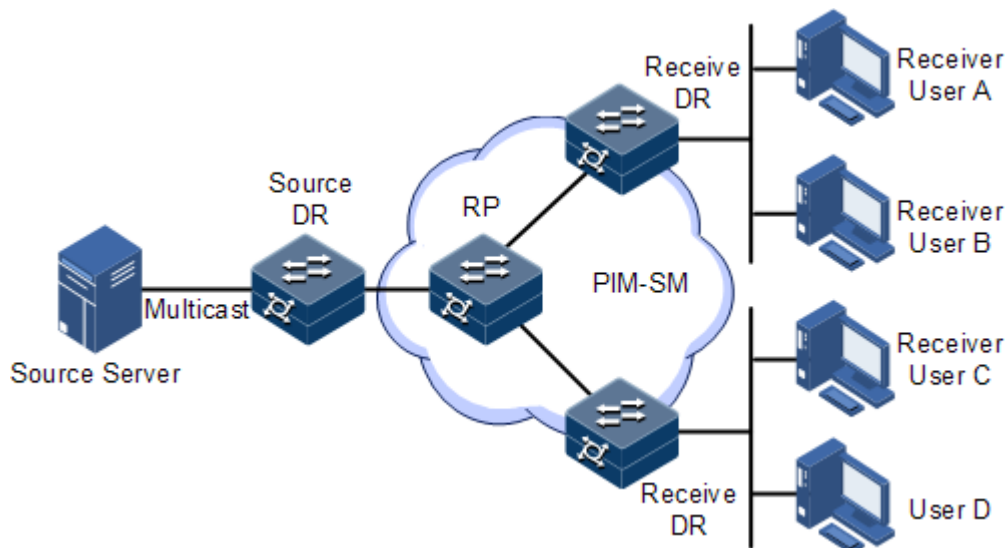


Figure 7-7 PIM-SM networking

PIM-SM devices discover neighbors by sending Hello packets. Once a PIM-SM device is started, it periodically sends Hello packets on the PIM-SM interface. The neighbor discovery mechanism defines the neighbor holding time of Hello packets, namely, the maximum time for a neighbor to wait for the next Hello packet. If the neighbor receives the next Hello packet within the time, it deletes the device from its neighbor list.

PIM-SM uses joining and pruning to establish multicast distribution trees. The receiver sends the Report message to the receiver DR, which then sends the (*,G) joining packet towards the RP direction to establish the shared tree. The multicast source sends data and DR sends an application to be registered by the RP.

- If the RP has a receiver, it sends the (S,G) joining packet in the multicast source direction to establish the source tree. The multicast source packets in the PIM-SM network reach the RP along the shared tree to the receiver. When the receiver leaves, it sends the Leave packet to the receiver DR, which then sends the (*,G) pruning packets to prune the shared tree.
- If the RP has no receiver, it sends the (S,G) pruning packets to the multicast source direction to prune the source tree.

PIM-SM uses SPT switching to relieve the load of the shared tree. The receiving DR chooses a proper switching policy to switch (S,G) data to the SPT tree to relieve the load of the RPT tree. When the receiving DR meets the switching policy, the receiving DR sends the (S,G) joining packet to the multicast source direction to establish the SPT tree from the multicast source to the receiving DR, and sends the (S,G,rpt) pruning packet in the RP direction to prune multicast traffic of (S,G) on the RPT tree, thus relieving the load of the shared tree.

7.6.2 Preparing for configurations

Scenario

PIM-SM is a dense mode multicast route protocol, and is fit for small network with multicast member densely distributed. By configuring PIM-SM, you can implement multicast route and data forwarding.

Prerequisite

N/A

7.6.3 Default configurations of PIM-SM

Default configurations of PIM-SM are as below.

Function	Default value
Interface PIM-SM status	Disable
DR priority	1
Multicast source KeepAlive time	210s

7.6.4 Configuring dynamic RP

Configure the dynamic RP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip pim sparse-mode	Enable PIM-SM on the physical interface.
4	Switch(config-gigaethernet1/1/1)# ip pim dr-priority <i>priority-value</i>	Configure the DR priority of the physical interface.
5	Switch(config-gigaethernet1/1/1)# exit Switch(config)# router pim	Enter PIM mode.
6	Switch(config-router-pim)# bsr-candidate { <i>interface-type interface-number vlan vlan-id loopback interface-number</i> } [hash-mask-length <i>mask-length</i>] [priority <i>priority</i>]	Configure the candidate BSR.

Step	Command	Description
7	Switch(config-router-pim)# rp-candidate { <i>interface-type interface-number</i> vlan <i>vlan-id</i> loopback <i>interface-number</i> } [group <i>ip-addresss/mask</i>]	Configure the candidate RP.
8	Switch(config-router-pim)# spt-threshold infinity [group-policy <i>acl-number</i>]	Configure SPT switching control parameters.
9	Switch(config-router-pim)# source-lifetime <i>interval</i>	Configure the aging time of multicast routing entries.

7.6.5 Configuring static RP

Configure the static RP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# ip pim sparse-mode	Enable PIM-SM on the physical interface.
4	Switch(config-gigaetherne1/1/1)# exit Switch(config)# router pim	Enter PIM mode.
5	Switch(config-router-pim)# rp-address <i>ip-address</i> [group <i>ip-addresss/mask</i>]	Configure the IP address of the static RP.

7.6.6 Configuring Layer 3 multicast forwarding

Configure Layer 3 multicast forwarding for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip multicast routing	Enable Layer 3 multicast forwarding.

7.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip pim neighbor	Show information about PIM neighbors.
2	Switch# show ip pim interface	Show information about PIM interfaces.
3	Switch# show ip pim bsr-router	Show BSR information.
4	Switch# show ip pim rp-candidate	Show information about candidate RPs.
5	Switch# show ip pim rp	Show RP information.
6	Switch# show ip pim route	Show information about the PIM multicast routing table.

8 Security

This chapter describes basic principle and configuration of security and provides related configuration examples, including the following sections.

- ACL
- Secure MAC address
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+

8.1 ACL

8.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the SWITCH to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from influencing network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port ID of data packets. The SWITCH judges receiving or rejecting packets according to the rules.

8.1.2 Preparing for configurations

Scenario

ACL can help a network device recognize filter data packets. The device recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL is divided into the following types:

- IP ACL: define classification rules according to source or destination address taken by packets IP head, port ID used by TCP or UDP (being 0 by default), etc. attributes.
- MAC ACL: define classification rules according to source MAC address, destination MAC address, Layer 2 protocol type taken by packets Layer 2 frame head, etc. attributes.
- MAP ACL: MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, also can match any Bytes from Byte 0 to Byte 127 of Layer 2 data frame according to user's definition (the offset starts from 0).

There are 4 ACL modes according to difference of application environment:

- ACL based on device
- ACL based on interface
- ACL based on flow from ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

8.1.3 Configuring MAC ACL

Configure MAC ACL for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# access-list <i>acl-number</i> [name <i>acl-name</i>]	Create an ACL, and enter ACL configuration mode. <ul style="list-style-type: none"> • When the ACL number is 1000–1999, this configuration enters basic IP ACL configuration mode. • When the ACL number is 2000–2999, this configuration enters extended IP ACL configuration mode. • When the ACL number is 3000–3999, this configuration enters MAC ACL configuration mode. • When the ACL number is 5000–5999, this configuration enters User ACL configuration mode. • When the ACL number is 6000–6999, this configuration enters IPv6 ACL configuration mode. • When the ACL number is 7000–7999, this configuration enters advanced ACL configuration mode.
3	Switch(config-acl-ip-std)# rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address</i> <i>source-ip-mask</i> any }	(Optional) configure the matching rule for basic IP ACL.
4	Switch(config-acl-ipv4-advanced)# rule [<i>rule-id</i>] { deny permit } { <i>protocol-id</i> icmp igmp ip } { <i>source-ip-address</i> <i>source-ip-mask</i> any } { <i>destination-ip-address</i> <i>destination-ip-mask</i> any } [dscp <i>dscp-value</i>] [ttl <i>ttl-value</i>] [fragment] [icmp-type <i>icmp-type-value</i>] [precedence <i>precedence-value</i>] [tos <i>tos-value</i>]	(Optional) configure the matching rule for extended IP ACL.

Step	Command	Description
	<pre>Switch(config-acl-ipv4-advanced)# rule [rule-id] { deny permit } { tcp udp } { source-ip-address source-ip-mask any } [source- port] [range minimum source port maximum source port] { destination- ip-address destination-ip-mask any } [destination-port] [ack ack- value] [dscp dscp-value] [fin fin-value] [fragment] [precedence precedence-value] [psh psh-value] [range minimum source port maximum source port] [rst rst-value] [syn syn-value] [tos tos-value] [urg urg-value] [ttl ttl-value]</pre>	
5	<pre>Switch(config-acl-mac)#rule [rule- id] { deny permit } { source-mac- address source-mac-mask any } { destination-mac-address destination-mac-mask any } [ethertype { ethertype [ethertype- mask] ip arp }] [svlan svlanid] [cos cos-value] [cvlan cvlanid] [inner-cos inner-cos]</pre>	(Optional) configure the matching rule for MAC ACL.
6	<pre>Switch(config-acl-udf)#rule [rule- id] { deny permit } { ipv4 layer2 } rule-string rule-mask offset</pre>	(Optional) configure the matching rule for User ACL.
7	<pre>Switch(config-acl-ipv6)#rule [rule- id] { deny permit } { protocol-id ipv6 icmpv6 } { source-ipv6- address/prefix any } { destination- ipv6-address/prefix any } [dscp dscp-value] [fragment] [flow-label flow label-value] Switch(config-acl-ipv6)#rule [rule- id] { deny permit } { tcp udp } { source-ipv6-address/prefix source- ip-mask any } { destination- ipv6-address/prefix any } [destination- port] [ack ack-value] [dscp dscp- value] [fin fin-value] [fragment] [flow-label flow label- value] [psh psh-value] [rst rst- value] [syn syn-value] [urg urg- value]</pre>	(Optional) configure the matching rule for MAP ACL.

Step	Command	Description
8	Switch(config)# rule [<i>rule-id</i>] { deny permit } { <i>source-mac-address</i> <i>source-mac-mask</i> any } { <i>destination-mac-address</i> <i>destination-mac-mask</i> any } [svlan <i>svlanid</i>] [cos <i>cos-value</i>] [cvlan <i>cvlanid</i>] [inner-cos <i>inner-cos</i>] { <i>source-ip-address</i> <i>source-ip-mask</i> any } { <i>destination-ip-address</i> <i>destination-ip-mask</i> any } [dscp <i>dscp-value</i>] [ttl <i>ttl-value</i>] [fragment] [precedence <i>precedence-</i> <i>value</i>] [tos <i>tos-value</i>]	(Optional) configure the matching rule for advanced ACL.

8.1.4 Configuring filter

Configure the filter for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# filter { ingress egress } access-list <i>acl-number</i> [statistics]	Apply ACL on the interface.

8.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show access-list [<i>acl-number</i>]	Show ACL configurations.
2	Switch# show acl resource { egress ingress } <i>interface-type interface-list</i>	Show resources used by ACL.
3	Switch# show filter interface Switch# show filter interface <i>interface-type</i> <i>interface-number</i> [ingress egress] Switch# show filter interface <i>interface-type</i> <i>interface-number</i> [ingress egress] [access-list <i>acl-number</i>]	Show filter configurations.

8.2 Secure MAC address

8.2.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side, which can ensure the security of access data in some interface, control the input packets according to source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

The static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the device. You can set the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses ages and does not support configuration load.

The dynamic secure MAC address can be converted to Sticky secure MAC address if necessary, so as not to be aged and supports auto-loading.

- Sticky secure MAC address

Sticky secure MAC address is generated from the manual configuration of user in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, Sticky secure MAC address needs to be used in conjunction with Sticky learning:

- When Sticky learning is enabled, Sticky secure MAC address will take effect and this address will not be aged.
- When Sticky learning is disabled, Sticky secure MAC address will lose effectiveness and be saved only in the system.



Note

- When Sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to Sticky secure MAC addresses.
- When Sticky learning is disabled, all Sticky secure MAC addresses on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating secure MAC address

When the number of secure MAC addresses has already reached the maximum number, the strange source MAC address packets inputting will be regarded as violation operation. For the illegal user access, there are different processing modes to configure the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system.
- Shutdown mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system and then shutdown the secure interface.



Caution

When the MAC address is in drift, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will take it as violation processing.

8.2.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the input packets according to source MAC address. With secure MAC address, you can configure permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with secure MAC address violation policies.

Prerequisite

N/A

8.2.3 Default configurations of secure MAC address

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	300s
Aging type of dynamic secure MAC address	Absolute
Restoration time of port security MAC	Disable, namely, no restoration
Dynamic secure MAC Sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
Maximum number of port security MAC	1

8.2.4 Configuring basic functions of secure MAC address



Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using MAC address management function to configure static MAC addresses when port security MAC is enabled.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.
- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of secure MAC address for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# switchport port-security	Enable port security MAC.
4	Switch(config- gigaethernet1/1/1)# switchport port-security maximum <i>maximum</i>	(Optional) configure the maximum number of secure MAC addresses.
5	Switch(config- gigaethernet1/1/1)# switchport port-security violation { protect restrict shutdown }	(Optional) configure secure MAC violation mode.
6	Switch(config- gigaethernet1/1/1)# no port- security shutdown Switch(config- gigaethernet1/1/1)# exit	(Optional) re-enable the interface which is shut down due to violating the secure MAC address.
7	Switch(config)# port-security recovery-time <i>second</i>	(Optional) configure the restoration time of port security MAC.



Note

When secure MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating secure MAC address. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

8.2.5 Configuring static secure MAC address

Configure static secure MAC address for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne t1/1/1)#switchport port-security	Enable port security MAC.
4	Switch(config-gigaetherne t1/1/1)#switchport port-security mac-address mac-address vlan vlan-id	Configure static secure MAC address.

8.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# port-security aging-time period	(Optional) configure the aging time of dynamic secure MAC address.
3	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Switch(config-gigaetherne t1/1/1)#switchport port-security aging-type { absolute inactivity }	(Optional) configure the aging type of port security MAC addresses.
5	Switch(config-gigaetherne t1/1/1)#switchport port-security	(Optional) enable port dynamic security MAC learning.
6	Switch(config-gigaetherne t1/1/1)#switchport port-security trap enable	(Optional) enable port security MAC Trap.



Note

The **switchport port-security** command can enable port security MAC as well as dynamic secure MAC learning at the same time.

8.2.7 Configuring Sticky secure MAC address



Caution

We do not recommend configuring Sticky secure MAC addresses when port Sticky security MAC is disabled. Otherwise, port Sticky security MAC may be in anomaly.

Configure Sticky secure MAC address for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaether- net1/1/1)# switchport port- security	Enable port security MAC.
4	Switch(config-gigaether- net1/1/1)# switchport port- security mac-address sticky	Enable Sticky secure MAC learning.
5	Switch(config-gigaether- net1/1/1)# switchport port- security mac-address sticky <i>mac-address</i> vlan <i>vlan-id</i>	(Optional) manually configure Sticky secure MAC addresses.



Note

After Sticky secure MAC address learning is enabled, dynamic secure MAC address will be converted to Sticky secure MAC address; the manually configured Sticky secure MAC address will take effect.

8.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show port-security [<i>interface-type interface-list</i>]	Show configurations of port security MAC.
2	Switch# show port-security mac-address [<i>interface-type</i> <i>interface-list</i>]	Show configurations of secure MAC address and secure MAC address learning.

8.2.9 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config-gigaether- net1/1/1)# clear port-security { all configured dynamic sticky }	Clear a specified secure MAC address type on a specified interface.

8.3 Dynamic ARP inspection

8.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: set the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

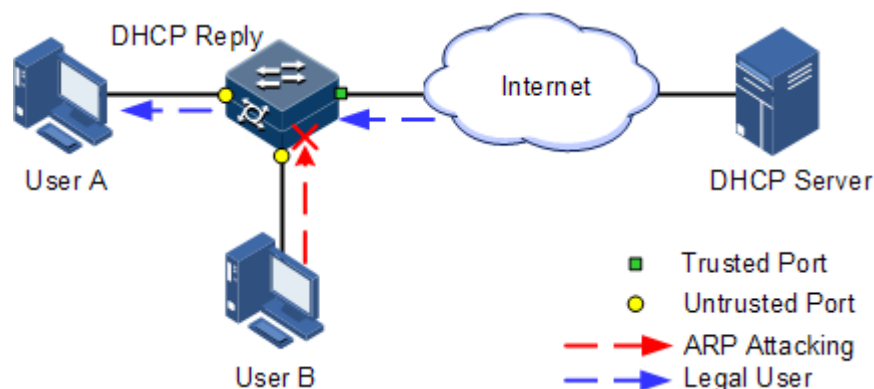


Figure 8-1 Principle of dynamic ARP inspection

Figure 8-1 shows the principle of dynamic ARP inspection. When the SWITCH receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the SWITCH by sending a large number of ARP packets to the SWITCH.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface receives an ARP attack, and then discard all received ARP packets to avoid the attack.
- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Dynamic ARP inspection can also protect the specified VLAN. After the protection VLAN is configured, the ARP packets in specified VLAN on an untrusted interface will be protected. Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

8.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent the common ARP spoofing attacks on the network, which isolates the ARP packets with unsafe sources. Trust status of an interface depends whether it trust ARP packets. However, the binding table decides whether the ARP packets meet requirement.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

8.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Dynamic ARP inspection dynamic binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting on ARP packets	Disable
Interface rate limiting on ARP packets	60 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

8.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# ip arp-inspection trust	Set the interface to a trusted interface. Use the no ip arp-inspection trust command to set the interface to an untrusted interface, that is, the interface does not trust the ARP packet.

