OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управление коммутатором с помощью интерфейса командной строки (CLI)

Прежде чем приступать к эксплуатации изделия, внимательно прочтите настоящее руководство

www.osnovo.ru

SEC.RU | Короткий путь к информации Скачано с sec.ru

Оглавление

First chapters 13
Introduction of CLI command line 13
1.1 Access switch CLI 14
1.1.1 Users access CLI through Console port 14
1.1.2 Users access CLI through TELNET 15
1.2 CLI mode introduction 16
1.2.1 The role of CLI model 17
1.2.2 Identification of CLI mode 17
1.2.3 Classification of CLI patterns 18
1.3 Introduction to command syntax 19
1.3.1 Command composition 20
1.3.2 Parameter type 20
1.3.3 Command syntax rules 20
1.3.4 Command abbreviation 22
1.3.5 Grammar help 22
1.3.6 Command line error message 23
1.4 Command line shortcuts 23
1.4.1 Line edit shortcut key 23
1.4.2 Display command shortcut key 24
1.5 History command 25
Second chapters 25
System management configuration 25
2.1 System security configuration 25
2.1.1 Multi-user management control 26
2.1.2 TACACS+ authentication authorization 27
2.1.3 Anonymous user password control 29
2.1.4 Enable password control 30
2.1.5 TELNET service control 31
2.1.6 SNMP service control 32
2.1.7 HTTP service control 33
2.1.8 SSH service control 34
2.2 System maintenance and debugging 34
2.2.1 Configure the host name of the system 34
2.2.2 Configuring the system clock 35
2.2.3 Configure terminal timeout attributes 36

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2.4 System reset 36
2.2.5 View system information 37
2.2.6 Network connectivity debugging 37
2.2.7 Detecting line distance 38
2.2.8 Traceroute debugging 38
2.2.9 Telnet client 38
2.2.10 UDLD configuration 39
2.3 Configuration file management 40
2.3.1 View configuration information 41
2.3.2 Save configuration 41
2.3.3 Delete configuration file 42
2.3.4 Download configuration files 42
2.4 Software version upgrade 45
2.4.1 Software version upgrade commands 45
2.4.2 Software upgrade process 45
Third chapters 48
port configuration 48
3.1 Common configuration for ports 49
3.1.1 Port rate configuration 49
3.1.2 Display port information 49
3.2 Configuration MIRROR 50
3.2.1 Configuration of the MIRROR listen on port and is listening on port 50
3.2.2 Display the configuration of MIRROR 51
3.3 Configuring STORM-CONTROL 51
3.3.1 Default configuration 52
3.3.2 Broadcast suppression configuration 52
3.3.3 Multicast suppression configuration 52
3.3.4 DLF suppression configuration 53
3.3.5 Inhibition rate configuration 53
3.3.6 Display STORM-CONTROL configuration 53
3.4 Configuring STORM-CONSTRAIN 53
3.5 Configuring FLOW-CONTROL 56
3.5.1 Default configuration 56
3.5.2 Set port receive and send side flow control 57
3.5.3 Closed port flow control 57
3.5.4 Display flow control information 57
3.6 Configuring port bandwidth 57
3.6.1 Default configuration 58

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.6.2 Set port send or receive bandwidth control 58
3.6.3 Cancellation of port transmit or receive bandwidth control 58
3.6.4 Bandwidth control of display port configuration 58
3.7 Configuring TRUNK 59
3.7.1 LACP protocol configuration 60
3.7.2 Configuration of TRUNK group 61
3.7.3 TRUNK group member port configuration 61
3.7.4 TRUNK load balancing policy configuration 62
3.7.5 Display of TRUNK 62
3.8 Configure super large frame 62
3.8.1 Oversize introduction 62
3.8.2 Oversize configuration 63
3.9 Configuring redundant ports 63
3.9.1 Configuration of redundant ports 63
3.9.2 Display of redundant ports 64
3.10 Configuring LLDP 65
3.10.1 LLDP configuration 65
3.10.2 LLDP display 66
Fourth chapters 66
Port based MAC security 66
4.1 brief introduction 67
4.2 MAC binding configuration 67
4.3 MAC filter configuration 68
4.4 Port learning constraint configuration 69
Fifth chapters 70
Port IP and MAC binding 70
5.1 brief introduction 70
5.2 IP and MAC binding configurations 71
5.3 Configuration example 71
5.4 Configuration misarrangement 73
Sixth chapters 74
VLAN configuration 74
6.1 VLAN introduce 74
6.1.1 The benefits of VLAN 75
6.1.2 VLAN ID 76
6.1.3 VLAN port member type 77
6.1.4 Default VLAN of port 77
6.1.5 Port VLAN mode 77

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1.6 VLAN relay....78
6.1.7 Data flow is forwarded in VLAN....78
6.2 VLAN configuration....80
6.2.1 Creating and deleting VLAN....80
6.2.2 Configuring port VLAN mode....81
6.2.3 VLAN configuration of ACCESS mode....81
6.2.4 VLAN configuration of TRUNK mode....82
6.2.5 HYBRID mode VLAN configuration....83
6.3VLAN configuration example....86
6.3.1 VLAN based on PORT....86
6.3.2 VLAN based on 802.1Q....87
6.4 MAC, IP subnet, protocol VLAN....89
6.5 Voice VLAN....90
6.6 VLAN mapping....92
6.7 QinQ....92
Seventh chapters....95
QoS configuration....95
7.1 QoS introduce....95
7.1.1 QoS based on COS....96
7.1.2QoS based on DSCP....97
7.1.3 Policy based QOS....97
7.2 QoS configuration....97
7.2.1 Default configuration for QoS....97
7.2.2 Configuration scheduling mode....99
7.2.3 Configuring queue weights....99
7.2.4 Configure the mapping relationship between DSCP and QosProfile....99
7.2.5 Configuring port QoS....99
7.2.6 Configuring the port user priority (COS value)....102
7.4 Policy QoS configuration example....103
Eighth chapters....104
MSTP configuration....104
8.1 MSTP introduce....104
8.1.1 overview....104
8.1.2 Multiple spanning tree domains....104
8.1.3 IST, CIST, and CST....105
8.1.4 Intra domain operation....105
8.1.5 Inter-domain operation....106
8.1.7 Boundary port....107

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.1.9 Port role 108
8.1.10 A brief introduction to 802.1D spanning tree 110
8.2 MSTP configuration 112
8.2.2 General configuration 112
8.2.3 Domain configuration 115
8.2.4 Instance configuration 115
8.2.6 PORTFAST related configuration 118
8.3 MSTP configuration example 121
Ninth chapters 122
EAPS configuration 122
9.1 EAPS brief introduction 122
9.2 Basic concepts of EAPS 123
9.3 EAPS protocol introduction 123
9.3.1Link-Down alarm 124
9.3.2 Loop inspection 124
9.3.3 Ring restoration 124
9.3.4 Extreme compatible with EAPS 125
9.3.5 Multi EAPS Domain 125
9.4EAPS configuration 125
9.5 Restrictive conditions 125
9.6 A brief introduction to the EAPS command 126
9.7 Single - loop configuration example 127
9.8 Example of cross ring data forwarding configuration 132
Tenth chapters 136
ERPS configuration 136
10.1 ERPS overview 136
10.2 Introduction of ERPS Technology 136
10.2.1 ERPS ring 136
10.2.2 ERPS node 136
10.2.3 Link and channel 137
10.2.4 ERPS VLAN 137
10.3 ERPS Working principle 138
10.3.1 Normal state 138
10.3.2 Link failures 138
10.3.3 Link recovery 139
10.4 Technical features of ERPS 140
10.4.1 ERPS load balancing 140
10.4.2 Good safety 141

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.4.3 Multi-loop intersecting is supported 141
10.5 ERPS protocol command 142
10.6 Typical use of ERPS 144
10.6.1 Example of single ring 144
10.6.2 Multi ring example 147
10.6.3 Multi instance load balancing example 153
Eleventh chapters 161
AAA configuration 161
11.1 802.1x introduce 162
11.1.1 802.1x device composition 163
11.1.2 Brief introduction of protocol package 164
11.1.3 Protocol flow interaction 165
11.1.4 802.1x port state 166
11.2 RADIUS introduce 167
11.2.1 Brief introduction of protocol package 168
11.2.2 Protocol flow interaction 169
11.2.3 User authentication method 170
11.3 Configuring 802.1x 171
11.3.1 802.1x default configuration 171
11.3.2 Start and close 802.1x 172
11.3.3 Configuring 802.1x port status 172
11.3.4 Configuring 802.1x port authentication 173
11.3.5 Configuring 802.1x port guest VLAN 173
11.3.6 Configuration re authentication mechanism 174
11.3.7 Maximum number of configuration port access host 174
11.3.8 Configure interval times and resend times 175
11.3.9 Configuration port is the transport port 175
11.3.10 Configuring the 802.1x client version number 176
11.3.11 Configure whether to check the client version number 176
11.3.12 Configuration authentication method 176
11.3.13 Configure whether to check the client's timing packet 177
11.3.14 Display 802.1x information 177
11.4 configuration RADIUS 177
11.4.1 RADIUS Default configuration 178
11.4.2 Configuring the IP address of the authentication server 178
11.4.3 Configuring shared keys 178
11.4.4 Start and close billing 179
11.4.5 Configuring RADIUS ports and attribute information 179

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11.4.6 Configuring RADIUS roaming function 179
11.4.7 Display RADIUS information 180
11.5 Configuration example 180
Twelfth chapters 181
GMRPconfiguration 181
12.1 GMRP introduce 181
12.2 configuration GMRP 181
12.2.1 Open GMRP settings 182
12.2.2 View GMRP information 182
12.3 Examples of typical GMRP configurations 182
Thirteenth chapters 184
SNOOPING configuration 184
13.1 IGMP SNOOPING introduce 184
13.1.1 IGMP SNOOPING processing 184
13.1.2 Second layer dynamic multicast 185
13.1.3 Join a group 186
13.1.4 Leave a group 188
13.2 IGMP SNOOPING configuration 188
13.2.1 IGMP SNOOPING default configuration 188
13.2.2 Open and close IGMP SNOOPING 189
13.2.3 Configuration survival time 189
13.2.4 configuration fast-leave 190
13.2.5 configuration MROUTER 190
13.2.6 display information 190
13.3 The IGMP SNOOPING configuration example 191
Fourteenth chapters 192
MVR configuration 192
14.1 MVR profile 192
14.2 configuration MVR 193
14.3 MVR configuration example 193
Fifteenth chapters 195
DHCP SNOOPING configuration 195
15.1 DHCP SNOOPING introduce 195
15.1.1 DHCP SNOOPING processing 196
15.1.2 DHCP SNOOPING binding table 196
15.1.3 DHCP SNOOPING specifies the physical port of the linked server 197
15.1.4 DHCP SNOOPING binding list is uploaded and downloaded 197
15.2 DHCP SNOOPING configuration 198

SEC.RU | Короткий путь к информации
Скачано с sec.ru

15.2.1 DHCP SNOOPING default configuration 198
15.2.2 Global open and close DHCP SNOOPING 198
15.2.3 The interface opens and closes DHCP SNOOPING 199
15.2.4 DHCP SNOOPING binding list is uploaded and downloaded 199
15.2.5 display information 200
15.3 DHCP SNOOPING configuration example 200
15.3.1 configuration 200
15.4 DHCP SNOOPING configuration error 202
Sixteenth Chapters 203
MLD SNOOPING configuration 203
16.1 MLD SNOOPING introduce 203
16.1.1 MLD SNOOPING processing 204
16.1.2 Second layer dynamic multicast 205
16.1.3 Join a group 205
16.1.4 Leave a group 207
16.2 MLD SNOOPING configuration 207
16.2.1 MLD SNOOPING default configuration 207
16.2.2 Open and close MLD SNOOPING 208
16.2.3 Configuration survival time 208
16.2.4 configuration fast-leave 209
16.2.5 configuration MROUTER 209
16.2.6 display information 209
16.3 MLD SNOOPING configuration example 210
Seventeenth chapters 211
ACL configuration 211
17.1 Introduction of ACL resource library 212
17.2 ACL filtering introduction 214
17.3 ACL repository configuration 215
17.4 ACL based on time interval 218
17.5 ACL filter configuration 221
17.6 ACL configuration example 221
17.7 ACL configuration debugging 222
Eighteenth chapters 223
TCP/IP basic configuration 223
18.1 Configuring the VLAN interface 223
18.2 Configuring ARP 225
18.2.1 Configuring static ARP 226
18.2.2 View ARP information 227

SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.3 Configuring static routing 228
18.4 TCP/IP basic configuration example 231
18.4.1 Three layer interface 231
18.4.2 Static routing 232
18.4.3 ARP 232
Nineteenth chapters 233
SNMP configuration 233
19.1 SNMP introduce 233
19.2 SNMP configuration 234
19.3 SNMP configuration example 237
Twentieth chapters 238
RMON configuration 238
20.1 RMON introduce 238
20.2 RMON configuration 239
20.3 RMON configuration example 241
Twenty-first chapters 242
Cluster configuration 242
21.1 Introduction of cluster management 242
21.1.1 Cluster definition 242
21.1.2 Cluster role 243
21.1.3 NDP profile 244
21.1.4 NTDP profile 245
21.1.5 Cluster management maintenance 246
21.1.6 Managing VLAN 248
21.2 Brief introduction of cluster configuration 249
21.3 Configuration management equipment 249
21.3.1 Enable system and port NDP capabilities 249
21.3.2 Configuring NDP parameters 250
21.3.3 Enable system and interface NTDP capabilities 250
21.3.4 Configuring NTDP parameters 251
21.3.5 Configure manual collection of NTDP information 251
21.3.6 Enable cluster function 252
21.3.7 Build clusters 252
21.3.8 Configure the cluster's internal members to interact 254
21.3.9 Configuring cluster member management 255
21.4 Configuration member device 255
21.4.1 Enable system and port NDP capabilities 255
21.4.2 Enable system and port NTDP capabilities 255

SEC.RU | Короткий путь к информации
Скачано с sec.ru

21.4.3 Configure manual collection of NTDP information 255
21.4.4 Enable cluster function 255
21.5 Configuring access cluster members 255
21.6 Cluster management display and maintenance 256
21.7 Example of cluster management typical configuration 257
Twenty-second chapters 259
System log configuration 259
22.1 System log introduction 259
22.1.1 Format of log information 260
22.1.2 Log storage 261
22.1.3 Log display 262
22.1.4 Debugging tools 262
22.2 System log configuration 263
22.2.1 Configuring terminal real time display switch 263
22.2.2 View log information 264
22.2.3 Configure debugging switch 265
22.2.4 View debugging information 267
22.3 configuration SYSLOG 267
22.3.1 SYSLOG introduce 267
22.3.2 SYSLOG configuration 268
22.3.3 SYSLOG configuration example 269
Twenty-third chapters 270
Port loop 270
23.1 Profile 270
23.2 Protocol principle 271
23.2.1 Detection process 271
23.2.2 Recovery mode 271
23.2.3 Protocol security 271
23.3 Configuration introduction 272
23.3.1 Global configuration 272
23.3.2 Interface configuration 272
23.3.3 Display configuration 273
Twenty-fourth chapters 273
SNTP configuration 273
24.1 SNTP introduce 273
24.2 configuration SNTP 274
24.2.1 Default SNTP settings 274
24.2.2 Configuring SNTP Server address 274

SEC.RU | Короткий путь к информации
Скачано с sec.ru

24.2.3 Configure the SNTP sync clock interval 275
24.2.4 Configuring the local time zone 275
24.3 SNTP information display 276
Twenty-fifth chapters 277
OAM configuration 277
25.1 OAM introduce 277
25.1.1 Link performance monitoring 277
25.1.2 Remote fault detection 278
25.1.3 Distal loopback 278
25.2 configuration OAM 279
25.3 Typical configuration examples of OAM 280
Twenty-sixth 281
CFM configuration 281
26.1 CFM profile 281
26.1.1 Basic concepts of CFM 281
26.1.2 Various functions of CFM 285
26.2 Brief introduction of CFM configuration task 286
26.3 CFM base configuration 287
26.3.1 Enable CFM function 287
26.3.2 Configuration service instance 288
26.3.3 Configuration maintenance endpoint 288
26.3.4 Configuration maintenance intermediate point 289
26.4 Configure various functions of CFM 290
26.4.1 Configuration continuity detection function 290
26.4.2 Configuration loopback function 291
26.4.3 Configuring link tracking function 291
26.5 CFM display and maintenance 292
26.6 Typical configuration examples 293
Twenty-seventh chapters 298
IPv6 basic configuration 298
27.1 IPv6 profile 298
27.1.1 The characteristics of IPv6 protocol 298
27.1.2 IPv6 address introduction 300
27.1.3 IPv6 neighbor discovery protocol 303
27.1.4 IPv6 PMTU discovery 306
27.1.5 Protocol specification 306
27.2 IPv6 basic configuration task profile 307
27.3 Configure IPv6 basic functionality 307

SEC.RU | Короткий путь к информации
Скачано с sec.ru

27.3.1Configuring IPv6 unicast address 307
27.4 Configuring IPv6 neighbor discovery protocol 308
27.4.1 Configuring the parameters of the RA message 308
27.4.2 The number of sending neighbor request messages 311
27.5 IPv6 static routing configuration 312
27.6 IPv6 display and maintenance 312

First chapters

Introduction of CLI command line

This chapter gives a detailed description of the CLI command line interface，The main contents are as follows：

- Access switch CLI
- CLI mode introduction
- Introduction to command syntax
- Command line shortcuts
- History command

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.1 Access switch CLI

The CLI command line interface of the switch provides the interface for the user to manage the switch。The user can access the CLI command line interface of the switch through the Console port and the Telnet two terminals，The following are introduced separately。

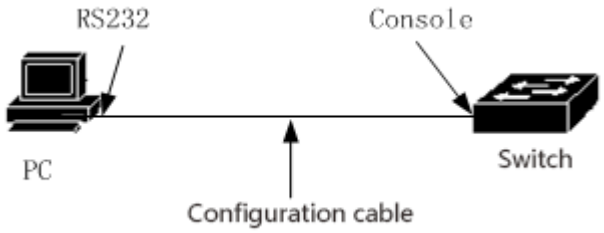
The main contents include：

- Users access CLI through Console port
- Users access CLI through TELNET

1.1.1 Users access CLI through Console port

The operating procedure is as follows：

First step：Connect the serial port of PC with the Console port of the switch by configuring the cable，The following diagram：



Second steps：Start the terminal emulation program on the PC machine (such as the super terminal of Windows)，Configuring communication parameters of terminal emulation program。The communication parameters of the terminal are configured as follows：

Baud rate：38400

Data bits：8

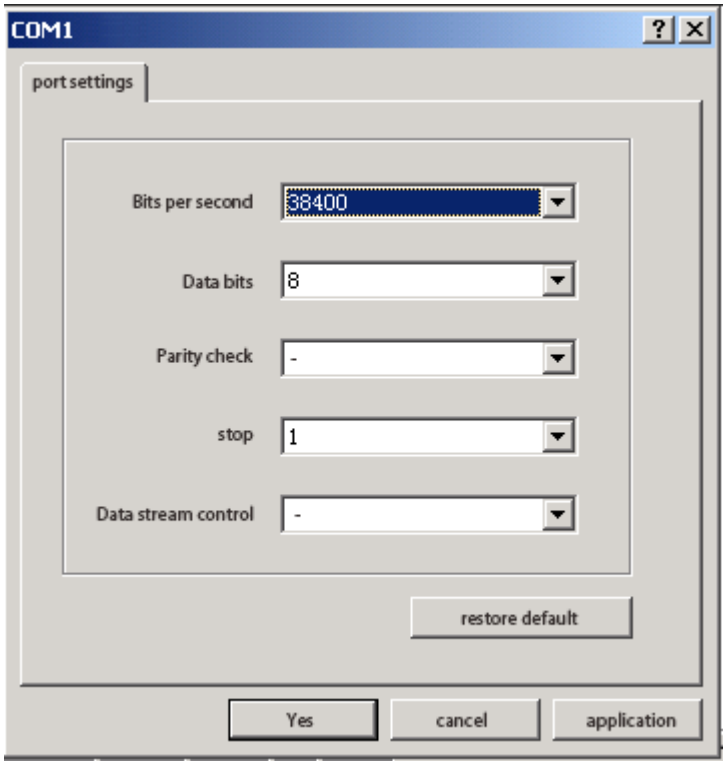
Parity check： nothing

Stop bit：1

Data stream control： nothing

The communication parameters configuration of the super terminal is shown below：

SEC.RU | Короткий путь к информации Скачано с sec.ru



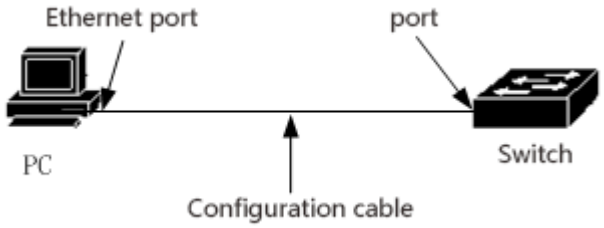
Third steps：Start switch，After the Switch is started, the CLI prompt will be displayed on the terminal (the default is Switch >)，Users can enter commands at this prompt，This allows the user to access the CLI of the switch。

1.1.2 Users access CLI through TELNET

The user can access the switch through the port of the switch。

The IP address of the port of the switch defaults to 192.168.0.1，The steps to access the switch through the port are as follows：

First step：Connect Ethernet port and switch port of PC through Ethernet cable。The following diagram：

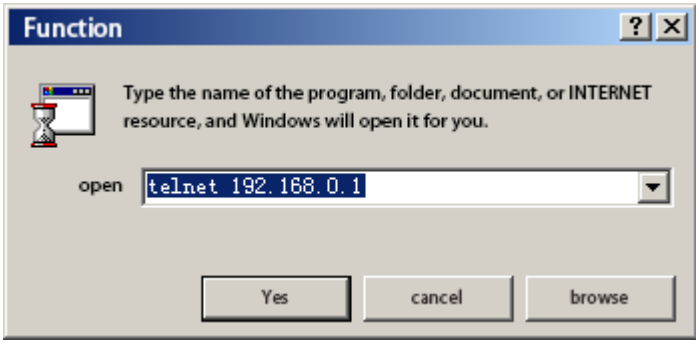


Second steps：Set the IP address of the Ethernet port of the PC machine，The IP address must be in the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

192.168.0.0/24 segment (such as IP address 192.168.0.100)。Judging the connectivity between PC and switch through Ping 192.168.0.1。

Third steps：If the PC is connected to the switch，Then Telnet 192.168.0.1 enters the Telnet terminal interface。The following diagram：



Fourth steps：If the system does not have a password, the Telnet interface goes directly to the CLI, and the CLI prompt appears (default is Switch >).；If the system sets the password, you need to enter the password on the Telnet interface to enter the CLI.

Two points should be paid special attention to：

- The IP address of the switch port is based on the VLAN three layer interface，Before accessing the switch，You must set the IP address of a VLAN interface，The default IP address of VLAN1 is 192.168.0.1，It can be used directly。The IP address of the VLAN interface can be configured through the Console port。
- The user accesses the switch through the port，You can connect PC and ports directly through Ethernet cable，You can also connect through a network，You just need PC to communicate with one of the VLAN switches。

1.2 CLI mode introduction

The main contents include：

- The role of CLI model
- Identification of CLI mode
- Classification of CLI patterns

SEC.RU | Короткий путь к информации Скачано с sec.ru

1.2.1 The role of CLI model

There are two main functions of the CLI model：

- Convenient classification of users，Prevent unauthorized users from using CLI illegally。

Users can be divided into two levels，That's the two category：Common users and privileged users。

Ordinary users can only see some of the running state of the switch，Use only display commands。

Privileged users can not only view the running state of the switch, but also maintain and configure the switch to change the behavior of the switch。

- Convenient for users to configure switches

Switches have a lot of configuration, and if you put all the configuration in one mode, it's very inconvenient for the user to use. To this end, the establishment of multiple modes on the CLI, the similar commands placed in a mode, user-friendly understanding and use. For example, put the commands associated with VLAN in the VLAN configuration mode.Put the interface related commands in the interface configuration mode。

1.2.2 Identification of CLI mode

The CLI prompt is the identity of the CLI mode，When the user is using CLI，By looking at the CLI prompt, you know the CLI model that you're currently in。

The CLI prompt consists of two parts，Part identifies the host，Another part identifies patterns。

The host part of the CLI prompt uses the hostname of the system，The host name of the system is configurable，the default is Switch，So the CLI prompt defaults to Switch，the CLI descriptor mentioned later generally uses the default host name。

The schema section in the CLI prompt is not configurable，each pattern has its own corresponding pattern string，some pattern strings are immutable，some pattern strings are mutable。If the pattern string of the VLAN configuration pattern is fixed, the pattern string of the interface configuration pattern is variable。

For example：

CLI prompt Switch# identifies privileged mode，Switch identifies the host, and # identification model。

The CLI prompt (config-ge1/1)# identifies the interface configuration mode and is configured with ge1/1 port，Switch identifies the host, and (config-ge1/1) # identification model。

The CLI prompt Switch(config-vlan2)# identifies the interface configuration mode，And configure the vlan2 interface，Switch identifies the host, and (config-vlan2) # identification model。

SEC.RU | Короткий путь к информации Скачано с sec.ru

1.2.3 Classification of CLI patterns

The CLI model is divided into four categories: general mode, privileged mode, global configuration mode and configuration sub pattern, while the configuration sub model is composed of many CLI modes.