8.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip arp-inspection static-config	Enable global static ARP binding.
3	Switch(config)# ip arp-inspection binding <i>ip-address</i> [<i>mac-address</i>] [vlan <i>vlan-id</i>] <i>interface-type interface-number</i>	Configure the static binding.

8.3.6 Configuring dynamic binding of dynamic ARP inspection



Caution

Before enabling dynamic binding of dynamic ARP inspection, you need to use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip arp-inspection dhcp-snooping	Enable global dynamic ARP binding.

8.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip arp-inspection dhcp-snooping	Enable global dynamic ARP binding.
3	Switch(config)# ip arp-inspection vlan <i>vlan-list</i>	Configure protection VLAN of dynamic ARP inspection.

8.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaehternet1/1/1)# ip arp-rate-limit enable	Enable interface ARP packet rate limiting.
4	Switch(config-gigaehternet1/1/1)# ip arp-rate-limit rate <i>rate-value</i>	Configure rate limiting on ARP packets on the interface.

8.3.9 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip arp-rate-limit recover enable	Enable auto-recovery for rate limiting on ARP packets.
3	Switch(config)# ip arp-rate-limit recover time <i>time</i>	Configure the auto-recovery time for rate limiting on ARP packets.

8.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip arp-inspection	Show configurations of dynamic ARP inspection.

No.	Command	Description
2	Switch# show ip arp-inspection binding [<i>interface-type interface-number</i>]	Show information about the dynamic ARP inspection binding table.
3	Switch# show ip arp-rate-limit	Show configurations of rate limiting on ARP packets.

8.4 RADIUS

8.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication

RADIUS adopts client/server mode, network access device is used as client of RADIUS server. RADIUS server receives user connecting requests and authenticates users, then reply configurations to all clients for providing services. Control user access device and network and improve network security.

Communication between client and RADIUS server is authenticated by sharing key, which will not be transmitted on network. Besides, all user directions need to be encrypted when transmitting between client device and RADIUS server to ensure security.

RADIUS accounting

RADIUS accounting is used to authenticate users through RADIUS. When logging in, a user sends a starting account packet to the RADIUS accounting server, according to the accounting policy to send update packet to the RADIUS server. When logging off, the user sends a stopping account packet to the RADIUS accounting server, and the packet includes user online time. The RADIUS accounting server can record the access time and operations for each user through packets.

8.4.2 Preparing for configurations

Scenario

You can deploy RADIUS server on the network to take authentication and accounting to control user access to device and network. This device can be used as agent of RADIUS server, which authorizes user accessing according to feedback from RADIUS.

Prerequisite

N/A

8.4.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS server	0.0.0.0
IP address of RADIUS accounting server	0.0.0.0
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with RADIUS accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0


8.4.4 Configuring RADIUS authentication

Configure RADIUS authentication for the SWITCH as below.

Step	Command	Description
1	Switch#radius [backup] ip-address [auth-port port-id] [vpn-instance vrf-name] [sourceip ip-address]	Assign the IP address and port ID for RADIUS authentication server. Configure the backup parameter to assign the backup RADIUS authentication server.
2	Switch#radius-key string	Configure the shared key for RADIUS authentication.
3	Switch#user login { local-radius local-user radius-local [server-no-response] radius-user local-tacacs tacacs-local [server-no-response] tacacs-user }	Configure users to perform login authentication through RADIUS.
4	Switch#enable login { local-tacacs tacacs-local tacacs-user }	Set the authentication mode for users to enter privileged EXEC mode to RADIUS.

8.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the SWITCH as below.

Step	Command	Description
1	Switch#aaa accounting login enable	Enable RADIUS accounting.
2	Switch#radius [backup] accounting-server ip-address [account-port] [sourceip ip-address]	Assign IP address and UDP port ID for RADIUS accounting server. Configure the backup parameter to assign the backup RADIUS accounting server.
3	Switch#radius accounting-server key string	Configure the shared key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
4	Switch#aaa accounting fail { offline online }	Configure the processing policy for accounting failure.
5	Switch#aaa accounting update minute	Configure the period for sending accounting update packets. If it is configured as 0, no accounting update packet is sent.  Note The RADIUS accounting server can record access time and operation for each user through accounting starting packets, update packets and accounting end packets.

8.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch#show radius-server	Show configurations of the RADIUS server.
2	Switch#show aaa	Show configurations of RADIUS accounting.

8.5 TACACS+

8.5.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UDP port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely used.

8.5.2 Preparing for configurations

Scenario

To control users accessing to the SWITCH and the network, you can authenticate and account users by deploying the TACACS+ server on the network. Compared with RADIUS, TACACS+ is safer and more reliable. The SWITCH can be used as the agent of the TACACS+ server, controlling users according to feedback result from the TACACS+ server.

Prerequisite

N/A

8.5.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key used for communication with TACACS+ accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0

8.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the SWITCH as below.

Step	Command	Description
1	Switch# tacacs-server [backup] <i>ip-address</i>	Assign the IP address and port ID for the TACACS+ authentication server. Configure the backup parameter to assign the backup TACACS+ authentication server.
2	Switch# tacacs-server key <i>string</i>	Configure the shared key for TACACS+ authentication.
3	Switch# user login { local-tacacs tacacs-local [server-no-response] tacacs-user }	Configure users to perform login authentication through TACACS+.
4	Switch# enable login { local-tacacs tacacs-local [server-no-response] tacacs-user }	Set the authentication mode for users to enter privileged EXEC mode to TACACS+.

8.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the SWITCH as below.

Step	Command	Description
1	Switch# aaa accounting login enable	Enable TACACS+ accounting.
2	Switch# tacacs [backup] accounting-server <i>ip-address</i>	Assign the IP address and UDP port ID for the TACACS+ accounting server. Configure the backup parameter to assign the backup TACACS+ accounting server.
3	Switch# tacacs-server key <i>string</i>	Configure the shared key to communicate with the TACACS+ accounting server.
4	Switch# aaa accounting fail { offline online }	Configure the processing policy for accounting failure.
5	Switch# aaa accounting update <i>period</i>	Configure the period for sending accounting update packets. If configured as 0, no accounting update packet is sent.

8.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show tacacs-server	Show configurations of the TACACS+ authentication server.

No.	Command	Description
2	Switch# show aaa	Show configurations of TACACS+ accounting.

8.5.7 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch# clear tacacs statistics	Clear TACACS+ statistics.

8.6 Storm control

8.6.1 Introduction

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm may occur and occupies much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the SWITCH does not support multicast nor have a multicast MAC address table, so it processes received multicast packets as unknown multicast packets.
- Broadcast packets: packets of which the destination MAC is a broadcast address. If these packets are excessive in a period, broadcast storm may occur.

Principle of storm control

Storm control allows an interface to filter broadcast packets received by the interface. After storm control is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

Types of storm control

Storm controls is performed in the following forms:

- Radio (bandwidth ratio): the allowed percentage of broadcast, unknown multicast, or unknown unicast traffic to total bandwidth
- Bits Per Second (BPS): the number of bits allowed to pass per second
- Packet Per Second (PPS): the number of packets allowed to pass per second

The SWITCH supports BPS and PPS storm control.

8.6.2 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply on the network. In this case, normal packets can be properly forwarded.

Prerequisite

N/A

8.6.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control	Enable
Multicast and unknown unicast storm control	Disable
Bytes of frame gap and preamble	20 Bytes
Storm control mode	bps
Bytes per second	64 Kbit/s
Number of allowed storm packets per second	1024 pps
DLF packet forwarding	Enable

8.6.4 Configuring storm control



Caution

Storm control and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.

Configure storm control for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# storm- control { broadcast multicast unicast } kbps value	Enable storm control over broadcast traffic, multicast traffic, and unknown unicast traffic.



Caution

The SWITCH does not support configuring multiple control modes on the same interface regardless whether storm control is enabled. To change the control mode and control threshold of some packet on the interface, perform one of the following operations:

- If the value is set to the default one, the control modes and control thresholds of all packets on an interface are identical.
- If the value is not set to the default one, configurations fail. In addition, the system asks you to delete configurations on the interface in advance. In this case, you should set the control threshold of all packets in a control mode to the default value. In addition, you should configure control modes of all packets and then configure other control thresholds.

8.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# d1f- forwarding enable	Enable DLF packet forwarding on an interface.

8.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show storm-control [<i>interface-type interface-</i> <i>number</i>]	Show configurations of storm control.
2	Switch# show d1f-forwarding	Show DLF packet forwarding status.

8.7 802.1x

8.7.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 8-2, 802.1x authentication uses C/S mode, including the following 3 parts:

- **Supplicant:** a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- **Authenticator:** an access control device supporting 802.1x authentication, such as a switch
- **Authentication Server:** a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

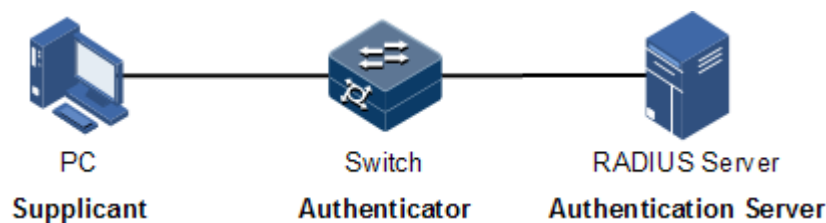


Figure 8-2 802.1x structure

Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- **Protocol authorized mode (auto):** the protocol state machine decides the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- **Force interface authorized mode (authorized-force):** the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- **Force interface unauthorized mode (unauthorized-force):** the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch, that is, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports finishing authentication procedure between the RADIUS server through EAP relay and EAP termination.

- EAP relay

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packet. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS protocol packet to be transmitted to the authentication server through a complex network. This procedure is call EAP relay.

Both the authenticator and the suppliant can initiate the 802.1x authentication procedure. This guide takes the suppliant for an example, as shown below:

- Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.
- Step 2 The authenticator sends an EAP-Request/Identity to the suppliant, asking the user name of the suppliant.
- Step 3 The suppliant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.
- Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS protocol packet and sends the RADIUS protocol packet to the authentication server.
- Step 5 The authentication server compares the received user name with the one in the database, finds the password for the user, and encrypts the password with a randomly-generated encryption word. Meanwhile it sends the encryption word to the authenticator who then sends the encryption word to the suppliant.
- Step 6 The suppliant encrypts the password with the received encryption password, and sends the encrypted password to the authentication server.
- Step 7 The authentication server compares with received encrypted password with the one generated by itself. If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the suppliant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the suppliant.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

802.1x timers

During 802.1x authentication, the following 5 timers are involved:

- **Reauth-period:** re-authorization timer. After the period is exceeded, the SWITCH re-initiates authorization.
- **Quiet-period:** quiet timer. When user authorization fails, the SWITCH needs to keep quiet for a period. After the period is exceeded, the SWITCH re-initiates authorization. During the quiet time, the SWITCH does not process authorization packets.
- **Tx-period:** transmission timeout timer. When the SWITCH sends a Request/Identity packet to users, the SWITCH will initiate the timer. If users do not send an authorization response packet during the tx-period, the SWITCH will re-send an authorization request packet. The SWITCH sends this packet three times in total.
- **Supp-timeout:** Supplicant authorization timeout timer. When the SWITCH sends a Request/Challenge packet to users, the SWITCH will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the SWITCH will re-send the Request/Challenge packet. The SWITCH sends this packet twice in total.
- **Server-timeout:** Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time is exceeded, the authenticator will end the session with RADIUS server and start a new authorization process.

8.7.2 Preparing for configurations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the SWITCH.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The SWITCH can ping through the RADIUS server successfully.

8.7.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	Chap
Interface access control mode	Auto
Authentication method	Portbased
Re-authentication	Disable

Function	Default value
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
transmission timeout timer	30s
Supplicant authorization timeout timer	30s

8.7.4 Configuring basic functions of 802.1x

Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# dot1x enable	Enable global 802.1x.
3	Switch(config)# dot1x authentication-method { chap pap eap }	Configure global authentication mode.
4	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
5	Switch(config-gigabitEthernet1/1/1)# dot1x enable	Enable interface 802.1x.
6	Switch(config-gigabitEthernet1/1/1)# dot1x auth-control { auto authorized-force unauthorized-force }	Configure access control mode on the interface.
7	Switch(config-gigabitEthernet1/1/1)# dot1x auth-method { portbased macbased }	Configure access control mode of 802.1x authentication on the interface.

Note

If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is set to force interface authorized mode.

8.7.5 Configuring 802.1x re-authentication



Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

Configure 802.1x re-authentication for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaetherne1/1/1)# dot1x reauthentication enable	Enable 802.1x re-authentication.

8.7.6 Configuring 802.1x timers

Configure 802.1x timers for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaetherne1/1/1)# dot1x timer reauth-period <i>reauth-period</i>	Configure the time of the re-authentication timer.
4	Switch(config- gigaetherne1/1/1)# dot1x timer quiet-period <i>second</i>	Configure the time of the quiet timer.
5	Switch(config- gigaetherne1/1/1)# dot1x timer supp-timeout <i>supp-timeout</i>	Configure the time of the supplicant authorization timeout timer.
6	Switch(config- gigaetherne1/1/1)# dot1x timer server-timeout <i>server-timeout</i>	Configure the time of the authentication server timeout timer.

8.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show dot1x interface-type interface-list	Show 802.1x configurations on the interface.
2	Switch# show dot1x interface-type interface-list statistics	Show 802.1x statistics on the interface.
3	Switch# show dot1x interface-type interface-list user	Show user information of 802.1x authentication on the interface.

8.7.8 Maintenance

Maintain the SWITCH as below.

Command	Description
switch(config)# clear dot1x interface-type interface-list statistics	Clear interface 802.1x statistics.

8.8 IP Source Guard

8.8.1 Introduction

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard binding entry

IP Source Guard is used to match the packets characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to combine with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entry, IP Source Guard can be divided into static binding and dynamic binding:

- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.

- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

Principle of IP Source Guard

The principle of IP Source Guard is to build an IP source binding table within the SWITCH. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 8-3 shows the principle of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

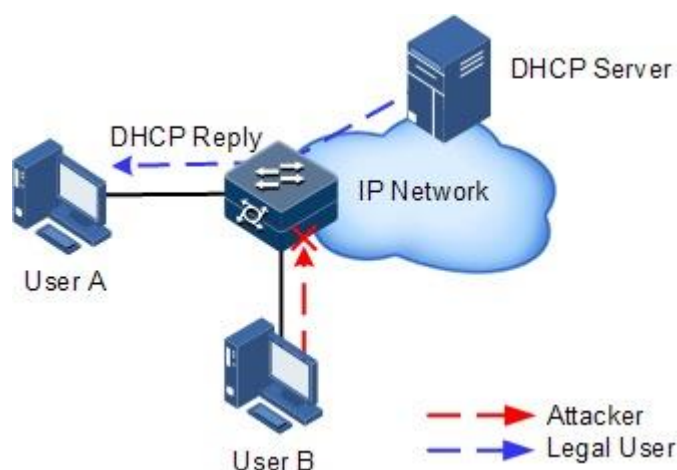


Figure 8-3 Principle of IP Source Guard

Before forwarding IP packets, the SWITCH compares the source IP address, source MAC address, interface number, and VLAN ID of the IP packets with binding table information. If the information matches, it indicates that it is a legal user and the packets are permitted to forward normally. Otherwise, it is an attacker and the IP packets are discarded.

8.8.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker forges legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This makes the legitimate users cannot get network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping before if there is a DHCP user.

8.8.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

8.8.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# in terface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# ip verify source trust	(Optional) configure the interface to a trusted interface. Use no ip verify source trust to configure the interface to an untrusted interface. In this case, all packets, but for DHCP packets and IP packets that meet binding, are not be forwarded. When the interface is in trusted status, all packets are forwarded normally.

8.8.5 Configuring IP Source Guide binding

Configuring IP Source Guide static binding

Configure IP Source Guide static binding for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip verify source	Enable IP Source Guide static binding.
3	Switch(config)# ip source binding <i>ip-address [mac-address]</i> <i>[vlan vlan-id] interface-type</i> <i>interface-number</i>	Configure static binding.



Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled can the static binding take effect.
- For an identical IP address, the manually configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guide dynamic binding

Configure IP Source Guide dynamic binding for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip verify source dhcp-snooping	Enable IP Source Guide dynamic binding.



Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IP address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

Configuring binding translation

Configure binding translation for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ip verify source dhcp-snooping	Enable IP Source Guide dynamic binding.
3	Switch(config)# ip source binding dhcp-snooping static	Translate the dynamic binding to the static binding.
4	Switch(config)# ip source binding auto-update	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

8.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ip verify source	Show global binding status and interface trusted status.
2	Switch# show ip source binding [<i>interface-type interface-number</i>]	Show configurations of IP Source Guard binding, interface trusted status, and binding table.