Ordinary users can only access common patterns, and privileged users can access all of the CLI patterns。

Console and Telnet terminals first enter the common mode, enter the enable command in the normal mode, and successfully verify the password, then enter privileged mode。On the Telnet terminal, ordinary users can only stay in the ordinary mode and cannot enter privileged mode。Enter configure terminal in privileged mode，CLI mode enters global configuration mode。In global configuration mode, you can enter the relevant commands and enter each configuration sub mode。

The following table lists the main CLI modes of switches：

mode	description	Prompt	Entry mode command	Exit mode command
Common mode	Provides a display command to view the status information of the switch。	Switch>	Terminal first entry mode。	On the Console terminal, there is no exit mode command, and exit or quit command is used to exit the Telnet terminal on the Telnet terminal.
Privileged mode	In addition to providing the display command to view the status information of the switch, it also provides commands such as debugging, version update and configuration maintenance。	Switch#	Enter the enable command in the normal mode。	Returns to normal mode using the disable command. On the Console terminal, use exit or quit command to retreat to the normal mode, and use the exit or quit command to exit the Telnet terminal on the Telnet terminal.
Global configuration mode	Provides generic commands that cannot be implemented in	Switch(config)#	Enter the configure terminal	Use exit, quit, or end commands to exit to privileged mode.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	configuration sub patterns, such as configuring static routing commands.		command in privileged mode.	
Interface configuration mode	Provides commands for configuring ports and VLAN interfaces。	port：Switch(config-ge1/1)# VLANInterface：Switch(config-vlan1)#	Input in global configuration modeinterface <if-name>命令。	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.
VLAN configuration mode	Provides commands for configuring VLAN. For example, commands for creating and deleting VLAN。	Switch(config-vlan)#	In the global configuration mode, enter the VLAN database command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode。
MSTP configuration mode	Provides commands for configuring MSTP. For example, commands for creating and deleting instances of MSTP.	Switch(config-mst)#	In the global configuration mode, enter the spanning-tree MST configuration command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.
Terminal configuration mode	Provides commands for configuring Console and Telnet terminals, such as configuring timeout time for a terminal.	Switch(config-line)#	In the global configuration mode, enter the line vty command.	Use the exit or quit command to exit to the global configuration mode and exit with the end command to the privileged mode.

1.3 Introduction to command syntax

The main contents include：

- Command composition
- Parameter type

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Command syntax rules
- Command abbreviation
- Grammar help
- Command line error message

1.3.1 Command composition

The CLI command consists of two parts, the keyword and the parameter. The first word must be a keyword, and the latter word can be a keyword or a parameter, and the keywords and parameters can appear alternately。A command must have a keyword, but it can have no parameters。For example, the command write is only one keyword without parameter; the command show version has two key words without parameter; the command VLAN <vlan-id> has a key and a instance <instance-id> VLAN <vlan-id> command parameters; two and two keywords and keyword parameters and parameters appeared alternately.

1.3.2 Parameter type

CLI order parameters are divided into two types: mandatory and optional parameters。The input command must enter the required parameters, and optional parameters can enter can not enter。If the parameters of command VLAN in <vlan-id> is the required parameter in the input command when this parameter must be entered; and show interface [if-name] in the command parameter is optional in the input command, this parameter can be input, can not enter。

1.3.3 Command syntax rules

When describing commands with text, the following rules must be satisfied：

1）Keywords are directly represented by words。

Such as command show version。

2）Parameter must be enclosed with < >。

Such as command VLAN <vlan-id>

3）If it's an optional parameter，The parameters must be enclosed with [...]。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Such as command show VLAN [<vlan-id>]

For this situation，The parameter <> can be omitted and changed：

Command show vlan [vlan-id]

That is, the parameter vlan-id can be input, nor can it be input。

If this is a required parameter, the parameters cannot have []。

4）If you have multiple keywords or parameters, you must choose one，Enclose a number of keywords or parameters with {}，Between multiple keywords or parameters with | separated，| required before and after a space。

If multiple keywords required command：

spanning-tree mst link-type {point-to-point | shared}

Between point-to-point and shared, you have to choose one。

A number of parameters required command：

no arp {<ip-address> | <ip-prefix>}

Keywords and parameters mixed with the necessary command：

Show spanning-tree mst {none|instance <0-15>}ng

5）If multiple keywords or parameters are selected one，Enclose a number of keywords or parameters with [...]，Between multiple keywords or parameters with | separated，| required before and after a space。

The following commands：

debug ip tcp [recv | send]

Keywords recv and send can choose one，You can't choose either。

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6）If you have a keyword or parameter or a set of keywords or parameters, you can repeat the input, and add the symbol "*" after the keyword or parameter"。

For example, the ping command：

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*

-j <count> <ip-address>* --- Multiple IP addresses can be repeatedly entered

-k <count> <ip-address>* --- Multiple IP addresses can be repeatedly entered

The entire option can also be repeated。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6）Parameters are represented by descriptors of one or more words. If it is more than one word, each word is separated by sign "-", and each word is lowercase。

Correct parameter representation：<vlan-id>，<if-name>，<router-id>， <count> etc.

Wrong parameter representation：<1-255>，<A.B.C.D>，<WORD>，<IFNAME> etc.

1.3.4 Command abbreviation

When the user enters the command on the CLI interface, the keyword of the command can be

1.3.5 Grammar help

The CLI command line interface is set with syntax help to support each level command and parameters：

1）Direct input in a CLI mode? key，On the terminal, the first keyword and its description of all commands under this mode are listed。for example Switch(config)#?。

2）Enter the preceding part of a command，Then enter the space and then enter key，On the terminal, all the keywords or parameters of the next level are listed and their descriptions are given。for example Switch#show ?。

3）Enter an incomplete keyword and enter it directly? Key, all keywords and their descriptions that match the input prefix are listed on the terminal。for example Switch#show ver?。

4）Enter the preceding part of a command, and then enter the space, and then enter the Tab key, the terminal will list all the keywords at the next level, the next level if it is the parameter, will not be listed。

5）The input is not a complete keyword directly enter the Tab key, if there is only one keyword and the input prefix matching, is directly filled, if there are multiple keyword matching with the input prefix, all matching keyword lists in the terminal.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.3.6 Command line error message

If the command entered by the user does not pass the syntax check, the error message will be displayed on the terminal. The common error information is shown in the following table。

error message	Wrong reason
Invalid input or Unrecognized command	No matching keywords found。 Parameter input incorrect。 Too many keywords or parameters are entered。
Incomplete command	Command input is incomplete, and the keyword or parameter is not entered。
Ambiguous command	The keyword input is incomplete, and multiple keywords match the input prefix。

1.4 Command line shortcuts

The main contents include：

- Line edit shortcut key
- Display command shortcut key

1.4.1 Line edit shortcut key

The CLI command line interface supports the line editing shortcut function, and the line edit shortcut can facilitate the input and editing of the CLI command. When the user enters or edits commands, you can use the line edit shortcut to accelerate the command input。The following table lists all the line edit shortcuts and functions to implement：

Shortcut key	function
Ctrl+p Or up arrow	The last command
Ctrl+n Or down arrow	Next command
Ctrl+u	Delete entire rows
Ctrl+a	The cursor back to the
Ctrl+f Or to key	The cursor moves to the right

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Ctrl+b Or left key	Move the cursor to the left
Ctrl+d	Delete the character at the cursor
Ctrl+h	Delete the previous character of the cursor
Ctrl+k	Delete all characters at the cursor and cursor
Ctrl+w	Delete all characters before cursor
Ctrl+e	Move the cursor to the end of the line
Ctrl+c	nterrupt, do not execute command line. If CLI is in the global configuration mode or the configuration sub mode, CLI will retreat to privileged mode; if CLI is in normal mode or privileged mode, the CLI schema remains unchanged, but CLI starts another new line.
Ctrl+z	Same function as Ctrl+c。
Tab	Enter this keyword when you enter an incomplete keyword, and if there is a keyword that matches the entered prefix, the keyword is padded; if more than one keyword matches the entered prefix, all matching keywords are listed; If there is no keyword match, this key is invalid。

Be careful：some ConsoleOn the terminal↑、↓、→、←The key is unavailable。

1.4.2 Display command shortcut key

The commands that start with the show keyword are all display commands. Some display commands can not be displayed in one screen because of the display of a lot of contents, and the terminal provides the function of screen display。After displaying a screen, the terminal waits for user input to determine the subsequent processing. The following table lists the shortcut keys for displaying commands and their functions。

Shortcut key	function
Space	Display next screen
Enter	Show next line
Ctrl+c	Break the execution of the command and exit to the CLI mode。
Other keys	Same function as Ctrl+c。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.5 History command

The CLI command line interface supports the history function of commands. It can remember the 20 historical commands that the user recently used, and save the commands that the user recently typed。You can use the show history to display commands that have been entered，You can also use it Ctrl+p,Ctrl+n or ↑、↓Key to select history commands。The history command function makes it easy for users to enter commands。

second chapters

System management configuration

Before configuring the related functions of the switch, you need to master the basic configuration of the system management and maintenance of the switch. This chapter describes the basic configuration of these system management and maintenance, including the following：

- System security configuration
- System maintenance and debugging
- Configuration file management
- Software version upgrade

2.1 System security configuration

In order to prevent illegal users from invading switches, the system provides several security measures for system management, mainly including：

- Multi-user management control
- TACACS+ authentication authorization
- Anonymous user password control
- Enable password control
- TELNET service control
- SNMP service control

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- HTTP service control
- SSH service control

2.1.1 Multi-user management control

Multi user management not only ensures the security of the switch system, but also provides the ability for multiple users to manage and maintain the switch simultaneously。Multi user management by giving each user a username, password and authority to ensure the safety of the system, the user first needs to authenticate a user name and password in the access switch, only the user name and password are correct and can be verified by the same。The user can access the switch after verification, but the user's permissions limit the scope of the user's access to the switch。

Multi user management divides users' rights into two levels: ordinary users and privileged users。Ordinary users can only stay in the ordinary mode of the CLI command line interface, and can only use the display command to query the information of the switch。Privileged users can access all the modes of the CLI command line interface, and all commands provided by CLI can be used to query the information of the switches and to maintain and manage the switches。

The multi user management function is only applied to the Telnet terminal, and the Console terminal is not controlled。When you use Console terminal to access the switch, you don't need to verify the username and password, and the user can access the CLI directly。And through the Telnet terminal to access the switch need to verify the user name and password, only the user name and password are verified before they can access the CLI。

There is no user in the switch default, that is to say, the user management function is not enabled by default. At this point, the login Telnet terminal does not need to verify the username and password。When a user name is added to the command, the multi user management function is enabled. At this point, the Telnet terminal needs to verify the username and password。When commands are used to delete all users, the multi-user management function is closed and the system returns to the default state。

The commands associated with multi-user management are as follows：

command	describe	CLI mode
username <user-name> password <key> {normal | privilege}	Add a user, if the specified user already exists, then modify the password and permissions of the user。The first parameter is the user name, the	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	second parameter is the password, the option represents the authority, the normal represents the ordinary user, and the privilege represents the privileged user.	
no username [user-name]	Delete one or all of the users。If you don't input a parameter, it means deleting all users, if the input parameter represents the user who deletes a specified user name。	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of multi user management。	Privileged mode

2.1.2 TACACS+ authentication authorization

TACACS+ authentication and authorization provide more strict user rights management, not only to verify the legitimacy of users, but also to authorize the command。After opening the TACACS+ authentication, the user first needs to verify the username and password through the TACACS+ server when accessing the switch. Only when the user name and password are correct and consistent can they pass the verification。The user can access the switch after verification。

TACACS+ also divides the user's permissions into two levels: ordinary users and privileged users。Ordinary users can only stay in the ordinary mode of the CLI command line interface, and privileged users can access all the patterns of the CLI command line interface。On the basis of permission level, it also sets the command execution authority, and the user enters a command (except enable, end and exit), which must be verified on the TACACS+ server, and the verification failure will not be executed。

The TACACS+ authentication and authorization function is only applied to Telnet and SSH terminals, and does not control the Console terminal。The user name and password need to be verified when accessing the switch through the Telnet or SSH terminal. Only the user name and password are verified before they can access the CLI。When SSH is accessed, only privileged users can pass it。TACACS+ authentication is also applied to WEB login, but only verify password privilege permissions, do not command authorization。

By default, the switch TACACS+ is not enabled, the Telnet, SSH or WEB landing using multi user management function, open the TACACS+ function, user management function can continue to configure, but not the actual use。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The TACACS+ authentication authorization related commands are as follows：

command	describe	CLI mode
tacacsplus enable	Open the TACACS+ function	Global configuration mode
tacacsplus disable	Close TACACS+ function	Global configuration mode
tacacsplus host A.B.C.D	Configuring the master server address, it is recommended to use Cisco's ACS	Global configuration mode
tacacsplus key WORD	Configure the shared key that encrypts the data and must be consistent with the configuration on the server	Global configuration mode
tacacsplus auth-type (PAP|CHAP)	Select authentication methods, including PAP and CHAP. Among them, PAP is the default mode, the field encapsulates the password, and CHAP encapsulates the password MD5 check code.	Global configuration mode
show tacacsplus	View TACACS+ configuration information	Global configuration mode
no tacacsplus host	Clear master server address	Global configuration mode
no tacacsplus key	Clearing shared keys	Global configuration mode

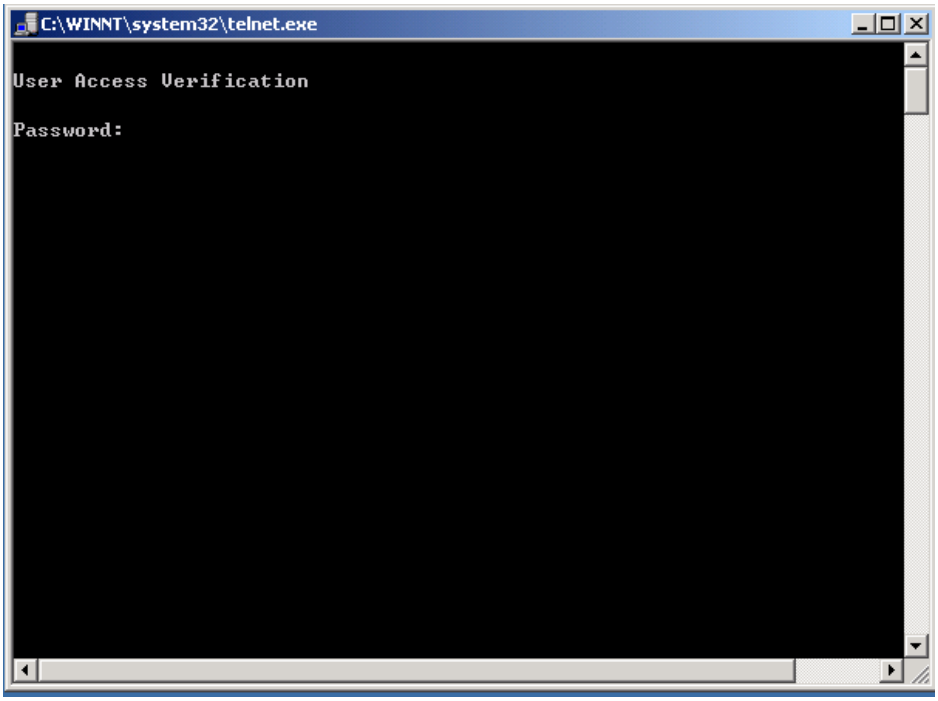
SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.1.3 Anonymous user password control

When multi-user management is not enabled, the user login Telnet terminal does not need to check the user name and password, you can directly access the Telnet CLI。In order to improve the security of the system, the switch adds anonymous user (admin) password to control Telnet and Web。When the switch is set the anonymous user password and user management is not enabled to do an anonymous user password check user login Telnet terminal and Web, only to enter the correct password to be able to access CLI and Web page。If the system uses multi-user management, anonymous user password will not be effective, the user access to the Telnet terminal and Web does not do anonymous user password check, but do more user management user name and password check.

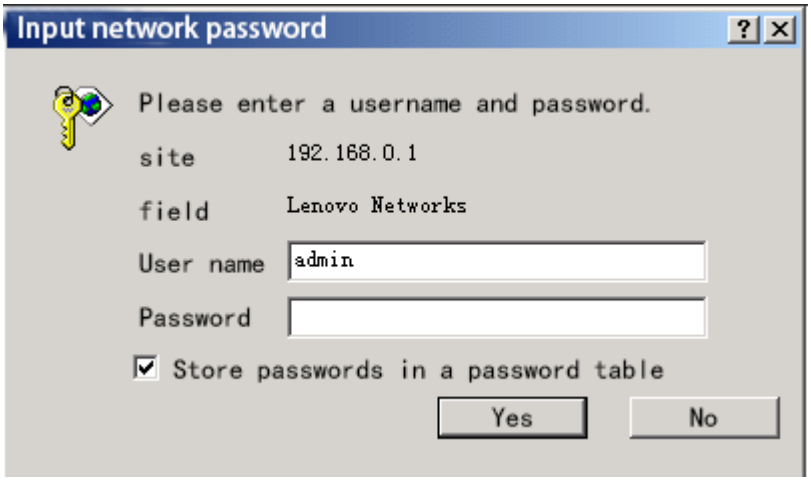
There is no anonymous user password in the switch. In this case, the user does not need to verify the anonymous user password when accessing the Telnet terminal and the Web。

The figure below is the user login Telnet terminal interface, enter anonymous user password at this interface。



SEC.RU | Короткий путь к информации
Скачано с sec.ru

The diagram below is the dialog box for the user to log in to Web. In this dialog box, the anonymous user admin and password are entered。



The associated commands for anonymous user passwords are listed below：

command	describe	CLI mode
password <key>	Setting anonymous user password。	Global configuration mode
no password	Clear anonymous user password。	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the anonymous user password.	Privileged mode

Be careful：For the security of the system, the administrator needs to set the anonymous user password of the system。

2.1.4 Enable password control

The Enable password is used to control the switch from normal mode to privileged mode，Before Enable password authentication，The user can only view the information of the switch，After the Enable password is verified, it is possible for the user to configure and maintain the switch。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Enable password does not depend on the user, any user login to the Console terminal or Telnet terminal, if you want to enter the privileged mode must verify the Enable password, if the authentication is not successful, you can only stay in normal mode。

In the normal mode, enter the Enable command, the terminal will prompt the user to enter the password, then the user can enter the Enable password, if the password verification is successful, the terminal into the privileged mode, otherwise, stay in the normal mode, for ordinary users whether the password is valid Can not enter the privilege mode。

Enable password defaults to empty, in this case, in the normal mode, enter the Enable command, the terminal does not prompt the password, enter the privileged mode directly。

The related commands of the Enable password are listed below：

command	describe	CLI mode
enable password <key>	Set the enable password of the system。	Global configuration mode
no enable password	Clear the enable password of the system, enable password is empty	Global configuration mode
show running-config	View the current configuration of the system, you can see the configuration of the enable password。	Privileged mode
enable	The interactive command verifies the enable password of the system. After the verification is successful, the terminal enters the privileged mode。	Normal mode

Note: for the security of the system, the administrator needs to set the Enable password of the system。

2.1.5 TELNET service control

In some cases, administrators do not need to switch the remote management, only through the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Console terminal to switch on the line in the local administration, at this time in order to improve the security of the system, to prevent illegal users remote login Telnet terminal, the administrator can shut down the Telnet service。The default Telnet service is open。

The related commands of Telnet service control are as follows：

command	describe	CLI mode
security-manage telnet enalbe	Open Telnet service。	Global configuration mode
security-manage telnet disable	Closing Telnet services。	Global configuration mode
security-manage telnet number <1-100>	The number parameter ranges from 1 to 100, and defaults to 5。	Global configuration mode
security-manage telnet access-group <1-99>	Specify a ACL group and open the source IP address control. If the specified ACL group does not exist or is not a standard ACL group, then the source IP address is not controlled。	Global configuration mode
no security-manage telnet access-group	Close source IP address control。	Global configuration mode
show security-manage	You can see the configuration of the service control。	Privileged mode

2.1.6 SNMP service control

The SNMP service control can open / close the SNMP service, and also control the IP address of the access switch by ACL。

The related commands of SNMP service control are as follows：

command	describe	CLI mode
security-manage snmp enalbe	Open SNMP service。	Global configuration mode
security-manage snmp disable	Closing SNMP services。	Global configuration mode
Security-manage snmp access-group <1-99>	Specify a ACL group and open the source IP address control. If the specified ACL group does	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	not exist or is not a standard ACL group, then the source IP address is not controlled。	
no security-manage snmp access-group	Close source IP address control。	Global configuration mode
show security-manage	You can see the configuration of the service control。	Privileged mode

2.1.7 HTTP service control

The HTTP service control can open / close the HTTP service, and also control the IP address of the access switch by ACL。

The related commands of HTTP service control are as follows：

command	describe	CLI mode
security-manage http enalbe	Open HTTP service。	Global configuration mode
security-manage http disable	Closing HTTP services.	Global configuration mode
security-manage http access-group <1-99>	Specify a ACL group and open the source IP address control. If the specified ACL group does not exist or is not a standard ACL group, then the source IP address is not controlled。	Global configuration mode
no security-manage http access-group	Close source IP address control。	Global configuration mode
show security-manage	You can see the configuration of the service control。	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.1.8 SSH service control

The traditional network service program, such as: FTP, pop and telnet are not safe in nature, because they use plaintext passwords and data transfer on the network, people have an ulterior motive is very easy to intercept these passwords and data。Moreover, the security verification of these service programs is also vulnerable, that is very easy to "man" (man-in-the-middle) in this way the attack。The so-called "middleman" attack, is the "middleman" to impersonate the real server to receive the data you send to the server, and then pretend to be you pass the data to the real server。When the data transfer between the server and you is done by the middleman, there will be a serious problem。By using SSH, you can encrypt all the data transmitted, so that "middleman" this attack can not be achieved, but also to prevent DNS spoofing and IP spoofing。The use of SSH, there is an additional benefit is that the transmission of data is compressed, so you can speed up the transmission speed. SSH has a lot of features, it can replace Telnet, but also for FTP, PoP, and even for PPP to provide a secure "channel"。

2.2 System maintenance and debugging

The basic functions of system maintenance and debugging include the following contents：

- Configure the host name of the system
- Configuring the system clock
- Configure terminal timeout attributes
- System reset
- View system information
- Network connectivity debugging
- Detecting line distance
- Traceroute debugging
- Telnet client
- UDLD configuration

2.2.1 Configure the host name of the system

The host name of the system is used to identify the switch, which facilitates the user to distinguish between different switches, while the host name of the system is part of the CLI prompt of the terminal。The host name of the system defaults to Switch。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The commands of the host name of the system are as follows：

command	describe	CLI mode
hostname <name>	Set the host name of the system。	Global configuration mode
no hostname	Clear the host name of the system, that is, the hostname returns to the default value Switch。	Global configuration mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the host name of the system。	Privileged mode