8.9 PPPoE+

8.9.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

With PPPoE dial-up mode, you can access the network through various interfaces of the device only when one authentication is successfully. However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication server cannot match with the configured one, authentication will fail. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

The PPPoE protocol adopts C/S mode, as shown in Figure 8-4. The Switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

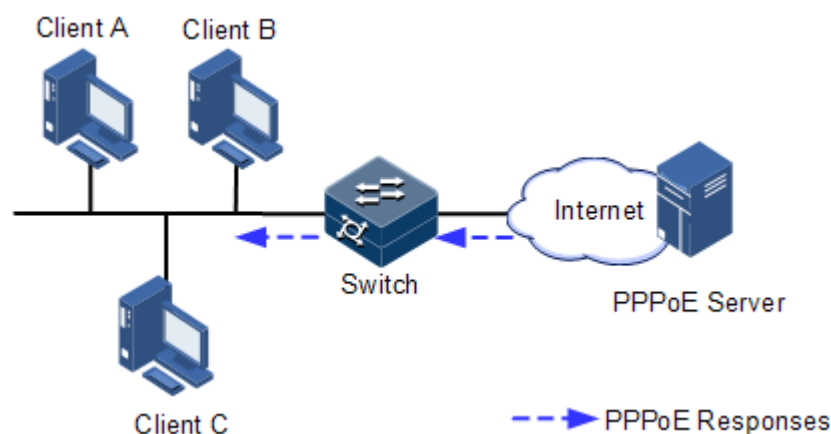


Figure 8-4 Accessing the network through PPPoE authentication

To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

- Step 2 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.
- Step 3 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- Step 4 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.
- Step 5 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

8.9.2 Preparing for configurations

Scenario

To prevent illegal client access during PPPoE authentication, you need to configure PPPoE+ to add additional user identification information in PPPoE packet for network security.

Because the added user identification information is related to the specified switch and interface, the authentication server can bind the user with the switch and interface to effectively prevent account sharing and theft. In addition, this helps users enhance network security.

Prerequisite

N/A

8.9.3 Default configurations of PPPoE+

Default configurations of I PPPoE+ are as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable



Note

By default, PPPoE packet is forwarded without being attached any information.

8.9.4 Configuring basic functions of PPPoE+



Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. Generally, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive. An interface is either enabled with PPPoE+ or is a trusted interface.

Enabling PPPoE+

After global PPPoE+ and interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# pppoeagent enable	Enable global PPPoE+.
3	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Switch(config- gigaethernet1/1/1)# pppoeagent enable	Enable interface PPPoE+.

Configuring PPPoE trusted interface

The PPPoE trusted interface can be used to prevent PPPoE server from being cheated and avoid security problems because PPPoE packets are forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is set to the trusted interface. PPPoE packets from the PPPoE client to the PPPoE server are forwarded by the trusted interface only. In addition, only PPPoE received from the trusted interface can be forwarded to the PPPoE client.

Configure the PPPoE trusted interface for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Switch(config-gigaehternet1/1/1)#pppoeagent trust	Configure the PPPoE trusted interface.



Note

Because PPPoE+ is designed for the PPPoE client instead of the PPPoE server, downlink interfaces of the device cannot receive the PADO and PADS packets. It means that interfaces, where PPPoE+ is enabled, should not receive PADO and PADS packet. If there interfaces receive these packets, it indicates that there are error packets and the packets should be discarded. However, these interfaces can forward PADO and PADS packets of trusted packet. In addition, PADI and PADR packets are forwarded to the trusted interface only.

8.9.5 Configuring PPPoE+ packet information

PPPoE is used to process a specified Tag in the PPPoE packet. This Tag contains Circuit ID and Remote ID.

- Circuit ID: is padded with the VLAN ID, interface number, and host name of request packets at the RX client.
- Remote ID: is padded with the MAC address of the client or the switch.

Configuring Circuit ID

The Circuit ID has 2 padding modes: Switch mode and ONU mode. By default, Switch mode is adopted. In ONU mode, the Circuit ID has a fixed format. The following commands are used to configure the padding contents of the Circuit ID in Switch mode.

In switch mode, the Circuit ID supports 2 padding modes:

- Default mode: when customized Circuit ID is not configured, the padding content is the VLAN ID, interface number, or the attached string. If the attached string is not defined, it is set to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit IS string.

Configure Circuit ID for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#pppoeagent circuit-id mode { onu switch }	Configure the padding mode of the Circuit ID.
3	Switch(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Switch(config-gigaehternet1/1/1)#pppoeagent circuit-id string	(Optional) set the Circuit ID to the customized string.

In default mode, the Circuit ID contains an attached string. By default, the attached string is set to the hostname of the switch. You can set it to a customized string.

Configure the attached string of the Circuit ID for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)# pppoeagent circuit-id attach-string string	(Optional) configure the attached string of the Circuit ID. If the Circuit ID is in default mode, attached string configured by this command will be added to the Circuit ID.

Configuring Remote ID

The Remote ID is padded with a MAC address of the switch or a client. In addition, you can specify the form (binary/ASCII) of the MAC address.

Configure the Remote ID for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#interface interface-type interface- number	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)#pppoeagent remote-id { client-mac switch-mac }	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	Switch(config- gigaethernet1/1/1)#pppoeagent remote-id format { ascii binary }	(Optional) configure the padding modes of the PPPoE+ Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if the PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#interface interface- type interface-number	Enter physical layer interface configuration mode.

Step	Command	Description
3	Switch(config-gigaetherne1/1/1)# pppoeagent vendor-specific-tag overwrite enable	Enable Tag overriding.

8.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show pppoeagent [<i>interface-type interface-list</i>]	Show PPPoE+ configurations.
2	Switch# show pppoeagent statistic [<i>interface-type interface-list</i>]	Show PPPoE+ statistics.

8.9.7 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear pppoeagent statistic	Clear PPPoE+ statistics.

9 Reliability

This chapter describes basic principle and configuration of reliability and provides related configuration examples.

- Link aggregation
- Interface backup
- Configuring ELPS
- Failover

9.1 Link aggregation

9.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. The link aggregation helps share traffics among members in an LAG. Besides effectively improving reliability on links between devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads.

- Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. LACP communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). In addition, you should manually configure the LAG. After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its system LACP protocol priority, system MAC address, interface LACP priority, interface number, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received by other interfaces to select a selected interface. Therefore, the interface and the peer are in the same Selected state. The operation key is a configuration combination automatically

generated based on configurations of the interface, such as the speed, duplex mode, and Up/Down status. In a LAG, interfaces in the Selected state share the identical operation key.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the LAG and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical.

In manual aggregation mode, all member interfaces are in forwarding state, sharing loads. In static/dynamic LACP mode, there are backup links.

Link aggregation is the most widely-used and simplest Ethernet reliability technology.

9.1.2 Preparing for configurations

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

Prerequisite

Before configuring link aggregation, you need to configure physical parameters on a port and make the physical layer **Up**.

In the same LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.

- QoS: traffic policing, rate limit, SP queue, WRR queue scheduling, interface priority and interface trust mode
- QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs
- VLAN: the allowed VLAN, default VLAN and the link type (Trunk or Access) on the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carry Tag
- Port properties: whether the interface is added to the isolation group, interface rate, duplex mode, and link Up/Down status
- MAC address learning: whether enabling the MAC address learning function, whether a limit is configured for the maximum value of learned MAC address

9.1.3 Configuring manual link aggregation

Configure manual link aggregation for the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#interface port-channel channel-number</code>	Enter LAG configuration mode.
3	<code>Switch(config-gigaethernet1/1/1-channel1)#mode manual</code>	Configure manual link aggregation mode.

Step	Command	Description
4	Switch(config-gigaetherne1/1/1-channel1)# max-active min-active } links value threshold	(Optional) configure the maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum number is 1.
5	Switch(config-gigaetherne1/1/1-channel1)# load-sharing mode { dip dmac smac sip sxordip sxordmac }	(Optional) configure a load balancing mode for link aggregation. By default, the load balancing algorithm is set to sxordmac . In this mode, select a forwarding interface based on the OR result of the source and destination MAC addresses.
6	Switch(config-gigaetherne1/1/1-channel1)# exit	Return to global configuration mode.

9.1.4 Configuring static LACP link aggregation

Configure static LACP link aggregation for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# lacp system-priority system-priority	(Optional) configure system LACP priority. The higher priority end is active end. LACP chooses active and backup interfaces according to the active end configuration. The smaller the number is, the higher the priority is. The smaller system MAC address device will be chosen as active end if devices system LACP priorities are identical. By default, system LACP priority is 32768.
3	Switch(config)# lacp timeout { fast slow }	(Optional) configure LACP timeout mode. By default, it is slow.
4	Switch(config)# interface port-channel channel-number	Enter LAG configuration mode.
5	Switch(config-gigaetherne1/1/1-channel1)# mode lacp	Configure the working mode of the LAG to static LACP LAG.
6	Switch(config-gigaetherne1/1/1-channel1)# max-active min-active } links value threshold	(Optional) configure maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum number is 1.
7	Switch(config-gigaetherne1/1/1-channel1)# exit	Return to global configuration mode.

Step	Command	Description
8	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter Layer 2 or 3 physical interface configuration mode.
9	Switch(config-gigaethernet1/1/1)# portswitch	Switch the interface from Layer 3 physical interface configuration mode to Layer 2 physical interface configuration mode.
10	Switch(config-gigaethernet1/1/1)# port-channel <i>channel-number</i>	Add the physical interface to the LAG.
11	Switch(config-gigaethernet1/1/1-channel1)# lACP mode { active passive }	(Optional) configure LACP mode for member interface. LACP connection will fail when both ends of a link are in passive mode. By default, it is in active mode.
12	Switch(config-gigaethernet1/1/1-channel1)# lACP port-priority <i>port-priority</i>	(Optional) configure interface LACP priority. The priority influences election for the default interface for LACP. The smaller the value is, the higher the priority is. By default, it is 32768.
13	Switch(config-gigaethernet1/1/1-channel1)# exit	Return to global configuration mode.



Note


- The system chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.
- In a static LACP LAG, a member interface can be an active/standby one. Both the active interface and standby interface can receive and send LACPDU. However, the standby interface cannot forward user packets.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface port-channel <i>channel-number</i>	Enter LAG configuration mode.
3	Switch(config-gigaethernet1/1/1-channel1)# mode manual backup	Configure the working mode of the LAG to manual backup LAG.
4	Switch(config-gigaethernet1/1/1-channel1)# master-port <i>interface-type interface-number</i>	(Optional) configure the active interface of the LAG.

Step	Command	Description
5	Switch(config-gigaetherne1/1/1-channel1)# restore-mode { non-revertive revertive [restore-delay <i>second</i>] }	Configure the restoration mode and wait-to-restore time of the LAG. By default, the restoration mode is non-revertive.
6	Switch(config-gigaetherne1/1/1-channel1)# exit	Return to global configuration mode.
7	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
8	Switch(config-gigaetherne1/1/1)# port-channel <i>channel-number</i>	Add member interfaces to the LAG.
9	Switch(config-gigaetherne1/1/1)# exit	Return to global configuration mode.

9.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show lacp internal	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	Switch# show lacp neighbor	Show information about LACP neighbors, including tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	Switch# show lacp statistics	Show statistics of interface LACP, including the total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, and the number of errored Marker Response packets,
4	Switch# show lacp sys-id	Show global LACP status of the local system, device ID, including system LACP priority and system MAC address.
5	Switch# show port-channel	Show link aggregation status of the current system, load sharing mode of link aggregation, all LAG member interfaces, and active member interfaces.  Note The active member interface refers to those whose interface status is Up.

9.2 Interface backup

9.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, but it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the Carrier-grade network core.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection links. It ensures performance and simplifies configurations.

Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

Principle

Interface backup is realized by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Up status, the other interface is in Standby status. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

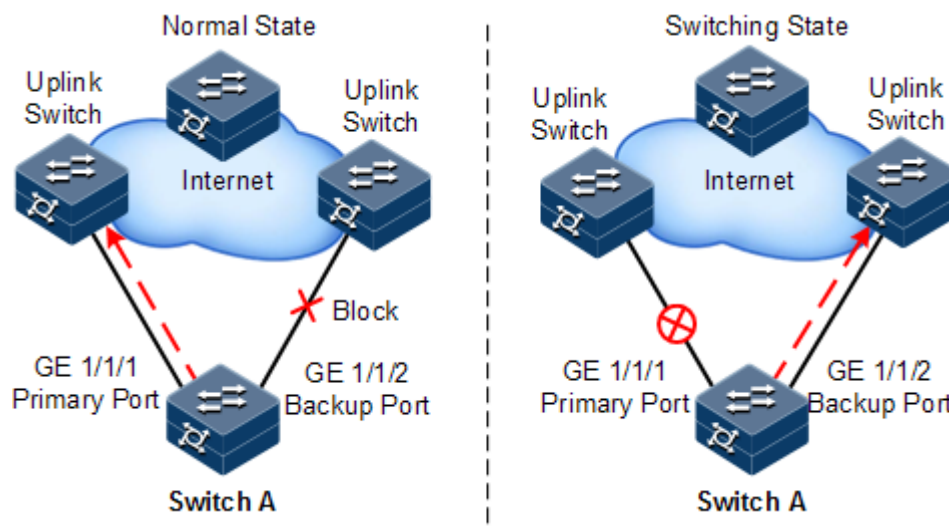


Figure 9-1 Principles of interface backup

As shown in Figure 9-1, Gigaethernet 1/1/1 and Gigaethernet 1/1/2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, Gigaethernet 1/1/1 is the primary interface while Gigaethernet 1/1/2 is the backup interface. Gigaethernet 1/1/1 and the uplink device forward packet while Gigaethernet 1/1/2 and the uplink device do not forward packets.
- When the link between Gigaethernet 1/1/1 and its uplink device fails, the backup Gigaethernet 1/1/2 and its uplink device forward packets.
- When Gigaethernet 1/1/1 restores normally and keeps Up for a period (restore-delay), Gigaethernet 1/1/1 restores to forward packets and Gigaethernet 1/1/2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NMS.

Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 9-2.

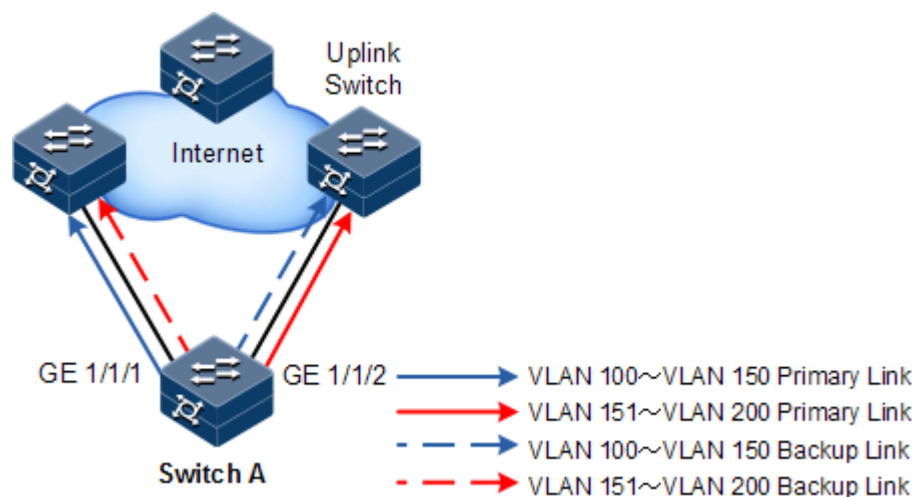


Figure 9-2 Networking with interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, Gigaethernet 1/1/1 is the primary interface and Gigaethernet 1/1/2 is the backup interface.
- In VLANs 151–200, Gigaethernet 1/1/2 is the primary interface and Gigaethernet 1/1/1 is the backup interface.
- Gigaethernet 1/1/1 forwards traffic of VLANs 100–150, and Gigaethernet 1/1/2 forwards traffic of VLANs 151–200.
- When Gigaethernet 1/1/1 fails, Gigaethernet 1/1/2 forwards traffic of VLANs 100–200.
- When Gigaethernet 1/1/1 restores normally and keeps Up for a period (restore-delay), Gigaethernet 1/1/1 forwards traffic of VLANs 100–150, and Gigaethernet 1/1/2 forwards VLANs 151–200.

Interface backup is used share service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

9.2.2 Preparing for configurations

Scenario

By configuring interface backup in a dual uplink network, you can realize redundancy backup and fast switching of the primary/backup link, and load sharing between different interfaces.

Compared with STP, interface backup not only ensures millisecond-level switching, also simplifies configurations.

Prerequisite

N/A

9.2.3 Default configurations of interface backup

Default configurations of interface backup are as below.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Interface connection mode (port-up)

9.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the SWITCH as below.



Caution

Interface backup and STP, loop detection, Ethernet ring, or G.8032 may interfere with each other. Configuring both of them on an interface is not recommended.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type primary-</i> <i>interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Switch(config- gigaethernet1/1/1)# switch port backup <i>interface-</i> <i>type backup-interface-</i> <i>number vlanlist vlan-list</i>	Configure the interface backup group. In the VLAN list, set the interface <i>backup-interface-number</i> to the backup interface and set the interface <i>primary-interface-number</i> to the primary interface.
	Switch(config- gigaethernet1/1/1)# switch port backup <i>interface-</i> <i>type backup-interface-</i> <i>number [vlanlist vlan-</i> <i>list]</i>	If no VLAN list is specified, the VLAN ranges from 1 to 4094.

Step	Command	Description
4	Switch(config-gigabitEthernet1/1/1)# exit	Return to global configuration mode.
	Switch(config-gigabitEthernet1/1/1-channel1)# exit	
5	Switch(config)# switchport backup restore-delay <i>period</i>	(Optional) configure the restore-delay period.
6	Switch(config)# switchport backup restore-mode { disable port-up }	(Optional) configure restoration mode.



Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a LAG cannot be a member of two interface backup groups simultaneously.

9.2.5 (Optional) configuring FS on interfaces



Caution

- After FS is successfully configured, the primary/backup link will be switched; namely, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface).
- In the FS command, the backup interface number is optional. If different VLANs of the primary interface are configured with multiple interface backup groups, you should input the backup interface ID.

Configure FS on interfaces for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type primary-interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Switch(config-gigabitEthernet1/1/1)# switchport backup [<i>interface-type backup-interface-number</i>] force-switch	Configure FS on the interface. Use the no switchport backup [<i>interface-type backup-interface-number</i>] force-switch command to

Step	Command	Description
	Switch(config-gigaethernet1/1/1-channel1)# switchport backup [<i>interface-type backup-interface-number</i>] force-switch	cancel FS. Then, the principles of selecting the current link according to link status are as below: <ul style="list-style-type: none"> • If the Up/Down statuses of the two interfaces are the same, the primary interface is of high priority. • If the Up/Down statuses of the two interfaces are different, the Up interface is of high priority.

9.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show switchport backup	Show related status information of interface backup.

9.3 Configuring ELPS

9.3.1 Preparing for configurations

Scenario

To make the Ethernet reliability up to Telecom-grade (network self-heal time less than 50ms), you can deploy ELPS at Ethernet. ELPS is used to protect the Ethernet connection. It is an end-to-end protection technology.



ELPS provides 3 modes to detect a fault.

- Detect faults based on the physical interface status: learning link fault quickly and switching services immediately, suitable for detecting the fault between neighbor devices.
- Detect faults based on CC: suitable for unidirectional detection or multi-device crossing detection.
- Detect faults based on the physical interface status and CC.

Prerequisite

- Connect interfaces and configure physical parameters for them. Make the physical layer **Up**.
- Create the management VLAN, the VLAN for the working interface, and the VLAN for the protection interface
- Configure CFM detection and form a neighbor relationship (preparing for CC mode).

9.3.2 Creating protection pair

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet line-protection line-id working { <i>interface-type interface-number</i> port-channel channel-number } vlan-list protection interface-type interface-number vlan-list one-to-one [non-revertive] [protocol-vlan vlan-id]	<p>Create the ELPS protection pair and configure the protection mode.</p> <p>The protection group is in non-revertive mode if you configure the non-revertive parameter.</p> <ul style="list-style-type: none"> • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line.
3	Switch(config)# ethernet line-protection line-id name <i>string</i>	(Optional) configure a name for the ELPS protection pair.
4	Switch(config)# ethernet line-protection line-id wtr-timer <i>wtr-timer</i>	<p>(Optional) configure the WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out.</p> <p>By default the WTR time value is set to 5min.</p> <p> Note</p> <p>We recommend that WTR timer configurations on both ends keep consistent. Otherwise, we cannot ensure 50ms quick switching.</p>
5	Switch(config)# ethernet line-protection line-id hold-off-timer <i>holdoff-timer</i>	<p>(Optional) configure the HOLDOFF timer. Keep configurations on both ends consistent.</p> <p>By default, the HOLDOFF timer value is 0.</p> <p> Note</p> <p>If the HOLDOFF timer value is over great, it may influence 50ms switching performance. Therefore, we recommend setting the HOLDOFF timer value to 0.</p>
6	Switch(config)# ethernet line-protection trap enable	<p>(Optional) enable ELPS Trap to be reported to the NMS.</p> <p>By default, it is disabled.</p>

9.3.3 Configuring ELPS fault detection modes

Choose one mode in Step 2 to configure the SWITCH as required.

 **Note**

- Fault detection modes of the working line and protection line can be different. However, we recommend that fault detection mode configurations of the working line and protection line keep consistent.

- To configure the end-to-end fault detection mode in the working or protection line with crossing other devices, we do not recommend physical link detection but CC detection.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet line-protection line-id { working protection } failure-detect physical-link	Configure the fault detection mode of the working line/protection line to failure-detect physical-link . By default, it is failure-detect physical-link .
	Switch(config)# ethernet line-protection line-id { working protection } failure-detect cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id	Configure the fault detection mode of the working line/protection line to failure-detect cc . This fault detection mode cannot take effect unless you finish related configurations on CFM.
	Switch(config)# ethernet line-protection line-id { working protection } failure-detect physical-link-or-cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id	Configure the fault detection mode of the working line/protection line to failure-detect physical-link-or-cc . In this mode, it believes that the link fails when a fault is detected on the physical link/CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.

9.3.4 (Optional) configuring ELPS switching control



Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ELPS switching control in some special cases.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet line-protection line-id lockout	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails.
3	Switch(config)# ethernet line-protection line-id force-switch	Switch the traffic from the working line to the protection line forcedly.
4	Switch(config)# ethernet line-protection line-id manual-switch	Switch the traffic from the working line to the protection line manually. Its priority is lower than the one of forced switch and APS.
5	Switch(config)# ethernet line-protection line-id manual-switch-to-work	In non-revertive mode, switch the traffic from the protection line to the working line.



Caution

After you execute a protection group command, if a fault/recovery event occurs or if other protection group commands, such as lockout, force-switch, and manual-switch, both ends of the protection group may select different lines. In this case, you should use the **clear ethernet line-protection *line-id* end-to-end command** command to delete the configured protection group command to make both ends of the protection group select the identical line.

9.3.5 Checking configurations

No.	Command	Description
1	Switch# show ethernet line-protection [<i>line-id</i>]	Show configurations of the protection pair.
2	Switch# show ethernet line-protection statistics	Show statistics of the protection pair.
3	Switch# show ethernet line-protection aps	Show APS information about the protection pair.

9.4 Failover

9.4.1 Introduction

Failover is used to provide port linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a failover group. Therefore, faults of uplink devices can be informed to the downlink devices to trigger switching. Failover can be used to prevent traffic loss due to uplink failure.

Once all uplink interfaces fail, down link interfaces are in Down status. When at least one uplink interface recovers, downlink interface recovers to Up status. Therefore, faults of uplink devices can be informed to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

9.4.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot switch to the standby link if it cannot notify downlink devices in time, and then traffic will be broken.

Failover can be used to add downlink interfaces and uplink interfaces of the middle device to a failover group and monitor uplink interfaces. When all uplink interfaces fails, faults of uplink devices can be informed to the downlink devices to trigger switching.

Prerequisite

N/A

9.4.3 Default configurations of failover

Default configurations of failover are as below.

Function	Default value
Failover group	N/A

9.4.4 Configuring failover



Note

Failover supports being configured on the physical interface and LAG interface.

Configure failover for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# link-state-tracking group <i>group-number</i>	Create the failover group and enable failover.
3	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Switch(config-gigaethernet1/1/1)# link-state-tracking group <i>group-number</i> { downstream upstream }	Configure the failover group of the interface and interface type. One uplink interface can belong to only one failover group. The downlink interface is free of this limit.
5	Switch(config) link-state-tracking group <i>group-number</i> trap { enable disable }	Enable/Disable Trap sending.
6	Switch(config) link-state-tracking group <i>group-number</i> action modify-pvid <i>pvid interface-type interface-number</i>	Configure the action taken for clearing the fault to modifying the interface PVID.
7	Switch(config) link-state-tracking group <i>group-number</i> action { delete-vlan suspend-vlan } <i>vlan-id</i>	Configure the action taken for clearing the fault to deleting and suspending the VLAN.
8	Switch(config) link-state-tracking group <i>group-number</i> action block-vlan <i>vlan-id interface-type interface-number</i>	Configure the action taken for clearing the fault to blocking the interface VLAN.

**Note**

- One failover group can contain several uplink interfaces. Failover will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, failover occurs.
- In global configuration mode, use the **no link-state-tracking group *group-number*** command to disable failover. The faulty source and fault action will be deleted. The failover group does not exist.
- In global configuration mode, use the **no link-state-tracking group *group-number* action** command to delete the action for the failover group.

9.4.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Switch# show link-state-tracking group <i>group-number</i>	Show configurations and status of the failover group.

10 OAM

This chapter describes principles and configuration procedures of OAM, as well as related configuration examples, including following sections:

- Introduction
- Configuring EFM
- E-LMI

10.1 Introduction

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak because of its small size and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in Telecom network becomes wider and wider. Compared with LAN, the link length and network size of Telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the Telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm, and locate faults on network, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

10.1.1 EFM

Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification, etc. for a link between two directly connected devices. EFM is mainly used for Ethernet links on edges of the network accessed by users.

OAM mode and OAM discovery

The Ethernet OAM connection process is the OAM discovery phase, where an OAM entity discovers a remote OAM entity and establishes a session with it.

In the discovery phase, a connected Ethernet OAM entity (interface enabled with OAM) informs others of its Ethernet OAM configurations and Ethernet OAM capabilities supported by the local node by exchanging information OAM PDU. After the OAM entity receives

parameters of the peer, it decides whether to establish OAM connection. If both ends agree on establishment of the OAM connection, Ethernet OAM protocol will work on the link layer.

The SWITCH can choose one of the following 2 modes to establish Ethernet OAM connection:

- Active mode
- Passive mode

Only the OAM entity in active mode can initiate OAM connection while the OAM entity in passive mode just waits for connection request of the active OAM entity.

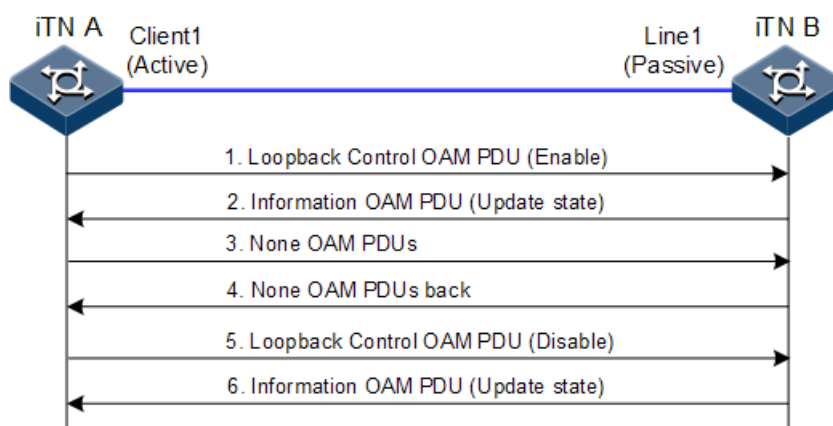
After the OAM connection is established, both ends keep connected by exchanging information OAM PDU. If an OAM entity does not receive information OAM PDU within 5s, it believes that connection expires and connection re-establishment is required.

OAM loopback

OAM loopback occurs only after the Ethernet OAM connection is established. When connected, the active OAM entity initiates OAM loopback command, and the peer OAM entity responds to the command.

When the remote OAM entity is in loopback mode, all packets but OAM PDU packets are sent back. By observing the returned PAMPDU packets, the network administrator can judge the link performance (including packet loss ratio, delay, and jitter).

Figure 10-1 OAM loopback



As shown in Figure 10-1, Port 1 on iTN A works in active mode. After the 802.3ah OAM connection between iTN A and iTN B is established, enable remote loopback on Client 1.

The process for OAM loopback is as below:

- Step 1 iTN A sends a Loopback Control OAM PDU packet with the Enable information to iTN B, and waits for response.
- Step 2 After receiving the Loopback Control OAM PDU packet with the Enable information, iTN B replies the Information OAM PDU packet to iTN A, and enters the loopback state.
- Step 3 After receiving the response, iTN A sends a non-OAM PDU test packet to iTN B.
- Step 4 After receiving a non-OAM PDU test packet, iTN B sends it back to iTN A.

Stop OAM loopback as below:

- Step 5 If iTN A needs to stop remote loopback, it sends a Loopback Control OAM PDU packet with the Disable information to iTN B.
- Step 6 After receiving the Loopback Control OAM PDU packet with the Disable information, iTN B exits loopback state and sends an Information OAM PDU packet to iTN A.

You can troubleshoot the fault through loop detection in different phases.

OAM events

It is difficult to detect Ethernet failures, especially when the physical communication works properly while the network performance deteriorates slowly. A flag is defined in OAM PDU packet to allow an OAM entity to transmit fault information to the peer. The flag may stand for the following threshold events:

- Link fault: signals from the peer are lost.
- Dying gasp: an unpredictable event occurs, such as power failure.
- Critical event: an uncertain critical event occurs.

In the OAM connection, an OAM entity keeps sending Information OAM PDUs. The local OAM entity can inform the peer OAM entity of threshold events through Information OAM PDUs. In this way, the network administrator can learn the link state and take actions accordingly.

The network administrator monitors Ethernet OAM through the Event Notification OAM PDU. When a link fails, the passive OAM entity detects the failure, and actively sends Event Notification OAM PDU to the peer active OAM entity to inform the following threshold events. Therefore, the network administrator can dynamically master the network status through the link monitoring process.

- Error frame event: the number of error frames exceeds the threshold in a time unit.
- Error frame period event: the number of error frames exceeds the threshold in a period (specified N frames).
- Error frame second event: the number of error frames in M seconds exceeds the threshold. The second when an errored frame is generated is called the errored frame second.
- Error symbol period event: the number of error symbols received in a period (monitor window) exceeds the threshold.



Note

If an errored frame occurs in a second, the second is called the errored frame second.

Acquiring OAM MIB

The SWITCH learns the status and parameters of the peer link by acquiring link configurations/statistics of the peer through OAM.

10.1.2 CFM

To extend the application of Ethernet technologies in the carrier-grade network, Connectivity Fault Management provides OAM tools for the carrier-grade network and makes the Ethernet reach the same CoS of the carrier-grade transport network.

Connectivity Fault Management (CFM) is a network-level Ethernet OAM technology, providing end-to-end connectivity fault detection, fault notification, fault judgement, and fault

location. It is used to diagnose fault actively for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solution, and improve network maintenance via the fault management function.

The SWITCH provides CFM that is compatible with both ITU-Y.1731 and IEEE 802.1ag standards.

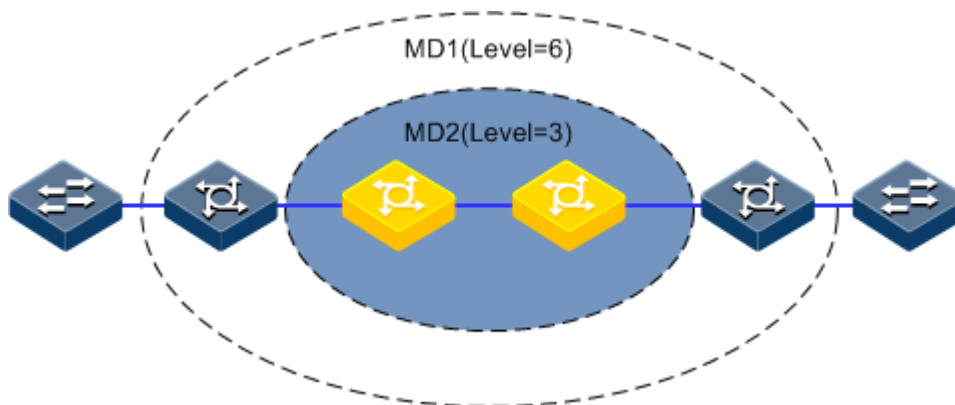
CFM consists of following components:

- MD

Maintenance Domain (MD), also called Maintenance Entity Group (MEG), is a network that runs CFM. It defines network range of OAM management. MD has a level property, with 8 levels (level 0 to level 7). The bigger the number is, the higher the level is and the larger the MD range is. Protocol packets in a lower-level MD will be discarded after entering a higher-level MD. If no Maintenance association End Point (MEP) but a Maintenance association Intermediate Point (MIP) is in a high-level MD, the protocol can traverse the higher-level MD. However, packets in a higher-level MD can traverse lower-level MDs. In the same VLAN range, different MDs can be adjacent, embedded, but not crossed.

As shown in Figure 10-2, MD 2 is in MD 1. Packets in MD 1 need to traverse MD 2. Configure MD 1 to be at level 6, and MD 2 to be at level 3. Then packets in MD 1 can traverse MD 2 and implement connectivity fault management of the whole MD 1. However, packets in MD 2 cannot diffuse into MD 1. MD 2 is a server layer while MD 1 is a client layer.

Figure 10-2 MDs at different levels



- MA

The Maintenance Association (MA) is also called the service instance. It is a part of a MD. One MD can be divided into one or multiple MAs. One MA corresponds to one service and is mapped to a group of VLANs. VLANs of different MAs cannot cross. Though a MA can be mapped to multiple VLANs, one MA can only use a VLAN for sending or receiving OAM packets. This VLAN is the master VLAN of the MA.