2.2.2 Configuring the system clock

The switch provides the function of real time clock, the current clock can be set by the command, and the current clock can also be viewed。The system clock is powered by the internal, so that the real time clock can be operated continuously when the system is powered off, and the system does not need to reset the clock after starting。

The switch has been set up in the factory clock, the user does not need to set again, if the user found that the time is not allowed, the user can reset the clock。

The related commands of the system clock are as follows：

command	describe	CLI mode
set date-time <year> <month> <day> <hour> <minute> <second>	Set the current clock of the system, you need to input parameters of year, month, day, hour, minute and second。	Privileged mode
show date-time	The current clock of the display system。	Normal mode，Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2.3 Configure terminal timeout attributes

For the security of the terminal, when the terminal has no key input, more than a certain period of time, the terminal will do the exit processing。Console terminal and Telnet terminal exit processing is not the same, for the Console terminal, when the terminal timeout, CLI mode back to normal mode, for the Telnet terminal, when the terminal timeout, Telnet connection is interrupted, Telnet terminal exit。

The terminal timeout time is 10 minutes by default, and the user can also set the terminal without timeout。

The related commands for terminal timeout are listed below：

command	describe	CLI mode
exec-timeout <minutes> [seconds]	Set terminal timeout time, if the parameters are 0, indicating that the terminal will never timeout。	Terminal configuration mode
no exec-timeout	Set the terminal timeout time back to the default, that is, 10 minutes。	Terminal configuration mode
show running-config	View the current configuration of the system, you can see the terminal timeout configuration。	Privileged mode

2.2.4 System reset

The system provides a reset method：

- Reset switch

The related commands of system reset are as follows：

command	describe	CLI mode
reset	Reset switch。	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2.5 View system information

The system provides rich display commands to see the system running status and system information, here only lists a few commonly used system maintenance display commands, the following table：

command	describe	CLI mode
show version	Display system version number and compile time of executable file connection。	Normal mode，Privilege mode
show snmp system information	Display the basic information of the system, including how long the system started after the operation。	Normal mode，Privilege mode
show history	Displays the list of recently entered commands on the CLI command line。	Normal mode，Privilege mode

2.2.6 Network connectivity debugging

In order to debug the connectivity of the switch with another device in the network, you need to ping the switch on the switch and ping the IP address of the peer. If the switch receives a ping reply from the other party, it indicates that the two ends are connected. Both ends can not communicate。

The switch not only implements the ping command, but also supports many options on the ping command. The user uses these options to make more precise and complex debugging。

The ping command follows the table：

command	describe	CLI mode
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*	It can be used without any options, or with one or more options. If you do not have any options, it is the simplest ping command。When the command is executed, you can type the execution of the Ctrl+c interrupt command。	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2.7 Detecting line distance

command	describe	CLI mode
show cable-diag interface IFNAME	Detection of electrical cable distance	Privileged mode

2.2.8 Traceroute debugging

In order to debug the intermediate devices that the switch communicates with another device in the network, it is necessary to implement the trace-route command on the switch。When using the trace-route command on the switch, specify the IP address of the other party. When the command is executed, the path through the middle will be displayed.。

The switch not only implements the trace-route command, but also supports many options on the trace-route command, which allows users to make more precise and complex debugging by using these options。

The trace-route command follows the table：

command	describe	CLI mode
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	You can use one or more options when you're using it without any options。If you don't have any options, it's the simplest trace-route command。When the command is executed, you can type the execution of the Ctrl+c interrupt command。	Privileged mode

2.2.9 Telnet client

The series switches provide Telnet client functions, and users can access other devices remotely through the Telnet client。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
telnet <ip-address>	The parameter is the IP address of the target device	Privileged mode

2.2.10 UDLD configuration

UDLD （UniDirectional Link Detection）：Is a two-layer protocol that monitors the physical configuration of an Ethernet link using fiber or twisted pair connections. When a unidirectional link (only one direction is transmitted, for example, I can send you data, Receive, but you send me the data I can not receive), UDLD can detect this situation, close the corresponding interface and send a warning message。Unidirectional links can cause a lot of problems, especially spanning trees, which may cause loops。Note: UDLD requires both ends of the link to be supported for normal operation。

UDLD supports two modes of work: common (normal) mode (default) and radical (aggressive) mode UDLD supports two modes of work: common (normal) mode (default) and radical (aggressive) mode UDLD supports two modes of work: common (normal) mode (default) and radical (aggressive) mode UDLD supports two modes of work: common (normal) mode (default) and radical (aggressive) mode。

General (normal) mode: in this mode, UDLD can detect unidirectional links and label ports as undetermined states to generate system logs，In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended period of time.

Aggressive mode: In this mode, UDLD can be detected by a unidirectional link. And will try to rebuild the link, continuous transmission of 8 seconds UDLD message, if there is no UDLD echo response, this port will be placed in the errdisable state。

command	describe	CLI mode
udld enable	Global enable UDLD function	Global configuration mode
udld message time <time>	UDLD message transmission interval	Global configuration mode
udld port	Port enable UDLD	Interface configuration mode
udld aggressive	Enable port radical mode, default normal mode	Interface configuration mode
show udld <ifname>	View the port UDLD information	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.3 Configuration file management

The configuration is divided into the current configuration and the initial configuration. The current configuration refers to the configuration of the system runtime, the existence of the system memory, and the initial configuration is used to start the system configuration, there is the system FLASH, that is, the configuration file。When the user executes the relevant command to modify the current configuration of the system, only the implementation of the save command before the current configuration to write to the initial configuration for the next system to start。When the system is started, the system does not have any configuration. The current configuration information of the system is the same as the initial configuration information.。

The current configuration and the initial configuration using the same format, are command-line text format, very intuitive, easy for users to read。The format of the configuration file has the following features：

- The configuration file is a text file。
- All the commands are saved。
- Only save non default configurations and do not save the default configuration。
- The commands are organized in the CLI mode, and the commands in the same CLI mode are organized together to form a segment separated by a "!"。For commands within the global configuration mode, organize commands with the same function or function to be separated by "!"。
- For a command that configures a subpattern, there is a space before the command, and no commands are required for commands in the global configuration mode。
- With "end" as the end of the configuration。

Configuration file management mainly includes the following：

- View configuration information
- Save configuration
- Delete configuration file
- Download configuration files

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.3.1 View configuration information

View configuration information including viewing the current configuration and initial configuration of the system。The initial configuration is actually in the FLASH configuration file, when the FLASH does not exist in the configuration file, the system starts using the default configuration, this time if you view the initial configuration of the system, the system will prompt the configuration file does not exist。

The commands for viewing configuration information are shown in the following table：

command	describe	CLI mode
show running-config	See the current configuration of the system。	Privileged mode
show startup-config	See the initial configuration of the system。	Privileged mode

2.3.2 Save configuration

When the user changes the current configuration of the system, these configurations need to be saved to the configuration file, so that the next configuration after the start still exist, otherwise, after the restart these configuration information is lost。Save configuration is to save the current configuration to the initial configuration。

Save the configuration command as follows：

command	describe	CLI mode
write	Save current configuration。	Privileged mode

Note: You need to use this command to save the configuration after configuring the switch. Otherwise, the configuration will be lost after the system reboot.。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.3.3 Delete configuration file

When the user wants to return to the initial configuration of the system default configuration can be deleted when the configuration file, the impact on the current configuration did not delete the configuration file, if you go back to the default configuration of the current configuration to the system, you need to restart the switch。Users must be cautious when deleting configuration files, otherwise the configuration will be lost。

The commands for deleting configuration files are as follows，

command	describe	CLI mode
delete startup-config	Delete the configuration file of the system。	Privileged mode

2.3.4 Download configuration files

In order to configure the security of the file, the user can use the command to upload the configuration file to the PC to do the backup, when the system configuration is missing or modified to return to the original configuration, you can download the original configuration file from the PC To the switch, download the configuration file after the system's current configuration has no effect, you must restart the switch after the configuration will take effect。WEB can also be configured to upload and download files, specific operations can refer to the WEB manual。

The commands downloaded from the configuration file are as follows：

command	describe	CLI mode
upload configure <ip-address> <file-name>	Upload the configuration file to the PC machine, the first parameter is the IP address of the PC machine, and the second parameter is the file name of the configuration file stored on the PC machine。	Privileged mode
download configure <ip-address> <file-name>	The configuration file is downloaded to the PC, the first parameter is the PC's IP address, the second parameter is the configuration file stored on the PC file name。	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The configuration file is downloaded and used to the TFTP protocol. The TFTP client software is run on the switch and the TFTP server software is run on the PC server。The operating steps downloaded from the configuration file are as follows：

First step： Build network environment。

Second steps： Start the TFTP server software on the PC, and set the directory stored in the configuration file。

Third steps： Save configuration on switch。

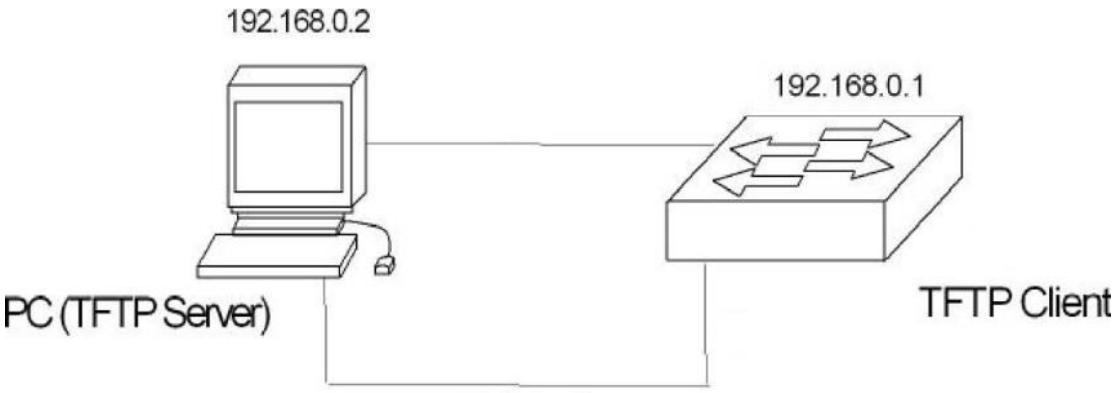
Fourth steps： The configuration file upload command is executed on the switch, and the configuration files are backed up to the PC。

Fifth steps： When the switch needs the configuration file on the PC machine, the configuration file download command is executed on the switch, and the configuration file on the PC machine is downloaded to the switch。

Sixth steps：To make the configuration effective, the switch must be restarted。

Sample： A switch that has been configured with VLAN and interface addresses, which needs to be downloaded on the configuration file。

First step：Build the following network environment。

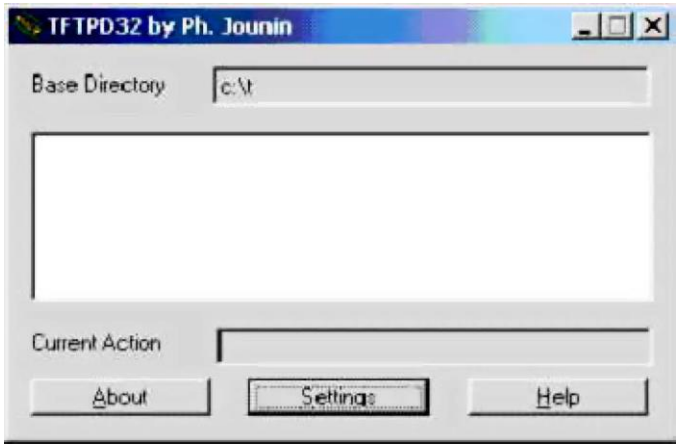


The configuration port of the switch is connected to a configuration terminal through the cable and connected with a PC through the network cable。Install TFTP Server in PC, configure Ethernet port IP address of PC, assume the IP address of PC is 192. 168.0.2。Then, configure the IP address of the switch, where the IP address of the switch is assumed to be 192.168. 0.1 to ensure the connectivity between the PC and the switch。