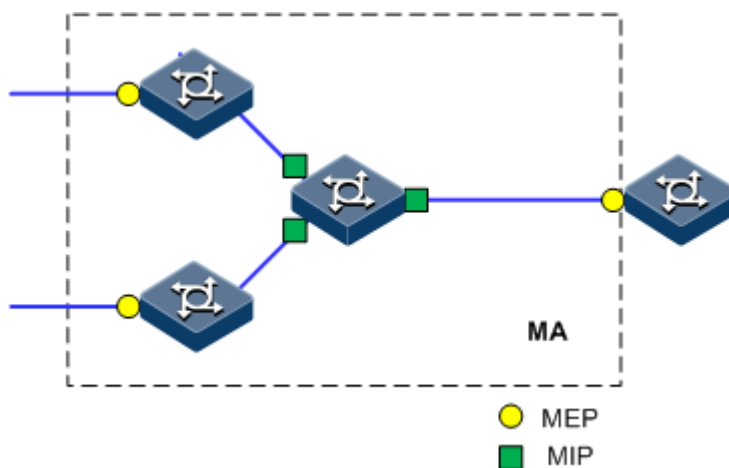
- MEP

As shown in Figure 10-3, the MEP is an edge node of a MA. MEPs can be used to send and process CFM packets. The MA and the MD where the MEP locates decide VLANs and levels of packets received and sent by the MEP.

For any device that runs CFM in the network, the MEP is called local MEP. For MEPs on other devices of the same MA, they are called Remote Maintenance association End Points (RMEP).

Multiple MEPs can be configured in a MA. Packets sent by MEPs in one MA take identical SVLAN TAG, priority, and CVLAN TAG. A MEP can receive OAM packets sent by other MEPs in the same MA, intercept packets which at the same or lower level, and forward packets of higher level.

Figure 10-3 MEP and MIP



- MIP

As shown in Figure 10-3, the MIP is the internal node of a MA, which is automatically created by the device. MIP cannot actively send CFM packets but can process and response to LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are called Maintenance Point (MP).

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)

The function is realized by periodically sending Continuity Check Messages (CCMs). One MEP sends CCM and other MEPs in the same service instance can verify the RMEP status when receiving this packet. If the SWITCH fails or a link is incorrectly configured, MEPs cannot properly receive or process CCMs sent by RMEPs. If no CCM is received by a MEP during 3.5 CCM intervals, it is believed that the link fails. Then a fault Trap will be sent according to configured alarm priority.

- Fault acknowledgement (LoopBack, LB)

This function is used to verify the connectivity between two MPs through the source MEP sending LoopBack Message (LBM) and the destination MP sending LoopBack Reply (LBR). The source MEP sends a LBM to a MP who needs to acknowledge a fault. When receiving the LBM, the MP sends a LBR to the source MEP. If the source MEP receives this LBR, it is believed that the route is reachable. Otherwise, a connectivity fault occurs.

- Fault location (LinkTrace, LT)

The source MEP sends LinkTrace Message (LTM) to the destination MP and all MPs on the LTM transmission route will send a LinkTrace Reply (LTR) to the source MEP. By recording valid LTR and LTM, this function can be used to locate faults.

- Alarm Indication Signal (AIS)

This function is used to inhibit alarms when a fault is detected at the server layer (sub-layer, as shown in Figure 10-2). When detecting a fault, the MEP (including the server MEP) sends an AIS frame to the client MD. By transmitting ETH-AIS frames, the device can inhibit or stop an alarm on MEP (or server MEP).

When receiving an AIS frame, the MEP must inhibit alarms for all peer MEPs regardless of connectivity, because this frame does not include information about MEPs that are at the same level with the failed MEP. With AIS, the device can inhibit the alarm information at client level when the server layer (sub-layer) fails. Therefore, the network is easy for maintenance and management.

- Ethernet lock signal (Lock, LCK)

This function is used to notify managed lock and service interruption of server layer (sub-layer) MEPs. The data traffic is sent to a MEP that expects to receive it. This function helps the MEP that receives ETH-LCK frame to identify a fault. It is a managed lock action for server layer (sub-layer) MEP. Lock is an optional OAM management function. One typical scenario for applying this function is to perform detection when services are interrupted.

In general, CFM is an end-to-end OAM technology at the server layer. It helps reduce operation and maintenance cost. In addition, it improves the competitiveness of service providers.

10.2 Configuring EFM

10.2.1 Preparing for configurations

Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

10.2.2 Configuring basic functions of EFM

Configure basic functions of EFM for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# oam { active passive }	Configure a working mode of EFM. By default, the SWITCH is in passive mode.

Step	Command	Description
4	Switch(config-gigaetherne1/1/1)# oam send-period <i>period-number</i> timeout time	(Optional) Configure the period for sending OAM PDUs and the OAM link timeout. By default, the period is set to 1s (namely, <i>period-number</i> is 10, $10 \times 100\text{ms} = 1\text{s}$), and timeout is 5s.
5	Switch(config-gigaetherne1/1/1)# oam enable	Enable interface OAM. By default, OAM is disabled on the interface.

10.2.3 Configuring EFM active function



Note

The EFM active function can be configured only when the SWITCH is in active mode.

(Optional) enabling EFM remote loop



Note

- Perform loopback detection periodically can discover network fault in time. Loopback detection in network sections can locate exact fault area and help users clear fault.
- In link loopback status, the SWITCH sends back all packets except OAM packets received by the link to the peer device. Disable this function in time if no loopback detection is needed.

Enable EFM remote loop for the SWITCHSWITCH (R) as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interfac e interface-type <i>interface-number</i>	Enter physical interface configuration mode.
3	Switch(config-gigaetherne1/1/1)# oam remote-loopback	Configure the interface to start EFM remote loopback.
4	Switch(config-gigaetherne1/1/1)# oam loopback timeout time	(Optional) Configure the timeout for remote loopback on the physical interface. By default, it is 3s.
5	Switch(config-gigaetherne1/1/1)# oam loopback retry times	(Optional) Configure the retry times for remote loopback on the physical interface. By default, it is 3.

(Optional) showing current variable information about peer device



Note

By obtaining the current variable of the peer, you can learn status of current link. IEEE802.3 Clause 30 defines and explains supported variable and its denotation obtained by OAM in details. The variable takes object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch and leaf description of attributes by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The SWITCH supports obtaining OAM information and interface statistics.

Peer variable cannot be obtained until EFM is connected.

Show current variable information about the peer device for the SWITCH as below.

Step	Command	Description
1	Switch#show oam peer oam-info [<i>interface-type interface-number</i>]	Obtain basic OAM information about the peer device.
	Switch#show oam peer [<i>interface-type interface-number</i>]	

10.2.4 Configuring EFM passive function



Note

The EFM passive function can be configured regardless the SWITCH is in active or passive mode.

(Optional) configuring device to respond with EFM remote loop

Configure the SWITCH to respond with EFM remote loop as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config)# oam loopback { ignore process }	Configure ignore or process EFM remote loopback. By default, the SWITCH responds to EFM remote loopback.

10.2.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring



Note

OAM link monitor is used to detect and report link error in different conditions. When the detection link has a fault, the SWITCH notifies the peer of the error generated time, window and threshold, etc. by OAM event, the peer receives event notification and reports the NMS through SNMP Trap. Besides, the local device can directly report events to the NMS center through SNMP Trap.

By default, the system has default values for error generated time, window and threshold setting.

Configure OAM link monitoring for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaethernet1/1/1)# oam errored-frame window <i>framewindow threshold framethreshold</i>	Configure errored frame monitor window and threshold. By default, the monitor window is 1s, and the threshold is 1 errored frame.
4	Switch(config-gigaethernet1/1/1)# oam errored-frame-period window <i>frameperiodwindow threshold frameperiodthreshold</i>	Configure errored frame period event monitor window and threshold. By default, the monitor window is 1000ms, and the threshold is 1 errored frame.
5	Switch(config-gigaethernet1/1/1)# oam errored-frame-seconds window <i>framesecswindow threshold framesecsthreshold</i>	Configure link errored frame second window and threshold. By default, the monitor window is 60s, and the threshold is 1s.
6	Switch(config-gigaethernet1/1/1)# oam errored-symbol-period window <i>sympriodwindow threshold sympriodthreshold</i>	Configure errored code window and threshold. By default, the monitor window is 1s, and the threshold is 1s.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# interface <i>interface-type interface-</i> <i>number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# oam notify { critical-event dying-gasp errored- frame errored-frame- period errored-frame- seconds errored-symbol- period } enable	Configure the OAM link event notification. By default, OAM link event notification is enabled.
4	Switch(config- gigaethernet1/1/1)# oam event trap enable	Enable local OAM event Trap to report link monitoring events to the NMS immediately. By default, local OAM event Trap is disabled.
5	Switch(config- gigaethernet1/1/1)# oam peer event trap { enable disable }	Enable peer OAM event Trap to report link monitoring events to the NMS immediately. By default, peer OAM event Trap is disabled.

10.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show oam [<i>interface-type</i> <i>interface-number</i>]	Show basic configurations of EFM.
2	Switch# show oam event [<i>interface-type interface-</i> <i>number</i>] [critical]	Show local OAM link events.
3	Switch# show oam loopback [<i>interface-type interface-</i> <i>number</i>]	Show configurations of OAM remote loopback.
4	Switch# show oam notify [<i>interface-type interface-</i> <i>number</i>]	Show configurations of OAM event notification.
5	Switch# show oam peer event [<i>interface-type interface-</i> <i>number</i>] [critical]	Show configurations of OAM peer events.
6	Switch# show oam peer link- statistic [<i>interface-type</i> <i>interface-number</i>]	Show statistics of peer OAM links.
7	Switch# show oam statistics [<i>interface-type interface-</i> <i>number</i>]	Show OAM statistics.
8	Switch# show oam trap [<i>interface-</i> <i>type interface-number</i>]	Show OAM Trap.

10.3 E-LMI

10.3.1 Introduction

Metro Ethernet Forum (MEF) defines the Ethernet Local Management Interface (E-LMI) based on Frame Relay Local Management Interface (FR-LMI). The E-LMI, an OAM protocol targeted for the User Network Interface (UNI), works between the Customer Edge (CE) and the Provider Edge (PE).

The E-LMI makes the SP automatically configure the CE according to services purchased by the user. Through the E-LMI, the CE can automatically receive the information on mappings between the customer VLAN and Ethernet Virtual Connection (EVC), and configurations of the bandwidth and Quality of Service (QoS). The auto-configuration function of the E-LMI CE not only reduces service establishment, also reduces coordination between the SP and enterprise users. Enterprise users do not have to learn how to configure CE devices which are configured and managed uniformly by the SP, thus reducing misoperation risks.

In addition, the E-LMI provides EVC status for CE devices. If an EVC fault is detected (for example, CFM is used to detect faults on EVC at the PE side), the PE informs the CE of the fault in time so that the CE can switch access routes quickly.

Figure 10-4 shows the location of E-LMI on the network.

Figure 10-4 Location of E-LMI on network



10.3.2 Preparing for configurations

Scenario

Through the E-LMI, the PE sends the mappings between the VLAN and EVC to the CE so that the CE implements auto-configuration. This not only reduces service establishment, but also reduces coordination between the SP and enterprise users. Enterprise users do not have to learn how to configure CE devices which are configured and managed uniformly by the SP, thus reducing misoperation risks.

Cooperating with the OAM protocol, the E-LMI provides EVC status for CE devices. If an EVC fault is detected, the PE informs the CE of the fault in time so that the CE can switch access routes quickly.

Prerequisite

- Connect interfaces. Configure physical parameters to make interfaces Up at the physical layer.

- Set the physical interface between of the PE to Trunk mode.
- Configure CFM between PEs.

10.3.3 Default configurations of E-LMI

Default configurations of the E-LMI are as below.


Function	Default value
Global E-LMI status	Enable
Interface E-LMI status	Disable
Working mode of the SWITCH	PE
Status of sending Trap	Disable
Informing mode for EVC messages	asyn
Value of the T391 timer	10s
Value of the T392 timer	15s
Status of the T392 timer	Enable
Value of the T391 counter	360
Value of the N393 counter	4

10.3.4 Configuring E-LMI on PE

Enabling E-LMI


Enable E-LMI for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet lmi enable	Enable the E-LMI globally. Use the ethernet lmi disable command to disable this function.
3	Switch(config)# ethernet lmi trap { enable disable }	(Optional) configure Trap status.
4	Switch(config)# ethernet lmi pe	Configure the SWITCH to the PE.
5	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
6	Switch(config-gigaethernet1/1/1)# ethernet lmi enable	(Optional) enable the E-LMI on the interface. Use the ethernet lmi disable command to disable this function.

Step	Command	Description
7	Switch(config-gigaetherne1/1/1)# ethernet lmi t392 enable	(Optional) enable the T392 timer of the E-LMI on the interface. Use the ethernet lmi t392 disable command to disable this function.
8	Switch(config-gigaetherne1/1/1)# ethernet lmi t392 value	(Optional) configure the value of the T392 timer.  Note The value of the T392 timer must be greater than the value of the T391 timer configured for the CE.
9	Switch(config-gigaetherne1/1/1)# ethernet lmi n393 value	(Optional) configure the value of the N393 counter for the PE.

Configuring EVC



Configure the EVC as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet lmi evc evc-number evc-name	Create an EVC, and enter EVC configuration mode.
3	Switch(config- evc)# oam-protocol cfm svlan vlan-id level level	Configure the bundling between the EVC and CFM. The CFM service instance to be bundled must exist, and the MEP is in Up direction.
4	Switch(config- evc)# uni count number	Configure the number of UNIs to be bundled with the EVC. The UNIs bundled with the EVC contain local UNIs and remote UNIs. <ul style="list-style-type: none"> • If the number is set to 2, the EVC is point to point. • If the number is set to 3 or larger, the EVC is point to multipoint.  Note The number of configured UNIs must equal to the number of MEPs bundled with CFM. <ul style="list-style-type: none"> • If the former is greater than the later, and all UNIs are Up, these UNIs are in partially active status. • If the former is smaller than the later and partial UNIs are Down, the UNIs are in active status.

Configuring UNI

Configure the UNI for the SWITCH as below.


Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config-gigaetherne t1/1/1) # ethernet lmi uni <i>uni-id</i>	Create a UNI. You can create only one UNI on each interface, and the <i>uni-id</i> should be globally unique.
4	Switch(config-gigaetherne t1/1/1) # ethernet lmi uni { bundling all-to-one-bundling service-multiplexing }	Configure the bundling type of the UNI. <ul style="list-style-type: none"> • bundling: the UNI can be bundled with one or more EVCs, and one or more CE-VLAN can be mapped to an EVC. • all-to-one-bundling: a UNI can be bundled with only one EVC and all CE-VLANs will be mapped to the EVC. • service-multiplexing: a UNI can be bundled to one or more EVCs but each EVC is mapped to a CE-VLANs.
5	Switch(config-gigaetherne t1/1/1) # ethernet lmi evc <i>evc-number</i>	Configure the bundling between the UNI and the EVC.
6	Switch(config-gigaetherne t1/1/1) # ethernet lmi ce-vlan map { <i>vlan-list</i> untagged all } evc <i>evc-number</i>	Configure the mapping between the EVC and CE-VLAN. If the mapping type of the UNI is all-to-one-bundling , all CE-VLANs will be mapped to the bundled EVCs. In this case, you do not need to configure this command.

Step	Command	Description
7	Switch(config-gigaetherne1/1/1) #ethernet lmi default-<i>evc-number</i>	<p>(Optional) set an EVC to the default EVC.</p> <p>All untagged CE-VLANs are mapped to the default EVC. For example, after you use the ethernet lmi ce-vlan-map 100-4094 evc evc1 command, VLANs 100–4094 are mapped to EVC 1. Then, set the EVC 2 to the default EVC, so the rest VLANs from VLAN 1 to VLAN 99 and untagged VLAN will be mapped to EVC 2.</p> <p>If you use this command, the system maps all VLANs to the default EVC. Then you cannot use the ethernet lmi ce-vlan-map { <i>vlan-list</i> untagged all } evc <i>evc-number</i> command.</p> <p> Note</p> <p>Only when the bundling type of the UNI is bundling, can you use this command.</p>
8	Switch(config-gigaetherne1/1/1) #ethernet lmi evc-notify { <i>asyn</i> <i>full</i> }	<p>(Optional) configure the notifying mode for EVC message on the PE.</p> <p> Note</p> <ul style="list-style-type: none"> When the notifying mode for EVC packets is <i>asyn</i>, the PE immediately sends messages to upon the change of the EVC. In this way, the CE can update EVCs. When the notifying mode for EVC packets is <i>full</i>, the PE does not inform the CE upon the change of the EVC; instead the PE waits to receive the valid Full Status Enquiry message and then replies with a Full or Full Continuous message.

10.3.5 Configuring E-LMI on CE

Configure the E-LMI on the CE for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# ethernet lmi enable	<p>Enable the E-LMI globally.</p> <p>Use the ethernet emi disable command to disable this function.</p>

Step	Command	Description
3	Switch(config)# ethernet lmi ce	Configure the SWITCH as the CE.  Note When you configure switching of device role, the system prompts that the existing E-LMI configurations will be cleared.
4	Switch(config)# interface <i>interface-type interface-number</i>	(Optional) enter physical layer interface configuration mode or aggregation group configuration mode.
5	Switch(config-gigaethernet1/1/1) #ethernet lmi enable	(Optional) enable the E-LMI on the interface. Use the ethernet lmi disable command to disable this function.
6	Switch(config-gigaethernet1/1/1) #ethernet lmi t391 value	(Optional) configure the value of the T391 timer.
7	Switch(config-gigaethernet1/1/1) #ethernet lmi n391 value	(Optional) configure the value of the T393 counter.
8	Switch(config-gigaethernet1/1/1) #ethernet lmi n393 value	(Optional) configure the value of the T393 counter on the CE.

10.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show ethernet lmi config <i>interface-type interface-number</i>	Show E-LMI configurations on the interface.
2	Switch# show ethernet lmi statistics <i>interface-type interface-number</i>	Show E-LMI statistics on the interface.
3	Switch# show ethernet lmi uni port-list <i>interface-type interface-number</i>	Show UNI configurations.
4	Switch# show ethernet lmi evc <i>evc-number</i>	Show EVC status.
5	Switch# show ethernet lmi evc map <i>interface-type interface-number</i>	Show mappings between the EVC and the CE-VLAN.
6	Switch# show ethernet lmi evc map oam	Show OAM protocol information about EVC mapping.

10.3.7 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear ethernet lmi statistics <i>interface-type interface-number</i>	Clear E-LMI statistics on the interface.

11 System management

This chapter describes basic principle and configuration of system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Cable diagnosis
- Memory monitoring
- Ping
- Traceroute

11.1 SNMP

11.1.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet.

Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Principle of SNMP

SNMP is separated into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets being sent through UDP.

NMS system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be realized through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed in the managed device, realizing the following functions:

- Receive/reply request packets from NMS
- Read/write packets and generate response packets according to the packets type, then return the result to NMS
- Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NMS through agent to report current status of device.



Note

An Agent can be configured with several versions, and different versions communicate with different NMSs. But SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

Protocol versions

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the SWITCH, the packet will be dropped.
- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMP v3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The SWITCH supports v1, v2c, and v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the SWITCH.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The SWITCH supports standard MIB.

11.1.2 Preparing for configurations

Scenario

When you need to log in to the SWITCH through NMS, configure SNMP basic functions for the SWITCH in advance.

Prerequisite

Configure the routing protocol and ensure that the route between the SWITCH and NMS is reachable.

11.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value																								
SNMP view	system and internet views (default)																								
SNMP community	public and private communities (default) <table border="1"> <thead> <tr> <th>Index</th> <th>CommunityName</th> <th>ViewName</th> <th>Permission</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>public</td> <td>internet</td> <td>ro</td> </tr> <tr> <td>2</td> <td>private</td> <td>internet</td> <td>rw</td> </tr> </tbody> </table>	Index	CommunityName	ViewName	Permission	1	public	internet	ro	2	private	internet	rw												
Index	CommunityName	ViewName	Permission																						
1	public	internet	ro																						
2	private	internet	rw																						
SNMP access group	initialnone and initial access groups (default)																								
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)																								
Mapping relationship between SNMP user and access group	<table border="1"> <thead> <tr> <th>Index</th> <th>GroupName</th> <th>UserName</th> <th>SecModel</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>initialnone</td> <td>none</td> <td>usm</td> </tr> <tr> <td>1</td> <td>initial</td> <td>md5priv</td> <td>usm</td> </tr> <tr> <td>2</td> <td>initial</td> <td>shapriv</td> <td>usm</td> </tr> <tr> <td>3</td> <td>initial</td> <td>md5nopriv</td> <td>usm</td> </tr> <tr> <td>4</td> <td>initial</td> <td>shanopriv</td> <td>usm</td> </tr> </tbody> </table>	Index	GroupName	UserName	SecModel	0	initialnone	none	usm	1	initial	md5priv	usm	2	initial	shapriv	usm	3	initial	md5nopriv	usm	4	initial	shanopriv	usm
Index	GroupName	UserName	SecModel																						
0	initialnone	none	usm																						
1	initial	md5priv	usm																						
2	initial	shapriv	usm																						
3	initial	md5nopriv	usm																						
4	initial	shanopriv	usm																						
Trap	Enable																								
SNMP target host address	N/A																								
SNMP engine ID	800022B603001FCE000016																								

11.1.4 Configuring basic functions of SNMP v1/v2c

To protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operating. Otherwise, their requests will not be accepted.

The community name uses different SNMP string to identify different groups. Different communities can have read-only or read-write access authority. Groups with read-only authority can only query the device information, while groups with read-write authority can configure the device and query the device information.

SNMP v1/v2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Configure basic functions of SNMP v1/v2c for the SWITCH as below.

Step	Command	Description
1	<code>Switch#config</code>	Enter global configuration mode.
2	<code>Switch(config)#snmp-server view view-name oid-tree [mask] { excluded included }</code>	(Optional) create SNMP view and configure MIB variable range. The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree.
3	<code>Switch(config)#snmp-server community community-name [view view-name] { ro rw }</code>	Create community name and configure the corresponding view and authority. Use default view internet if view view-name option is empty.

11.1.5 Configuring basic functions of SNMP v3

SNMPV3 uses USM mechanism. USM comes up with the concept of access group. One or more users correspond to one access group. Each access group sets the related read, write, and notification views. Users in an access group have access authorities of this view. The access group of users, who send Get and Set requests, must have authorities corresponding to the requests. Otherwise, the requests will not be accepted.

As shown in Figure 11-1, to access the switch through SNMP v3, you should perform the following configurations:

- Configure users.
- Configure the access group of users.
- Configure the view authority of the access group.
- Create views.

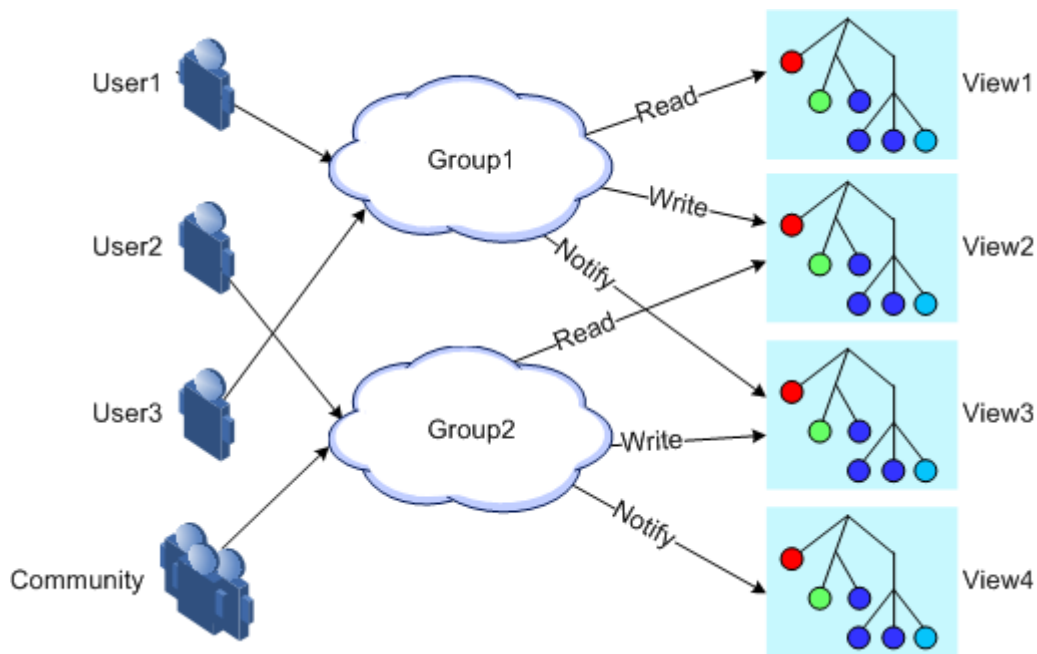


Figure 11-1 SNMP v3 authentication mechanism

Configure basic functions of SNMP v3 for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { excluded included }	(Optional) create SNMP view and configure MIB variable range.
3	Switch(config)# snmp-server user <i>user-name</i> [remote <i>engine-id</i>] authentication { md5 sha } <i>authpassword</i> [privacy <i>privacypassword</i>]	Create users and configure authentication modes.
4	Switch(config)# snmp-server user <i>user-name</i> [remote <i>engine-id</i>] authkey { md5 sha } <i>keyword</i> [privacy <i>privacypassword</i>]	(Optional) modify the authentication key and the encryption key.
5	Switch(config)# snmp-server access <i>group-name</i> [read <i>view-name</i>] [write <i>view-name</i>] [notify <i>view-name</i>] [context <i>context-name</i> { exact prefix }] usm { authnopriv authpriv noauthnopriv }	Create and configure the SNMP v3 access group.
6	Switch(config)# snmp-server group <i>group-name</i> user <i>user-name</i> usm	Configure the mapping relationship between users and the access group.

11.1.6 Configuring IP authentication by SNMP server

Configure IP authentication by SNMP server for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server server-auth enable	Enable SNMP server IP authentication.
3	Switch(config)# snmp-server server-auth ip-address	Configure IP authentication address of the SNMP server.


11.1.7 Configuring other information of SNMP

Other information of SNMP includes:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMP v1, v2c, and v3 support configuring this information.

Configure other information about SNMP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server contact <i>contact</i>	(Optional) configure the logo and contact method of the administrator.  Note For example, set the E-mail to the logo and contact method of the administrator.
3	Switch(config)# snmp-server location <i>location</i>	(Optional) specify the physical location of the device.

11.1.8 Configuring Trap



Trap configurations on SNMP v1, v2c, and v3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the SWITCH to the NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the SWITCH and NMS is reachable.

Configure Trap of SNMP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server host <i>ip-address</i> version 3 { authnopriv authpriv noauthnopriv } <i>user-</i> <i>name</i> [udpport <i>udpport</i>]	(Optional) configure SNMP v3-based Trap target host.
3	Switch(config)# snmp-server host <i>ip-address</i> version { 1 2c } <i>com-</i> <i>name</i> [udpport <i>udpport</i>]	(Optional) configure SNMP v1-/SNMP v2c-based Trap target host.
4	Switch(config)# snmp-server enable traps	Enable Trap.

11.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show snmp access	Show SNMP access group configurations.
2	Switch# show snmp community	Show SNMP community configurations.
3	Switch# show snmp config	Show SNMP basic configurations, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, and Trap status.
4	Switch# show snmp group	Show the mapping relationship between SNMP users and the access group.
5	Switch# show snmp host	Show Trap target host information.
6	Switch# show snmp statistics	Show SNMP statistics.
7	Switch# show snmp user	Show SNMP user information.
8	Switch# show snmp view	Show SNMP view information.
9	Switch# show snmp server-auth	Show SNMP server authentication configurations.

11.2 KeepAlive

11.2.1 Introduction

KeepAlive packet is a kind of KeepAlive mechanism running in High-Level Data Link Control (HDLC) link layer protocol. The SWITCH will send a KeepAlive packet to confirm whether the peer is online every several seconds to realize neighbour detection mechanism.

Trap is the unrequested information sent by the SWITCH actively to NMS, used to report some urgent and important events.

The SWITCH sends KeepAlive Trap packet actively to the NMS. The KeepAlive Trap packet includes the basic information of SWITCH, such as the name, OID, MAC address, and IP address. The NMS synchronizes device information based on IP address to discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator.

11.2.2 Preparing for configurations

Scenario

The SWITCH sends KeepAlive Trap packet actively to the NMS. Therefore, the NMS can discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator. You can enable or disable KeepAlive Trap and configure the period for sending KeepAlive Trap. When KeepAlive Trap is enabled, if configured with **snmp enable traps** and Layer 3 IP address, the SWITCH will send a KeepAlive Trap to all target hosts with Bridge Trap every KeepAlive Trap interval.

Prerequisite

- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMP v3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the SWITCH and NMS is reachable.

11.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

11.2.4 Configuring KeepAlive

Configure KeepAlive for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	Switch(config)#snmp-server keepalive-trap enable	Enable KeepAlive Trap.
3	Switch(config)#snmp-server keepalive-trap interval <i>period</i>	(Optional) configure the period for sending KeepAlive Trap.



Caution

To avoid multiple devices sending KeepAlive Trap at the same time according to the same period and causing heavy network management load, the real transmission period of KeepAlive Trap is timed as period+5s random transmission.

11.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch#show keepalive	Show KeepAlive configurations.

11.3 RMON

11.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and NMS.

RMON is achieved based on SNMP architecture, including the network management center and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis to achieve the monitoring to one network segment and the whole network, while SNMP only can monitor the partial information of a single device and it is difficult for it to monitor one network segment.

RMON Agent is commonly referred to as the probe program; RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report network management center, and describes the capture information under unusual circumstances so that the network management center does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This approach reduces the data flows between network management center and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe data collection methods:

- Distributed RMON: network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.

- **Embedded RMON:** embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information of RMON Agent.

The SWITCH adopts embedded RMON, as shown in Figure 11-2. The SWITCH implements RMON Agent. Through this function, the management station can obtain the overall flow, error statistics, and performance statistics of this network segment connected to the managed network device interface to a monitor the network segment.

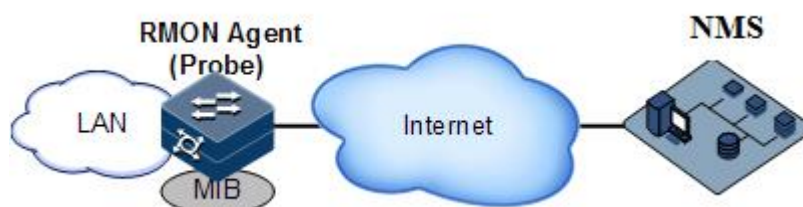


Figure 11-2 RMON

RMON MIBs are grouped into 9 groups according to functions. Currently, there are 4 groups achieved: statistics group, history group, alarm group, and event group.

- **Statistics group:** collect statistics on each interface, including number of received packets and packet size distribution statistics.
- **History group:** similar with the statistics group, but it only collect statistics in an assigned detection period.
- **Alarm group:** monitor an assigned MIB object, set the upper and lower thresholds in an assigned time interval, and trigger an event if the monitored object exceeds the threshold.
- **Event group:** cooperating with the alarm group, when alarm triggers an event, it records the event, such as sending Trap or writing it into the log, etc.

11.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the SWITCH actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the SWITCH and the NMS is reachable.

11.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enable on all interfaces
History group	Disable
Alarm group	N/A
Event group	N/A

11.3.4 Configuring RMON statistics

RMON statistics is used to take statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, and multicast packets, as well as received packet size.

Configure RMON statistics for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# rmon statistics <i>interface-type interface-list</i> [owner owner-name]	Enable RMON statistics on an interface and configure related parameters.



Note

When using the **no rmon statistics** *interface-type interface-list* command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

11.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# rmon history <i>interface-type interface-list</i> [shortinterval short-period] [longinterval long-period] [buckets buckets-number] [owner owner-name]	Enable RMON historical statistics on an interface and configure related parameters.



Note

When you use the **no rmon history interface-type interface-list** command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

11.3.6 Configuring RMON alarm group

You can monitor a MIB variable (*mibvar*) by setting a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. And then record the log or send Trap to the NMS according to the definition of alarm events.

The monitored MIB variable must be real, and the data value type is correct.

- If the setting variable does not exist or value type variable is incorrect, the system returns an error.
- For the successfully-set alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.

By default, the triggered event ID is 0, which indicates that no event is triggered. If the number is not set to 0 and there is no event configured in the event group, the event will not be successfully triggered when the monitored variable is abnormal. The event cannot be successfully triggered unless the event is established.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Configure the RMON alarm group for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# rmon alarm <i>alarm-id</i> <i>mibvar</i> [interval <i>period</i>] { absolute delta } rising-threshold <i>rising-value</i> [<i>rising-event-id</i>] falling-threshold <i>falling-value</i> [<i>falling-event-id</i>] [owner <i>owner-name</i>]	Add alarm instances to the RMON alarm group and configure related parameters.

11.3.7 Configuring RMON event group

Configure the RMON event group for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# rmon event <i>event-id</i> [log] [trap] [description <i>string</i>] [owner <i>owner-name</i>]	Add events to the RMON event group and configure processing modes of events.

11.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show rmon	Show RMON configurations.
2	Switch# show rmon alarms	Show information about the RMON alarm group.
3	Switch# show rmon events	Show information about the RMON event group.
4	Switch# show rmon statistics [<i>interface-type interface-number</i>]	Show information about the RMON statistics group.
5	Switch# show rmon history <i>interface-type interface-number</i>	Show information about the RMON history group.

11.3.9 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear rmon	Clear all RMON configurations.

11.4 LLDP

11.4.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very important. A lot of network management software adopts "auto-detection" function to trace changes of network topology, but most of the software can only analyze to the 3rd layer and cannot ensure that the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

Basic concepts

LLDP packet is to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 11-4, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

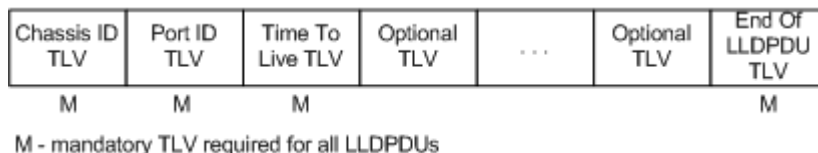


Figure 11-3 LLDPDU structure

TLV: unit combining LLDPDU, which refers to the unit describing the object type, length and information.

As shown in Figure 11-4, each TLV denotes piece of information at local, such as device ID, interface number, etc. related Chassis ID TLV, Port ID TLV fixed TLV.

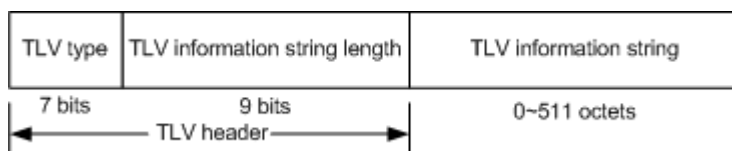


Figure 11-4 Basic TLV structure

Table 11-1 lists TLV type. At present only types 0-8 are used.