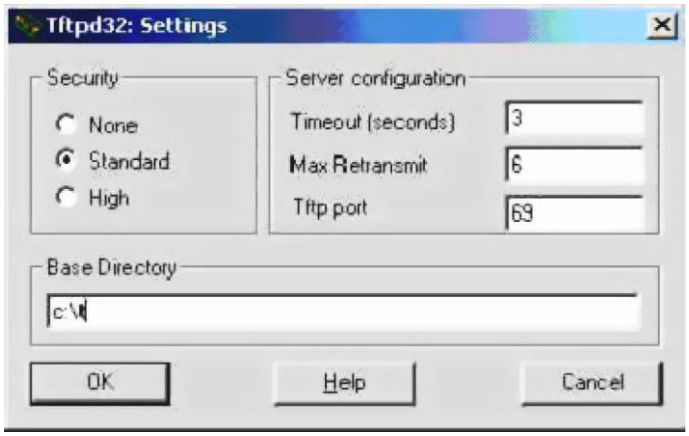
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Second steps：Start TFTP Server, configure TFTP Server parameters。

Run TFTP Server, the window interface as below：



Then, set the directory of the backup configuration file. The specific operation is, click the [Settings] button, set the interface, the following chart：



Enter the file path in "Base Directory". Click the [OK] button to confirm。

Third steps：Execute the write command on the switch and save the current configuration to the configuration file。

Fourth steps： To back up a file to a PC, run the Switch # upload configuration 192.168.0.2 beifen.cfg。

Fifth steps：If necessary, download the backup file to the switch and execute the command

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch#download configuration 192.168.0.2 beifen.cfg。

Sixth steps： If you want to download the configuration file to be effective, you must restart the switch, execute the command Switch#reset。

2.4 Software version upgrade

switches support online update of software versions. The upgrade is done by tool TFTP。

The main contents are as follows：

- Software version upgrade commands
- Software upgrade process

2.4.1 Software version upgrade commands

Upgrade the image file of the switch in global configuration mode. The commands are as follows：

download image <ip-address> <file-name>

Where <ip-address> is the IP address of the PC running the TFTP server and <file-name> is the image file name saved on the TFTP server。

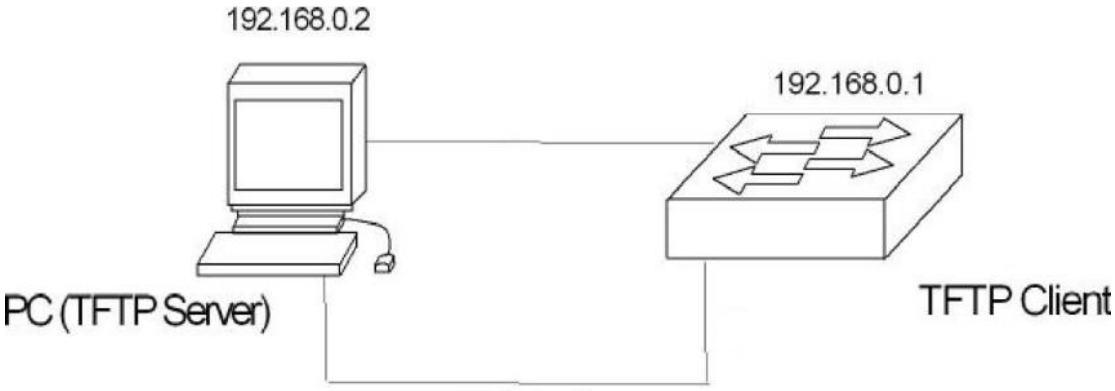
In the process of upgrading can not power, or switch the image file may be damaged and cause the switch can not start. After the download is complete, you need to restart the switch to run the newly downloaded image file program。The whole upgrade process takes a few minutes. Please be patient。

2.4.2 Software upgrade process

Update the image file steps as follows：

First step：Building upgrade environment。As shown in the following picture。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

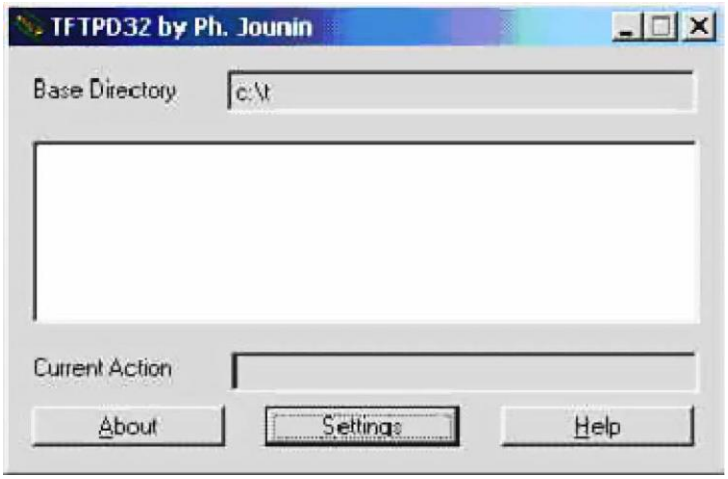


The construction process is as follows：

- Connect the console port of the switch to a console terminal (PC)。
- Install TFTP Server on PC。
- Copy the new image file to a path of PC, where the path is assumed to be c:\t；
- Configure the Ethernet port IP address of PC, where the IP address of PC is assumed to be 192.168.0.2 。
- Configure the IP address of the switch, where the IP address of the switch is assumed to be 192.168.0.1。

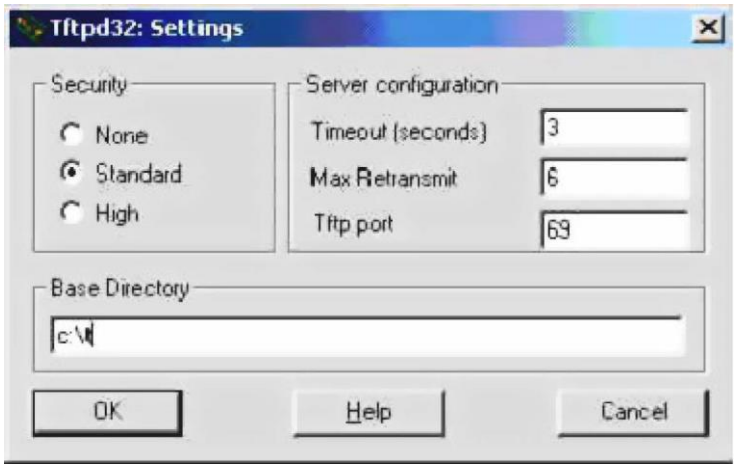
Second steps：Run TFTP Server and configure the TFTP server。

First： Run TFTP Server. TFTPD32 window interface as shown below：



Then： Setting the TFTP Server file directory。After you start TFTP Server, reset the TFTP Server file directory and copy the image files that you want to load into this directory。The specific operation is, click the [Settings] button, there TFTPD32 settings interface, as shown below。

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Enter the file path in the "Base Directory". Click the [OK] button to confirm。

Third steps：Upgrade file。

First：Connect the port of the switch to the PC of the TFTP Server program through the Ethernet network. The ping command is used to check the connection between the host and the switch。

Then：Enter the command at the super terminal Switch# prompt：

Switch# download image 192.168.0.2 switch.img，Enter and wait for the upgrade file to finish。

Software is updating. Please wait and down't powerdown!

……

Updating is completed. Do you wish to reset?[Y/N]

After the file transfer is completed, the system will indicate whether you need to restart the switch；In general, we recommend that you choose 'Y' to restart the switch, because the system upgrade can only take effect after restarting；If your configuration file is not saved, you can choose "N" first, do not restart; complete the disk and other operations, then restart the switch。

Switch#

note：

The switch can not be switched off during the upgrade process.

Fourth steps： Reboot。

Switch# reset

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Third chapters
port configuration

This chapter introduces the port related configuration, mainly including the following contents：

- Common configuration for ports
- Configuration MIRROR
- Configuring STORM-CONTROL
- Configuring STORM-CONSTRAIN
- Configuring FLOW-CONTROL
- Configuring port bandwidth
- Configuring TRUNK
- Configure super large frame
- Configuring redundant ports
- Configuring LLDP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.1 Common configuration for ports

The administrator can switch off the port by configuring the access port under the control port of the switch. If the user is not allowed to access the network under the port, the administrator can turn off the port。This section describes the general configuration of the port, including：

- Opening and closing ports
- Port rate configuration
- Display port information

3.1.1 Port rate configuration

The default rate configuration for all ports is adaptive (autonegotiate)。

The following command configures the port rate in the interface configuration mode：

speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }

autonegotiate--- self-adaption

full-1000------- Full duplex Gigabit

full-100-------- Full duplex fast

full-10 -------- Full duplex ten trillion

half-100-------- Half duplex Gigabit

half-10--------- Half duplex ten trillion

For example, the rate of port 1/1 is configured by full duplex 100M：

Switch(config-ge1/1)# speed full-100

3.1.2 Display port information

The following command displays information about one or more ports in common mode or privileged mode：

show interface [if-name]

For example, display port 1/1 information：

Switch# show interface ge1/1

For example, displays all ports information：

Switch# show interface

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.2 Configuration MIRROR

The port mirroring is a very useful function for monitoring the flow of packets received and sent by one or more ports. It can use mirroring ports to monitor packets received and sent from one or more ports。switches support port mirroring capabilities, mirroring the port's ability to monitor incoming data from other ports and the data that goes out. A mirrored port can monitor multiple ports at the same time。This section focuses on the configuration of MIRROR, including the following：

- Configuration of the MIRROR listen on port and is listening on port
- Display the configuration of MIRROR

3.2.1 Configuration of the MIRROR listen on port and is listening on port

When the administrator configures the monitoring port, you need to enter the interface configuration mode to set up the monitored port. For example, setting port ge1/1 monitoring port ge1/2, you need to enter the port ge1/1 and type the command：

Switch(config-ge1/1)# mirror interface ge1/2 direction both

At this point, the port ge1/1 is set to the listening port, and the ge1/2 is set to the listening port。

The command to set up the monitored port is as follows：

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

At this time, ge1/1 port is set to monitor port, <if-name> is set to be listening port, while behind the {both receive transmit} | | pointed out the direction of monitoring：Receive represents the received packets; the transmit monitors the packets sent; the both monitors all packets sent and received. such as：

Switch(config-ge1/1)#mirror interface ge1/2 direction both

Represents the sending and receiving packets of the port ge1/1 monitoring port ge1/2。

If you want to set multiple monitored ports, you need to execute multiple commands。

In the interface configuration mode, the administrator can cancel the monitored port, and the command is as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-ge1/1)#no mirror interface <if-name> direction { receive | transmit}

When the <if-name> is no longer listening port, {receive | transmit} pointed out the direction is not listening：Receive indicates that the packet is not monitored; transmit indicates that the packet is not monitored。such as：

Switch(config-ge1/1)# no mirror interface ge1/2 receive

Indicates that the port ge1/1 no longer listens to the packets received by the port ge1/2。

When all the monitored ports are canceled, the listening port will also be cleared。

3.2.2 Display the configuration of MIRROR

The administrator can view the configured MIRROR configuration through the following command in normal mode or privileged mode：

Switch# show mirror

need to pay attention to the following points：

- A port can not be set as a listening port and a listening port simultaneously。
- There are only one port to monitor, but there are multiple ports to be monitored。

3.3 Configuring STORM-CONTROL

In real life, a NIC card with a high rate of unicast, multicast, broadcast packets can make the network failure, in this case, the switch on the suppression function is particularly important, it can prevent the packet into the Network is congested, all ports of the switch support the suppression of broadcast packets, multicast packets, and DLF packets.。

This section gives a detailed description of the configuration of STORM-CONTROL, including the following：

- Default configuration
- Broadcast suppression configuration
- Multicast suppression configuration
- DLF suppression configuration
- Inhibition rate configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Display STORM-CONTROL configuration

3.3.1 Default configuration

The switch supports setting broadcast, multicast, DLF switches for each port separately, and the three setting has a separate rate limit。The broadcast packet rejection of the default port is open, with a rejection rate of 64K. The purpose is to prevent the network from forming a broadcast storm。The DLF package and multicast package are not suppressed by default。

3.3.2 Broadcast suppression configuration

The following command configures the broadcast suppression of this port in the interface configuration mode：

storm-control broadcast

The following command cancels the broadcast suppression configuration for this port in the interface configuration mode：

no storm-control broadcast

3.3.3 Multicast suppression configuration

The following command configures multicast suppression for this port in the interface configuration mode：

storm-control multicast

The following command cancels the configuration of multicast suppression for this port in the interface configuration mode：

no storm-control multicast

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.3.4 DLF suppression configuration