Table 11-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Port ID	Required
3	Time To Live	Required
4	Port Description	Optional
5	System Name	Optional
6	System Description	Optional
7	System Capabilities	Optional
8	Management Address	Optional

Principle of LLDP

LLDP is a kind of point-to-point one-way issuance protocol, which sends link status of the local device to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local device to the peer end.

The procedure of packet exchange is as below:

- When the local device transmits packet, it obtains system information required by TLV from NMS (Network Management System), obtains configurations from LLDP MIB, generates TLV, makes LLDPDU, encapsulates information to LLDP packets, and send LLDP packets to the peer end.
- The peer end receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and the NMS will be notified.

The aging time of Time To Live (TTL) in local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$:

- Interval: indicate the period for sending LLDP packets from the neighbor node.
- Hold-multiplier: the aging coefficient of device information in neighbor node.

11.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NMS for topology discovery, the SWITCH needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NMS queries.

Prerequisite

N/A

11.4.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP	Disable
LLDP interface status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
Alarm function	Enable

Function	Default value
Alarm notification timer	5s
Destination MAC address of LLDP packet	0180.c200.000e

11.4.4 Enabling global LLDP



Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

When you obtain connection information between devices through the NMS for topology discovery, the SWITCH needs to enable LLDP, sends their information to the neighbours mutually, and stores neighbour information to facilitate query by the NMS.

Enable global LLDP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# lldp enable	Enable global LLDP.

11.4.5 Enabling interface LLDP

Enable interface LLDP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Switch(config- gigaethernet1/1/1)# lldp enable	Enable LLDP on an interface.

11.4.6 Configuring basic functions of LLDP



Caution

When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

Configure basic functions of LLDP for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# lldp message-transmission interval <i>period</i>	(Optional) configure the period timer of the LLDP packet.
3	Switch(config)# lldp message-transmission delay <i>period</i>	(Optional) configure the delay timer of the LLDP packet.
4	Switch(config)# lldp message-transmission hold-multiplier <i>hold-multiplier</i>	(Optional) configure the aging coefficient of the LLDP packet.
5	Switch(config)# lldp restart-delay <i>period</i>	(Optional) restart the timer. When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

11.4.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NMS immediately.

Configure LLDP alarm for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server lldp-trap enable	Enable LLDP alarm.
3	Switch(config)# lldp trap-interval <i>period</i>	(Optional) configure the period timer of LLDP alarm Trap.



Note

After enabled with LLDP alarm, the SWITCH will send Traps after detecting aged neighbours, newly-added neighbours, and changed neighbour information.

11.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show lldp local config	Show LLDP local configurations.
2	Switch# show lldp local system-data [<i>interface-type interface-number</i>]	Show information about the LLDP local system.

No.	Command	Description
3	Switch# show lldp remote [<i>interface-type interface-number</i>] [detail]	Show information about the LLDP neighbor.
4	Switch# show lldp statistic [<i>interface-type interface-number</i>]	Show statistics of LLDP packets.

11.4.9 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear lldp statistic <i>interface-type interface-number</i>	Clear LLDP statistics.
Switch(config)# clear lldp remote-table [<i>interface-type interface-number</i>]	Clear LLDP neighbor information.
switch(config)# clear lldp global statistic	Clear global statistics of LLDP.

11.5 Optical module DDM

11.5.1 Introduction

Digital Diagnostic Monitoring (DDM) on the SWITCH supports diagnosing the Small Form-factor Pluggable (SFP) module.

SFP DDM provides a method for monitoring performance. By analyzing monitored data provided by the SFP module, the administrator can predict the lifetime for the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

The SFP module offers 5 performance parameters:

- Module temperature
- Internal Power Feeding Voltage (PFV)
- Launched bias current
- Launched optical power
- Received optical power

When SFP performance parameters exceed thresholds or when SFP state changes, related Trap is generated.

11.5.2 Preparing for configurations

Scenario

SFP DDM provides a method for monitoring performance parameters of the SFP module. By analyzing monitored data, you can predict the lifetime of the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

Prerequisite

N/A

11.5.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Global optical module DDM	Disable
Interface optical module DDM	Enable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Disable
Interface optical DDM password check	Disable

11.5.4 Enabling optical module DDM

Enable optical module DDM for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#transceiver ddm enable	Enable SFP DDM globally.
3	Switch(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Switch(config-gigaethernet1/1/1)#transceiver ddm enable	Enable interface optical module DDM. Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the SWITCH perform DDM.

11.5.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server trap transceiver enable	Enable optical module DDM Trap globally.
3	Switch(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Switch(config-gigaetherne t1/1/1)#transceiver trap enable	Enable interface optical module DDM Trap. Only when global optical DDM Trap is enabled, the optical module, where interface optical module DDM Trap is enabled, can the SWITCH send Traps.

11.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show transceiver	Show global optical module DDM and interface optical module DDM configurations.
2	Switch# show transceiver ddm interface-type interface-number [detail]	Show optical module DDM performance parameters.
3	Switch# show transceiver interface-type interface-number history [15m 24h]	Show historical information about optical module DDM.
4	Switch# show transceiver information interface-type interface-number	Show basic information about the optical module.
5	Switch# show transceiver threshold-violations interface-type interface-number	Show the information when the optical module parameters exceed the thresholds.

11.6 System log

11.6.1 Introduction

The system log refers that the SWITCH records the system information and debugging information in a log and sends the log to the specified destination. When the SWITCH fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- File: send the log message to the Flash of the device.
- Buffer: send the log message to the buffer.
- SNMP server: convert logs to Trap and then outputs Trap to the SNMP server.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 11-2.

Table 11-2 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information



Note

The severity of output information can be manually set. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For example, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3, that is, the severity ranges from emergencies to errors, can be sent.

11.6.2 Preparing for configurations

Scenario

The SWITCH generates critical information, debugging information, or error information of the system to system logs and outputs the system logs to log files or transmit them to the host, Console interface, or monitor for viewing and locating faults.

Prerequisite

N/A

11.6.3 Default configurations of system log

Default configurations of system log are as below.

Function	Default value
System log	Enable
Output log information to Console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Disable, the fixed level is warning (4).
Output log information to monitor	Disable, the default level is information (6).
Output log information to buffer	Disable, the default level is information (6).
Log Debug level	Low
Output log information to history list	Disable
Log history list size	1
Transfer log to Trap	Disable, the default level is warning (4).
Log buffer size	4 KBytes
Transmitting rate of system log	No limit
Timestamp of system log information	<ul style="list-style-type: none"> • Debug: no timestamp to debug level (7) Syslog information. • Log: The timestamp to 0–6 levels Syslog information is absolute time.

11.6.4 Configuring basic information of system log

Configure basic information of system log for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# logging on	(Optional) enable system log.
3	Switch(config)# logging time-stamp { debug log } { datetime none uptime }	<p>(Optional) configure timestamp for system log.</p> <p>The optional parameter debug is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp</p> <p>The optional parameter log is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.</p>

Step	Command	Description
4	Switch(config)# logging rate-limit <i>log-num</i>	(Optional) configure transmitting rate of system log.
5	Switch(config)# logging sequence-number	(Optional) configure sequence of system log. The sequence number only applies to Console, monitor, log file, and log buffer, but not log host and history list.
6	Switch(config)# logging discriminator <i>discriminator-number</i> { facility mnemonics msg-body } { { drops includes } <i>key</i> none }	(Optional) create and configure system log filter. The filter can filter output log from Console, monitor, log file and log buffer.
7	Switch(config)# logging buginf [high normal low none]	(Optional) configure sending Debug-level logs.

11.6.5 Configuring system log output

Configure system log output for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# logging console [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings discriminator <i>discriminator-number</i>]	(Optional) output system logs to the Console.
3	Switch(config)# logging host <i>ip-address</i> [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings discriminator <i>discriminator-number</i>]	(Optional) output system logs to the log host. Up to 10 log hosts are supported.
	Switch(config)# logging [<i>host ip-address</i>] facility { alert audit auth clock cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp security syslog user uucp }	Configure the facility field of the log to be sent to the log host. Configuration may fail if you do not create the log host. This configuration is available for all log hosts configured on the SWITCH.

Step	Command	Description
4	Switch(config)# logging monitor [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the monitor.
5	Switch(config)# logging file [discriminator <i>discriminateor-number</i>]	(Optional) output system logs to the Flash of the SWITCH. Only warning-level logs are available.
6	Switch(config)# logging buffered [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the buffer.
	Switch(config)# logging buffered size <i>size</i>	(Optional) configure the system log buffer size.
7	Switch(config)# logging history	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	Switch(config)# logging history size <i>size</i>	(Optional) configure the log history list size.
	Switch(config)# logging trap [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) enable translating specified logs in the history list to Traps. Configurations may fail if the system logs are not output to the log history list.

11.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show logging	Show configurations of system log.
2	Switch# show logging buffer	Show information about the system log buffer.
3	Switch# show logging discriminator	Show filter information.
4	Switch# show logging file	Show contents of system log.

No.	Command	Description
5	Switch# show logging history	Show information about the system log history list.

11.6.7 Maintenance

Maintain the SWITCH as below.

Command	Description
Switch(config)# clear logging buffer	Clear log information in the buffer.
Switch(config)# clear logging statistics	Clear log statistics.

11.7 Alarm management

11.7.1 Introduction

Alarm means when a fault is generated on the SWITCH or some working condition changes, the system will generate alarm information according to different faults.

Alarm information is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

Alarm information is stored in the alarm buffer. Meanwhile, the alarm information is generated to log information. If a Network Management System (NMS), the alarm information will be sent to network management system through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

There are three kinds of alarm information according to properties of an alarm:

- Fault alarm: refers to alarms for some hardware fault or some abnormal important functions, such as port Down alarm;
- Recovery alarm: refers to alarms that are generated when device failure or abnormal function returns to normal, such as port Up alarm;
- Event alarm: refers to prompted alarms or alarms that are generated because of failure in relating the fault to the recovery, such as alarms generated by failing to Ping.

The alarm information can be divided into five types according to functions:

- Communication alarm: refers to alarms related to the processing of information transmission, including alarms that are generated by communication fault between Network Elements (NE), NEs and NMS, or NMS and NMS.

- Service quality alarm: refers to alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing.
- Processing errored alarm: refers to alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and the abnormal program aborts.
- Environmental alarm: refers to alarms caused by equipment location-related problems, including the environment temperature, humidity, ventilation and other abnormal working conditions.
- Device alarm: refers to alarms caused by failure of physical resources, including power, fan, processor, clock, input/output ports and other hardware.

Alarm output

There are three alarm information output modes:

- Alarm buffer: alarm information is recorded in tabular form, including the current alarm table and history alarm table.
 - Current alarm table, recording alarm information which is not cleared, acknowledged or restored.
 - History alarm table, consisting of acknowledged and restored alarm information, recording the cleared, auto-restored or manually acknowledged alarm information.
- Log: alarm information is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm information sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the SWITCH, including CLI terminal and NMS.

Log output of alarm information starts with the symbol "#", and the output format is: #Index TimeStamp HostName ModuleName/Severity/name:Arise From Description.

Table 11-3 lists descriptions about alarm fields.

Table 11-3 Alarm fields

Field	Description
TimeStamp	Time when an alarm is generated
ModuleName	Name for a module where alarms are generated
Severity	Alarm level
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 11-4.

Table 11-4 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time to avoid more serious fault.	3 (Error)
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm inhibition

The SWITCH only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B which is in the inhibition list of alarm A, then alarm B is inhibited and does not appear in alarm buffer and record the log information when enabling alarm inhibition. By enabling alarm inhibition, the SWITCH can effectively reduce the number of alarms.

Alarm A and alarm B will be recorded on the SWITCH and reported to the NMS when alarm inhibition is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to NMS automatically with its generation and you do not need to initiate inquiries or synchronization.

You can set auto-report to some alarm, some alarm source, or the specified alarm from specified alarm source.



Note

The alarm source refers to an entity that generates related alarms, such as ports, devices, or cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

- When the alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to the configurations of the alarm module, such as recording alarm in alarm buffer, or recording system logs, etc;
- When the alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the SWITCH.

You can perform the alarm monitoring on some alarm, alarm source or specified alarm on from specified alarm source.

- Alarm reverse mode

Alarm reverse refers to the device will report the information opposite to actual status when recording alarm information, or report the alarm when there is no alarm information. Not report if there is alarm information.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be set; the specific definitions are as below:

- Non-reverse mode

The device alarm is reported normally.

- Manual reverse mode

Set the alarm reverse mode of an interface as manual reverse mode, then no matter what the current alarm state is, the reported alarm state of the interface will be changed opposite to the actual alarm state immediately, that is to say, not report when there are alarms, report when there are not alarms actually. The interface will maintain the opposite alarm state regardless of the alarm state changes before the alarm reverse state being restored to non-reverse mode.

- Auto-reverse mode

Set the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the setting will return fail; if the interface has actual reverse alarm, the setting is success and enter reverse mode, i.e. the interface reported alarm status is changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm state can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the SWITCH will record alarms and report them to NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, the device alarm is reported once generating (0s), which is instant reporting; clear alarm once it ends (0s), which is instant clearing.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

- **stop**: stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.

- **loop**: wrapping mode, when the alarm buffer is full, the new generated alarms will replace old alarm information and take rolling records.

Use configured storage mode to deal with new generated alarm information when the alarm information in device alarm table is full.

- Clearing alarms

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the history alarm table.

- Viewing alarms

The administrator can check alarms and monitor alarm information directly on the SWITCH. If the SWITCH is configured with NMS, the administrator can monitor alarms on the NMS.

11.7.2 Preparing for configurations

Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm information can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management makes it easy for the user to take alarm inhibition, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. When you need to send alarm information to the system log host, configure the IP address of the system log host for the device.
- In Trap output mode: configure the IP address of the NMS for the device.

11.7.3 Configuring basic functions of alarm management

Configure basic information of alarm management for the SWITCH as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	Switch# confi	Enter global configuration mode.

Step	Command	Description
2	Switch(config)# alarm inhibit enable	Enable alarm inhibition. By default, it is enabled.
3	Switch(config)# alarm auto-report all enable	Enable alarm auto-reporting.
	Switch(config)# alarm auto-report alarm-restype alarm-restype-value enable	Enable alarm auto-reporting of a specified alarm source.
	Switch(config)# alarm auto-report type alarm-type enable	Enable alarm auto-reporting of a specified alarm type.
	Switch(config)# alarm auto-report type alarm-type alarm-restype alarm-restype-value enable	Enable alarm auto-reporting of a specified alarm source and type.
4	Switch(config)# alarm monitor all enable	Enable alarm monitoring.
	Switch(config)# alarm monitor alarm-restype alarm-restype-value enable	Enable alarm monitoring of a specified alarm source.
	Switch(config)# alarm monitor type alarm-type enable	Enable alarm monitoring of a specified alarm type.
	Switch(config)# alarm monitor type alarm-type alarm-restype alarm-restype-value enable	Enable alarm monitoring of a specified alarm source and type.
5	Switch(config)# alarm inverse interface-type interface-number { none auto manual }	Configure alarm reverse modes. By default, it is none; namely, alarm reverse is disabled.
6	Switch(config)# alarm { active cleared } delay second	Configure alarm delay. By default, it is 0s.
7	Switch(config)# alarm active storage-mode { loop stop }	Configure alarm storage modes. By default, it is stop.
8	Switch(config)# alarm clear all	(Optional) clear all current alarms.
	Switch(config)# alarm clear index index	(Optional) clear current alarms of the specified alarm index.
	Switch(config)# alarm clear alarm-restype alarm-restype-value	(Optional) clear current alarms of the specified alarm source.
	Switch(config)# alarm clear type alarm-type	(Optional) clear current alarms of the specified alarm type.

Step	Command	Description
	Switch(config)# alarm clear type <i>alarm-type alarm-restype alarm-restype-value</i>	(Optional) clear current alarms of the specified alarm source and type.
9	Switch(config)# alarm syslog enable	(Optional) enable alarms to be output to system logs. By default, it is disabled.
10	Switch(config)# exit Switch# show alarm active [<i>module_name</i> severity severity]	(Optional) show information about current alarms.
	Switch# show alarm cleared [<i>module_name</i> severity severity]	(Optional) show information about historical alarms.



Note

You can enable/disable alarm monitoring, alarm auto-reporting, and alarm clearing on modules that support alarm management.

11.7.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show alarm management [<i>alarm_type</i>]	Show parameters of current alarms, including status of alarm inhibition, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	Switch# show alarm log	Show alarm statistics in the system log.
3	Switch# show alarmmanagement statistics	Show alarm management module statistics.
4	Switch# show alarm active	Show information about current alarms.

11.8 Hardware environment monitoring

11.8.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the SWITCH. The monitoring alarm events include:

- Power supply state alarm
- Temperature beyond threshold alarm

- Voltage beyond threshold alarms
- Abnormal interface status alarm
- Flash monitoring alarm

There are several ways to notify users when an alarm is generated. The alarm event output methods are as below:

- Save to the device hardware environment monitoring alarm buffer;
- Output Syslog system log;
- Send Trap to network management center;
- Output to the relay fault indication LED.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms

Power supply state alarms include 2 types.