The following command configures the DLF suppression of this port in the interface configuration mode：

storm-control dlf

The following command cancels the DLF suppression configuration of this port in the interface configuration mode：

no storm-control dlf

3.3.5 Inhibition rate configuration

The following command configures the inhibit rate of this port in the interface configuration mode：

storm-control ratelimit { broadcast | dlf | multicast } <1- 1048575 >

3.3.6 Display STORM-CONTROL configuration

The following command displays the STORM-CONTROL configuration in normal mode or privileged mode：

show storm-control

3.4 Configuring STORM-CONSTRAIN

Port traffic threshold control is used to control message storm on ethernet. The ports that enable this function detect the unicast traffic, multicast traffic and broadcast message traffic at the destination port at regular intervals。If a class of message traffic exceeds a preset upper limit threshold, the user can configure to determine whether to block the port or to shut the port, and whether to send Trap and Log information。

When a certain type of message traffic exceeds the upper limit specified by the message, the system provides two processing methods：

(1) Block: if the port of unicast, multicast or broadcast in a message flow is greater than the upper threshold, the port will suspend forwarding the packets (other types of packet forwarding, as

SEC.RU | Короткий путь к информации
Скачано с sec.ru

usual) port in the blocking state, but the port is still statistics of the kind of message flow。When this kind of message traffic is less than the lower threshold, the port will resume the forwarding of this kind of message。

(2) Shutdown mode: if a class of unicast, multicast or broadcast on the port is larger than the upper limit, the port will be closed, and the system will stop forwarding all packets。The port state can be restored by executing the undo shutdown command, and it can also be restored by canceling the port traffic threshold configuration。

Note: for a certain type of message traffic, it can be suppressed by the function or the storm suppression function of the Ethernet port, but the two functions can not be configured at the same time, otherwise the suppression effect is uncertain。For example, the unicast traffic threshold control function and unicast storm suppression function can not be configured at the same time。

The CLI configuration commands are as follows：

command	describe	CLI mode
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Storm control for broadcast, multicast, or unknown unicast messages under the interface	Interface configuration mode
no storm-constrain (broadcast|multicast|unicast|all)	Cancel storm control	Interface configuration mode
storm-constrain action (block|shutdown)	Configure storm control actions and, without default, storm control for messages	Interface configuration mode
no storm-constrain action	Cancel the configured storm control action	Interface configuration mode
storm-constrain enable (log|trap)	Switch to record or report alarm when storm control is opened	Interface configuration mode
no storm-constrain enable (log|trap|all)	Switch to log or report alarm when storm control is closed	Interface configuration mode
storm-constrain interval <6-180>	Configure the storm control detection interval, by default, the storm control detection time interval is 5 seconds	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

no storm-constrain interval	The detection interval of storm control is restored to the default value	Interface configuration mode
no storm-constrain	Delete the storm control function of the interface	Interface configuration mode
show storm-constrain	View storm control information for all interfaces	Privileged mode
show storm-constrain interface IFNAME	View the storm control information of the interface	Privileged mode

Configuration specification：

project	describe
interface	Interface name
type	Message type (1) broadcast- broadcast message; (2) multicast- multicast message; (3) unicast- unicast message
rate	Min- low threshold; max- high threshold
action	Storm control actions include (1) block- blocking messages; (2) shutdown- closing the interface
punish-status	The message state of the current interface includes (1) block- when the speed is greater than max-rate and the storm control action is a blocking message, the state is a blocking message； (2) Normal - normal forwarding； (3) shutdown-When the rate is greater than max-rate and the storm control action is to close the interface, the state is closed interface
trap	Alarm switch status，on/off
log	Log switch status，on/off
interval	The detection interval of storm control is in seconds, and the default value is 5 seconds
last-punish-time	Finally, the time of storm control punishment

(1) View the storm control information description table of the interface

(2) By executing the storm- constrain action command to configure the action of storm control, and executing the storm- constrain command to configure the high-low threshold of storm control,

SEC.RU | Короткий путь к информации
Скачано с sec.ru

the storm message can be controlled to prevent flooding。In the storm control detection interval, when the average rate of broadcast, multicast, or unicast packets on the interface is greater than the specified threshold, the storm control will block the packets according to the configured actions or shut down the interface. When the storm control action is blocked, if the traffic is below the minimum threshold, the interface resumes to the normal forwarding state. When the storm control action is closed, the interface can not be restored automatically. You need to manually execute the no shutdown command to restore the interface. Port storm control shutdown action configuration to restore。

(3The port traffic exceeds the upper threshold or falls from the upper limit to the lower threshold. Output log / trap information

3.5 Configuring FLOW-CONTROL

FLOW-CONTROL (flow control) is used to prevent packet loss in the case of port blocking. In half duplex mode, the flow control is realized by back pressure (Backpressure) technique, which reduces the sending speed of the information source。In full duplex mode, the flow control follows the IEEE802.3x standard. The blocking port sends the "Pause" packet to the information source to suspend the transmission。

This section gives a detailed description of the configuration of FLOW-CONTROL (flow control), including the following：

- Default configuration
- Set port receive and send side flow control
- Closed port flow control
- Display flow control information

3.5.1 Default configuration

The switch supports the flow control of sending and receiving ports for each port. The default port does not open the flow control function。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.5.2 Set port receive and send side flow control

The following command configures the port receive and send side flow control in the interface configuration mode：

flowcontrol

3.5.3 Closed port flow control

The following command closes the port send and receive side flow control in the interface configuration mode：

no flowcontrol

3.5.4 Display flow control information

The following command displays flow control information for all ports in normal mode or privileged mode：

show flowcontrol

The following command displays the flow control information of a port in common mode or privileged mode：

show flowcontrol interface <if-name>

Among them, <if-name> is the port name to query flow control information。

3.6 Configuring port bandwidth

Port bandwidth control is used to control the rate of port sending and receiving。

This section gives a detailed description of the port bandwidth configuration, including the following：

- Default configuration
- Set port send or receive bandwidth control
- Cancellation of port transmit or receive bandwidth control
- Bandwidth control of display port configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.6.1 Default configuration

The switch supports sending and receiving bandwidth to each port, respectively. The default port does not perform bandwidth control。

3.6.2 Set port send or receive bandwidth control

The following command sets the port to send or receive bandwidth control in the interface configuration mode：

portrate {egress | ingress} <rate>

Egress represents bandwidth control over packets sent。

Ingress represents bandwidth control of the received packets。

<rate> said to set the bandwidth value range is 11024000, unit is kbits。

3.6.3 Cancellation of port transmit or receive bandwidth control

The following command cancels the bandwidth control of the port in the interface configuration mode：

no portrate {egress | ingress}

Egress represents bandwidth control to cancel sending packets。

Ingress represents the bandwidth control of the cancelled packet。

3.6.4 Bandwidth control of display port configuration

The following command looks at bandwidth control of port configuration in common mode or privileged mode：

show portrate interface <if-name>

<if-name> is the port name to query bandwidth control information。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.7 Configuring TRUNK

TRUNK is the integration of multiple ports into a logical port, which can be used to increase bandwidth, provide redundant backup connections, and can also be used for load balancing。When the TRUNK group is used as the output logic port, the switch will send a packet from the port group by selecting a port according to the aggregation policy set by the user。The configuration of port and aggregation strategy in TRUNK group is completed by software, but the forwarding of data stream is accomplished by hardware。

All ports in the TRUNK group must be configured at the same speed, and in full duplex mode。switches can support up to 8 groups of TRUNK, each group of TRUNK members up to 8。Special attention should be paid to that each port can only belong to a TRUNK group。

LACP protocol is a protocol based on IEEE802.3ad standard。LACP protocol interacts with the client via LACPDU (Link Aggregation Control Protocol Data Unit)。

The interface in the aggregation group enables the LACP protocol. The interface advertises the LACP protocol priority, the system MAC address, the LACP priority of the port, the port number, and the operation key to the peer through the LACPDU. After receiving the LACPDU, the peer compares the information with the information received by other interfaces to select the interface that can be in the selected state, so that the two parties can agree on the interface in the selected state。

The operation key is a configuration combination that is automatically generated according to some configurations of member ports during link aggregation. It includes port rate, duplex mode, up / down status, VLANs allowed on port, VLAN default VLAN ID , The link type of the port (that is, Trunk, Hybrid, Access type) and so on. In the aggregation group, the member ports in the selected state have the same operation Key。

This section gives a detailed description of the configuration of TRUNK, including the following：

- LACP protocol configuration
- Configuration of TRUNK group
- TRUNK group member port configuration
- TRUNK load balancing policy configuration
- Display of TRUNK

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.7.1 LACP protocol configuration

command	describe	CLI mode
lacp system-priority <1-65535>	Setting priority of LACP system	Global configuration mode
no lacp system-priority	Restore system priority defaults 32768	Global configuration mode
lacp max-active-link-number <1-8>	Set LACP to activate the upper bound of the polymerization port	Global configuration mode
no lacp max-active-link-number	Restore LACP to activate aggregate port default limit 8	Global configuration mode
lacp port-priority <1-65535>	Set LACP port priority	Interface configuration mode
no lacp port-priority	Restore port priority defaults 32768	Interface configuration mode
lacp timeout (short|long)	Set LACP port timeout, missing governor timeout	Interface configuration mode
show lacp summary	Shows all the simple things about LACP polymerization	Privileged mode
show lacp detail	Show all the LACP polymerization scenarios	Privileged mode
show lacp <1-8>	Details of the LACP polymerization port are shown	Privileged mode
show lacp port IFNAME	Show the details of the LACP port	Privileged mode
show lacp system-id	Display the LACP system	Privileged mode
show lacp counter <1-8>	Show the statistics of LACP polymerization port	Privileged mode
show lacp counter	Show the statistics of all LACP ports	Privileged mode
clear lacp <1-8> counters	Clear the statistics of LACP polymerization port	Privileged mode
clear lacp counters	Clear statistics of all LACP ports	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.7.2 Configuration of TRUNK group

The following command creates a manual TRUNK group in global configuration mode：

trunk <trunk-id>

Create TRUNK group, the <trunk-id> value range is 1-8, indicating the TRUNK group ID number to be created, the most configurable 8 groups of TRUNK；After creating the success, the TRUNK group interface name is trunk+id, such as group ID number 1 TRUNK group interface name is trunk1。You can configure the mode with "interface trunk+id" command to enter interface configuration mode, and then operate on the TRUNK group, such as the use of interface command interface mode trunk1 into TRUNK 1, the configuration of the TRUNK 1。

The following command creates a static LACP TRUNK group in global configuration mode：

trunk <1-8> dynamic

The following command deletes a TRUNK group in global configuration mode：

no trunk <trunk-id>

When you delete a TRUNK group, you must ensure that the TRUNK group does not have a member port。

3.7.3 TRUNK group member port configuration

The following command in interface configuration mode of new members of TRUNK port：

trunk interface IFNAME (passive|)

<if-name> is the port name that needs to be added to the TRUNK group, and must be the two layer interface. Each group of TRUNK can add 8 two layer interfaces at most。If the TRUNK group is a static LACP TRUNK group, the add interface defaults to the active state and can be configured as a passive state。

The following command deletes all the member ports of the TRUNK group in the interface configuration mode：

no trunk interface

The following command deletes the specified TRUNK group member port in the interface configuration mode：

no trunk interface <if-name>

You can use this command multiple times to delete the multiple member ports of the TRUNK group。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.7.4 TRUNK load balancing policy configuration

The following command sets the load balancing policy of TRUNK in the interface configuration mode：

trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}

dst-mac-------- Equilibrium strategy based on objective MAC

dst-ip---------- Equilibrium strategy based on objective IP

src-dst-mac--- Equilibrium strategy based on source MAC and destination MAC

src-dst-ip------ Equilibrium strategy based on source IP and destination IP

src-mac-------- Equilibrium strategy based on source MAC

src-ip---------- Equilibrium strategy based on source IP

The following command sets the default TRUNK load balancing policy in the interface configuration mode：

no trunk load-balance

The default port load balancing policy is src-dst-mac (a balanced strategy based on source MAC and destination MAC)。