- Power supply voltage anomaly alarm

An alarm is generated when the power supply voltage is 20% greater than the pre-configured voltage (12 V) or is 20% smaller than the pre-configured voltage (12 V). In addition, an alarm is generated when the voltage value returns to normal state. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

- Power supply state change alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The SWITCH supports dual power supplies. Therefore, power supply state change alarms are divided into the single power supply state change alarm and device dying gasp alarm.

- Dual power supply state change alarm: notify users that power supply 1/power supply 2 changes. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.
- Device dying gasp alarm: dual power modules are unplugged, namely, two power modules are out of position. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

- Temperature beyond threshold alarm

The device supports temperature beyond threshold alarm event, when the current temperature is lower than low temperature threshold, the low temperature alarm event will generate. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

When the device current temperature is higher than high temperature threshold, the high temperature alarm event will generate. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

- Voltage beyond threshold alarm

The device supports voltage beyond threshold alarm event, when the current voltage is lower than low voltage threshold, the low voltage alarm event will generate. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

When current voltage value of the monitored voltage is greater than the threshold, a high voltage alarm is generated. The SWITCH supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.



Note

The SWITCH monitors 3.3V master chip voltage only.

- Interface status alarm

Each interface has two alarm events:

- Interface link-fault alarm: link failure alarm refers to the peer link signal loss. The alarm event only aims at optical port, but not power port.
- Interface link-down alarm: interface status Down alarm.

The SWITCH supports saving these two types of alarm events to the device hardware environment monitoring alarm buffer, sending Trap to the NMS, and outputting to the system log and relay.

Alarm output modes

Hardware environment monitoring alarm output modes are as below.

- Hardware environment monitoring alarm buffer output, which is recorded to the hardware environment monitoring alarm table
 - The hardware environment monitoring current alarm table, recording current alarm information which has not been cleared and restored.
 - The hardware environment monitoring history alarm table, recording current, restored, and manually cleared alarms.

Hardware environmental monitoring alarm information can be recorded in the current hardware environment monitoring alarm table and hardware environment monitoring history alarm table automatically without configuring manually.

- Trap output

Alarms are output to network management center in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 11-5 describes Trap information.

Table 11-5 Trap information

Field	Description
Alarm status	<ul style="list-style-type: none"> • asserted (current alarm) • cleared (alarm recovery) • clearall (clear all alarm information)

Field	Description
Alarm source	<ul style="list-style-type: none"> • device (global alarm) • Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	<ul style="list-style-type: none"> • dev-power-down (power-down alarm) • power-abnormal (power-abnormal alarm, one of two powers is power down.) • high-temperature (high-temperature alarm) • low-temperature (low-temperature alarm) • high-volt (high-voltage alarm) • low-volt (low-voltage alarm) • link-down (interface LinkDown alarm) • link-falut (interface LinkFault alarm) • all-alarm (clear all alarm information)

- Syslog output

Record alarm information to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Syslog output.

Table 11-6 describes Syslog information.

Table 11-6 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.
Severity	Level, see Table 11-2 for the same system log defined levels.
Mnemonics	Alarm event type, see Table 11-5 for the detailed type description.
Msg-body	Main body, describing alarm event contents.

- Relay output

"Outputting to relay" or "Outputting from relay" indicates outputting alarms to the relay and fault indication LED simultaneously. The relay and fault indication LED are bound together. Relay output and fault indicate LED output are controlled by the relay alarm output switch. As a public fault output mode for all alarms, the relationship among all alarms is logical "OR".

If any alarm is generated on the SWITCH, the device outputs the alarm from the relay. The relay cannot work properly unless all alarms are cleared.

Relay output cannot be enabled globally. Relay output is enabled for every monitored alarm.

11.8.2 Preparing for configurations

Scenario

Hardware environment monitoring provides environment monitoring for the devices, through which you can monitor the fault. When device operation environment is abnormal, this function will record hardware environment monitoring alarm list, generate system log, or send Trap and other alarms to notify taking corresponding measures and preventing fault.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. When you need to send alarm information to the system log host, please configure system log host IP address for the device.
- In Trap output mode: please configure network management center IP address for the device.
- In relay output mode: relay alarm output switch is enabled for every alarm.

11.8.3 Default configurations of hardware environment monitoring

Default configurations of hardware environment monitoring are as below.

Function	Default value
Global hardware environment monitoring alarm Syslog output	Disable
Global hardware environment monitoring alarm Trap output	Disable
Power down event alarm	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Enable relay output.
Temperature alarm output	
Voltage alarm output	
Interface link-down event alarm output	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Disable relay output.
Interface link-fault event alarm output	<ul style="list-style-type: none"> • Disable Trap output. • Disable Syslog system log output. • Disable relay output.
High temperature alarm threshold	102°C
Low temperature alarm threshold	-40°C
High voltage threshold	3450 mV
Low voltage threshold	3150 mV

11.8.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# logging alarm	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	Switch(config)# snmp-server alarm-trap enable	(Optional) enable global hardware environment monitoring alarm Trap.



Note

When enabling global hardware environment monitoring alarm Syslog output, alarm event can generate Syslog only when Syslog output under alarm event is also enabled.

When enabling global hardware environment monitoring alarm sending Trap, alarm event can send Trap only when Trap output under alarm event is also enabled.

When enabling global hardware environment monitoring alarm Relay output, alarm event can generate Relay only when Relay output under alarm event is also enabled.

11.8.5 Configuring temperature monitoring alarm


Configure temperature monitoring alarm for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# alarm temperature { high <i>high-value</i> low <i>low-value</i> notifies syslog relay }	Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes. <ul style="list-style-type: none"> • The high temperature threshold (high-value) must be greater than the low temperature threshold (low-value). • The low temperature threshold (low-value) must be smaller than the high temperature threshold (high-value).

11.8.6 Configuring voltage monitoring alarm


Configure voltage monitoring alarm for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.

Step	Command	Description
2	<pre>Switch(config)#alarm voltage { high high-value low low-value notifies syslog }</pre>	Enable voltage alarm output and configure voltage alarm output modes or voltage alarm threshold.  Note The SWITCH monitors 3.3V master chip voltage only.

11.8.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the SWITCH as below.

Step	Command	Description
1	Switch#config	Enter global configuration mode.
2	Switch(config)#clear alarm	Clear alarms manually.  Note Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list. If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.

11.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch#show alarm	Show global hardware environment monitoring alarm configurations.
2	Switch#show alarm <i>interface-type</i> <i>interface-number</i>	Show interface state alarms.
3	Switch#show alarm current	Show current alarms of hardware environment monitoring.
4	Switch#show alarm history	Show historic alarms of hardware environment monitoring.
5	Switch#show environment [power temperature voltage]	Show current power supply, temperature, and voltage alarms, as well as current environment information.

11.9 CPU monitoring

11.9.1 Introduction

The SWITCH supports CPU monitoring. It can monitor state, CPU utilization, and stack usage in real time. It helps to locate faults.

CPU monitoring can provide the following functions:

- View CPU utilization

It can be used to view CPU unitization in each period (5s, 1 minute, 10 minutes, and 2 hours). Total CPU unitization in each period can be shown dynamically or statically.

It can be used to view the operating status of all tasks and the detailed running status of assigned tasks.

It can be used to view history CPU utilization in each period.

It can be used to view death task information.

- CPU unitization threshold alarm

If system CPU utilization changes below lower threshold or above upper threshold in a specified sampling period, an alarm will be generated and a Trap message will be sent. The Trap message provides serial number and CPU utilization of 5 tasks whose CPU unitization is the highest in the latest period (5s, 1 minute, 10 minutes).

11.9.2 Preparing for configurations

Scenario

CPU monitoring can monitor state, CPU utilization, and stack usage in real time, provide CPU utilization threshold alarm, detect and eliminate hidden dangers, or help the administrator with fault location.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NMS.

11.9.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Disable
Upper threshold of CPU utilization alarm	99%
Lower threshold of CPU utilization alarm	1%

Function	Default value
Sampling period of CPU utilization	60s

11.9.4 Showing CPU monitoring information

Show CPU monitoring information for the SWITCH as below.

Step	Command	Description
1	Switch# show cpu-utilization [dynamic history { 10min 1min 2hour 5sec }]	Show CPU utilization.
2	Switch# show process [dead sorted { normal-priority process-name } taskname]	Show states of all tasks.
3	Switch# show process cpu [sorted [10min 1min 5sec invoked]]	Show CPU utilization of all tasks.
4	Switch(config)# cpu falling-threshold <i>value</i>	

11.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the SWITCH as below.

Step	Command	Description
1	Switch# config	Enter global configuration mode.
2	Switch(config)# snmp-server traps enable cpu-threshold	Enable CPU threshold alarm Trap.
3	Switch(config)# cpu rising-threshold <i>threshold-value</i>	(Optional) configure the rising threshold for CPU alarms.
4	Switch(config)# cpu falling-threshold <i>value</i>	(Optional) configure the falling threshold for CPU alarms.

11.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show cpu-utilization	Show CPU utilization and related configurations.

11.10 Cable diagnosis

11.10.1 Introduction

The SWITCH supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Time for last cable diagnosis
- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

11.10.2 Preparing for configurations

Scenario

After cable diagnosis is enabled, you can learn the running status of cables, locate and clear faults, if any, in time.

Prerequisite

N/A

11.10.3 Configuring cable diagnosis

Configure cable diagnosis for the SWITCH as below.

Step	Command	Description
1	Switch# test cable-diagnostics <i>interface-type interface-number</i>	Enable cable diagnosis.

11.10.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show cable-diagnostics [<i>interface-type interface-number</i>]	Show results of cable diagnosis.

11.11 Memory monitoring

11.11.1 Preparing for configurations

Scenario

Memory monitoring enables you to learn the memory utilization in real time, and provides memory utilization threshold alarms, thus facilitating you to locate and clear potential risks and help network administrator to locate faults.

Prerequisite

To output memory utilization threshold alarms as Trap, configure the IP address of the target host, namely, the IP address of the NMS.

11.11.2 Configuring memory monitoring

Configure memory monitoring for the SWITCH as below.

Step	Command	Description
1	Switch# memory utilization threshold <i>threshold-value</i>	Configure the upper threshold for memory utilization alarms. By default, it is 70, namely, 70%.
2	Switch# memory utilization monitor enable	Enable memory monitoring. By default, it is enabled.

11.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Switch# show memory [utilization threshold]	Show the memory utilization.

11.12 Ping

11.12.1 Introduction

Ping derives from the sonar location operation, which is used to detect whether the network is normally connected. Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information

is displayed on the sender, it indicates the route between source and destination addresses are unreachable.

Figure 11-5 shows the principle of Ping.

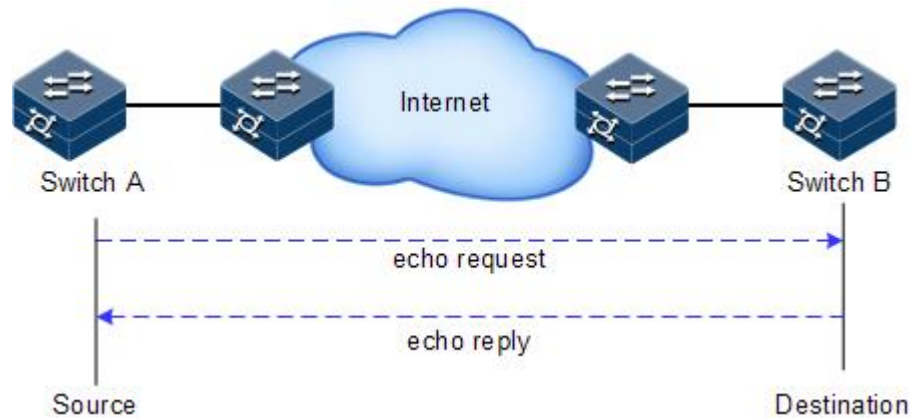


Figure 11-5 Principle of Ping

11.12.2 Configuring Ping

Configure Ping for the SWITCH as below.

Step	Command	Description
1	Switch#ping ip-address [count count] [size size] [waittime period]	(Optional) test the connectivity of the IPv4 network by the ping command.
2	Switch#ping ipv6 ipv6-address [count count] [size size] [waittime period]	(Optional) test the connectivity of the IPv6 network by the ping command.



Note

The SWITCH cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or break off Ping by pressing **Ctrl+C**.

11.13 Traceroute

11.13.1 Introduction

Just as Ping, Traceroute is a commonly used maintenance method in network management. **Traceroute** is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault

The following shows how Traceroute works:

- First, send a piece of TTL1 sniffer packet (where the UDP port number of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.

- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The above steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port number of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet. The Traceroute function principles are shown in Figure 11-6.

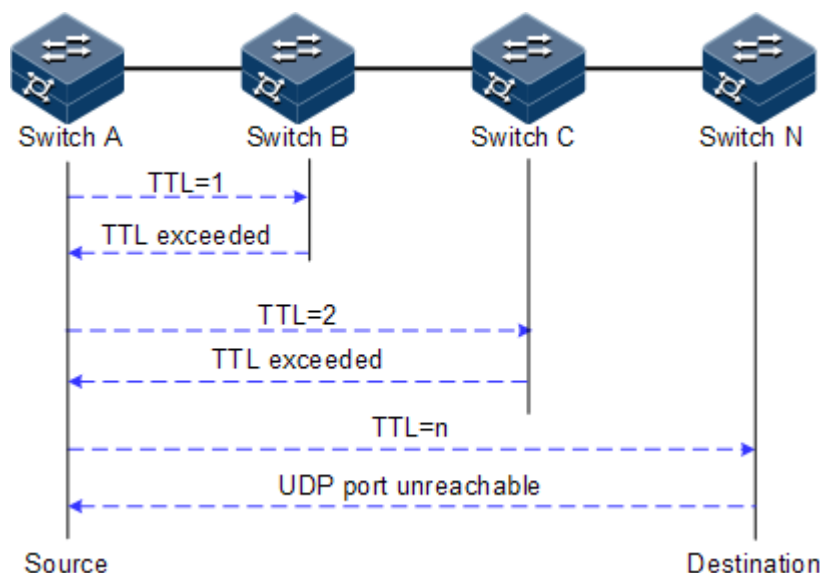


Figure 11-6 Principles of Traceroute

11.13.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the SWITCH.

Configure Traceroute for the SWITCH as below.

Step	Command	Description
1	Switch# traceroute ip-address [firstttl <i>fitst-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-id</i>] [waittime <i>second</i>] [count <i>times</i>]	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the traceroute command.
2	Switch# traceroute ipv6 ipv6-address [firstttl <i>fitst-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-id</i>] [waittime <i>second</i>] [count <i>times</i>]	(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the traceroute command.

12 Appendix

This chapter describes terms and abbreviations involved in this guide, including the following sections:

- Terms
- Acronyms and abbreviations

12.1 Terms

A

Access
Control List
(ACL)

A series of ordered rules composed of permit | deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, interface ID, etc. The device decides to receive or refuse the packets based on these rules.

Automatic
Laser
Shutdown
(ALS)

The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.

Auto-
negotiation

The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface, that is, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.

Automatic
Protection
Switching
(APS)

APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

B

Bracket

Small parts at both sides of the chassis, used to install the chassis into the cabinet

C

Challenge Handshake Authentication Protocol (CHAP) CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.

D

Dynamic ARP Inspection (DAI) A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.

Dynamic Host Configuration Protocol (DHCP) A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can realize centralized management of IP addresses.

E

Ethernet in the First Mile (EFM) Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification, etc. for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

Ethernet Ring Protection Switching (ERPS) It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Failover Failover provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.

Full duplex	In a communication link, both parties can receive and send data concurrently.
G	
GFP encapsulation	Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.
Grounding cable	The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the grounding cable properly is an important guarantee to lightning protection, anti-electric shock, and anti-interference.
H	
Half duplex	In a communication link, both parties can receive or send data at a time.
I	
Institute of Electrical and Electronics Engineers (IEEE)	A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
Internet Assigned Numbers Authority (IANA)	The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
Internet Engineering Task Force (IETF)	A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.
L	
Label	Symbols for cable, chassis, and warnings

Link Aggregation	With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.
Link Aggregation Control Protocol (LACP)	A protocol used for realizing link dynamic aggregation. The LACPDU is used to exchange information with the peer device.
M	
Multi-mode fiber	In this fiber, multi-mode optical signals are transmitted.
N	
Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.
O	
Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)
Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.
P	
Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered insecure.
Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.

Private VLAN (PVLAN) PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

Q

QinQ QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

Quality of Service (QoS) A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP) Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks

Remote Authentication Dial In User Service (RADIUS) RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP) A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

Simple Network Time Protocol (SNTP) SNTP is mainly used for synchronizing time of devices in the network.

Single-mode fiber In this fiber, single-mode optical signals are transmitted.

Spanning Tree Protocol (STP) STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.

V

Virtual Local Area Network (VLAN) VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.

VLAN mapping VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

12.2 Acronyms and abbreviations

A

AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

B

BC	Boundary Clock
BDR	Backup Designated Router

BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station
C	
CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree
D	
DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line
E	

EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection
F	
FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
H	
HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol
I	
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
NMS	Network Management System

O

OAM	Operation, Administration and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First
P	
P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Ping	Packet Internet Grope
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RPL	Ring Protection Link
RSTP	Rapid Spanning Tree Protocol

RSVP	Resource Reservation Protocol
S	
SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol
T	
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
U	
UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model
V	
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

W

WAN

Wide Area Network

WRR

Weight Round Robin