3.7.5 Display of TRUNK

The following command looks at all TRUNK group configurations in common mode or privileged mode：

show trunk

The following command looks at the specified TRUNK group configuration in common mode or privileged mode：

show trunk <trunk-id>

<trunk-id> is the ID number of the TRUNK group to be checked。

3.8 Configure super large frame

3.8.1 Oversize introduction

In order to achieve the port can receive super large frame, you can set the port to support the specific super frame length。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.8.2 Oversize configuration

The port configuration supports super frame length, in config mode, into the port configuration mode, such as interface ge1/1, execute the following command：

Switch(config-ge1/1)# jumbo frame 2000

Super large frame length supported by display portSwitch#show jumbo frame ge1/1

Port	Jumbo frame(bytes)
ge1/1	2000

3.9 Configuring redundant ports

In some special cases, such as the need to focus on the protection of certain servers linked to the stability of the network, the switch's redundant port can provide two ports linked to the server, and to ensure that at a time the server only one LINK UP port link network , When a port occurs LINK DOWN, the system immediately enable another port。

When a port in the redundant port group in the LINK UP, we call the Active state; the other hand, if a redundant port group in the LINK DOWN, we call the Disable state。

This section focuses on the configuration of redundant ports, including the following：

- Configuration of redundant ports
- Display of redundant ports

3.9.1 Configuration of redundant ports

Can configure 8 sets of redundant ports, a group of redundant ports can only configure 2 ports; one port can only be configured to a redundant port group。

A redundant port group can configure a primary-port and secondary-port. When configuring redundant port groups：

1、When the two ports are in the LINK UP state at the same time, the primary-port is set to the Acitve state, and the secondary-port is placed in the Disable state；

2、If only one port is in the LINK UP state, the current LINK UP port is set to the Active state, and the other port is in the Disable state；

3、Otherwise, the two ports are out of the Disable state。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

If a LINK DOWN event occurs on the port of the Active state, another port will be tried to be Active state。

There is also a configuration parameter is the force-switch, which is in the secondary-port in the Active, primary-port in the Disable state, if the primary-port LINK UP event occurs when the decision to re-switch to primary-port For Active, secondary-port is in the Disable state。If force-switch is configured as enable, then it is forced to switch, otherwise the port state of the original redundant port group will be retained。

command	describe	CLI mode
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Configuring a group of redundant ports，<1-8> is a group ofprimary-port IFNAME is the name of the main port interface，Secondary-port IFNAME is the alternate port interface name，Does force-switch use a mandatory toggle switch?	Global configuration mode
redundant-port <1-8> force-switch	Mandatory switch with redundant ports。	Global configuration mode
no redundant-port <1-8>	Delete redundant port groups。	Global configuration mode
no redundant-port <1-8> force-switch	Forced switch for closing redundant ports。	Global configuration mode

3.9.2 Display of redundant ports

Commands to display redundant ports

command	describe	CLI mode
show redundant-port	Configuration of all redundant port groups in the display system	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.10 Configuring LLDP

At present, the types of network devices are increasingly numerous and their configuration is complex. In order to enable different vendors' devices to discover and interact with each other in the network, they need a standard information exchange platform。

LLDP (Link Layer Discovery Protocol) is generated in this context, it provides a standard link layer discovery, the local equipment can be the main ability, management address, device identification, interface identification and other information organization (Type / Length / Value), and encapsulated in the LLDPDU (Link Layer Discovery Protocol Data Unit) issued to the neighbors directly connected with their neighbors to receive this information after the standard MIB (Management Information Base) in the form of preservation for the network management system to query and determine the link status of the communication。

This section focuses on the configuration of LLDP, including the following：

- LLDP configuration
- LLDP display

3.10.1 LLDP configuration

There are 4 types of LLDP port working modes：

TxRx: send and receive LLDP message。

Tx: send only not receive LLDP message。

Rx: only receive not send LLDP message。

Disable: neither sends nor receives LLDP messages。

When the port's LLDP operating mode changes, the port will initialize the protocol state machine. In order to avoid the frequent change of port operation mode and cause the port to perform initialization operation continuously, the configurable port initialization delay time is delayed and the initialization operation is delayed when the port operation mode changes。

command	describe	CLI mode
lldp global enable	LLDP global enable command.	Global configuration mode
lldp hold-multiplier <num>	Lldp TTL multiples。	Global configuration mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][<	Configure LLDP various timers。	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

tx-interval ><time>]		
lldp enable	Enable interface LLDP	Interface configuration mode
lldp admin-status{ disable| rx|tx|rxtx}	Configuring the LLDP port mode of operation。	Interface configuration mode
lldp check-change-interval <time>	Configuring refresh interface information interval	Interface configuration mode
lldp management-address <A.B.C.D>	Configuring the interface LLDP to manage the address	Interface configuration mode
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Configure interface LLDP extended capability set switch	Interface configuration mode

3.10.2 LLDP display

LLDP command

command	describe	CLI mode
show lldp configuration [ifname]	Display lldp configuration information	Privileged mode
show lldp local-information [ifname]	Display lldp local information	Privileged mode
show lldp neighbor-information [ifname]	Display lldp neighbor information	Privileged mode
show lldp statistics [ifname]	Display lldp message statistics	Privileged mode
show lldp status [ifname]	Display lldp status information	Privileged mode

Fourth chapters

Port based MAC security

This chapter introduces the port based MAC security configuration, including the following contents：

- brief introduction
- MAC binding configuration
- MAC filter configuration
- Port learning constraint configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.1 brief introduction

Port based MAC security can provide three functions of MAC binding, MAC filtering and port learning control to improve the security performance of the two layer forwarding of the switch。

MAC binding can be MAC and port together, limiting a specified MAC address can only be in a specified port to access the network; the same time, the port can only allow these binding MAC address to access the network; a port can simultaneously Bind multiple MAC addresses. MAC binding can be applied to a designated port at the same time as 802.1x。This function is very useful for some devices that do not have 802.1x functionality or are not convenient to use 802.1x devices, such as printers, file servers, etc.。

MAC filtering allows some designated MAC addresses to fail to access the network. The main purpose is to prevent some illegal devices from accessing the network。When an MAC address is configured as a MAC filter, the MAC address cannot be accessed at any port of the switch in the network, also cannot receive the purpose of MAC is the specified MAC address data packets, and MAC binding, a port can also configure multiple MAC MAC address filtering。In application, if some virus software attacks the network through the forged MAC address, besides ACL, the attack of controlling these forged packets can be accessed by MAC filtering。

Port learning control can control a port to dynamically learn the number of MAC addresses. If a port specifies that it can dynamically learn the number of MAC addresses, when the number of MAC addresses learned by this port is equal to the number of the port configuration, the new MAC address will no longer be learned. For these new MAC addresses The packet will be discarded。

It's important to note that the MAC address here is actually MAC+VID, and the description behind this chapter is no longer necessary。In addition, MAC binding function and 802.1x can be configured on one port at the same time. MAC filtering and port learning limit can be configured on one port at the same time. MAC binding function, 802.1x and MAC filtering, port learning limit between the two groups can not be simultaneously Configured to the same port。

4.2 MAC binding configuration

The MAC binding configuration supports manually binding MAC addresses and automatically binding MAC addresses。Manual binding MAC address is the user through the command one by one input MAC address and port binding。Automatically binding the MAC address is to read the existing entries of the port in the two layer hardware forwarding table, and directly bind the MAC address。The command to read the two layer hardware table is Show bridge FDB。

Configuration command

command	describe	CLI mode
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094>	Manually bind a MAC address to an interface。	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

switchport-security mac-bind auto-conversion number <1-16383>	Automatically converts a specified number of MAC addresses to an MAC binding configuration。	Interface configuration mode
switchport-security mac-bind auto-conversion vlan <1-4094>	Automatically converts an MAC address of a specified VLAN to a MAC binding configuration。	Interface configuration mode
show port-security mac-bind [IFNAME]	Display MAC binding configuration	Privileged mode

The reason for invalid or failed MAC address binding may be as follows：

The port has been configured with 802.1x

The port has been configured with MAC filtering or configured port learning restrictions；

The MAC address has been bound to other ports, or configured with MAC filtering；

The L2 table of the switch is full。

4.3 MAC filter configuration

The MAC filter configuration supports manually binding MAC addresses and automatically binding MAC addresses。Manual configuration of MAC filter is the user through the command input one by one to filter the MAC and port binding。Automatic configuration MAC filtering is to read the existing entries of the port in the two layer hardware forwarding table, and directly configure the MAC filter。The command to read the two layer hardware table is Show bridge FDB。

command	describe	CLI mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Manually configure an interface for MAC filtering	Interface configuration mode
switch port-security mac- filter auto-conversion number <1-16383>	Automatically converts a specified number of MAC addresses to an MAC filter configuration	Interface configuration mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically converts the MAC address of a specified VLAN of an interface to the MAC filter configuration	Interface configuration mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

note：

The reason for invalid or failed MAC filter configuration may be as follows：

The port has been configured with MAC bindings or enabled the 802.1x protocol function；

The MAC address has been bound to other ports, or configured with MAC bindings；

The L2 table of the switch is full。

4.4 Port learning constraint configuration

switches can configure the maximum number of dynamic learning addresses per port。If a port is configured number of dynamic learning MAC address, then the port can only learn the corresponding number of MAC address, when beyond this number MAC address, not learning and forwarding at this port。

With no learning constraints, a port can learn at most 16383 MAC addresses。

Configuration command

command	describe	CLI mode
switchport port-security learn-limit <0-16383>	Configure the number of MAC addresses that an interface can learn。	Interface configuration mode
no switchport port-security learn-limit	Deletes the number of MAC addresses that an interface can learn。	Interface configuration mode
show port-security learn-lmit [IFNAME]	Display port learning configuration	Privileged mode

Configuration example

Configuring port ge1/5 can only learn 7 MAC addresses

Switch#configure terminal

Switch(config)interface ge1/5

Switch(config-ge1/5)switchport port-security learn-limit 7

note：

The reasons for invalid or failed port learning may be as follows：

The port has been configured with MAC bindings or enabled the 802.1x protocol function。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

OSNOVO
cable transmission

Fifth chapters

Port IP and MAC binding

This chapter introduces the port IP and MAC binding configuration, including the following contents：

- brief introduction
- IP and MAC binding configurations
- Configuration example
- Configuration misarrangement

5.1 brief introduction

Configuring IP and MAC binding on Layer 2 switch ports is a static defense against ARP attacks。ARP attackers attack MAC users by sending ARP messages with false MAC addresses, which causes the local ARP cache table to be covered by the attacker's address, so that the normal data flows to the attacker。In the switch port configuration command static binding user IP address and MAC address can effectively filter ARP attack packets。

In addition to anti-ARP spoofing function, IP MAC binding function can protect the IP and MAC one by one mapping relationship, that is an IP can only correspond to a MAC, a MAC can only correspond to an IP, if then The incoming device modifies this mapping, and it will not be able to communicate in this network。802.1x anti ARP spoofing function and DHCP SNOOPING protocol are the dynamic implementation of this function。

The four functions of IP MAC binding, ACL, 802.1x anti ARP spoofing and DHCP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

SNOOPING all use the same system resource CFP, and pay attention to whether the resources of CFP are exhausted when configuring。We have developed a compatibility relationship between them in the design。Following table：

	IP MAC binding	ACL	802.1x	DHCP SNOOPING
IP MAC binding	compatible	Incompatible	compatible	compatible
ACL	Incompatible	compatible	Incompatible	Incompatible
802.1x	compatible	Incompatible	compatible	Incompatible
DHCP SNOOPING	compatible	Incompatible	Incompatible	compatible

CFP is a limited hardware resource, the average to each port can only be configured 16 IP MAC binding entries, so in a network access to a host if only a few ports or a small number of IP and MAC addresses need to be controlled, you can use static The IP MAC binding function。Avoiding CFP function exhaustion leads to data forwarding failure。

In addition, as for the use of 802.1x or DHCP SNOOPING protocol, depending on the current situation, if you use a static IP address configuration and use the 802.1x protocol to access the network to use 801.1x anti-ARP spoofing can be effective, if the use of dynamic access to IP address , Use the DHCP SNOOPING protocol。

5.2 IP and MAC binding configurations

IP binds to MAC in the interface mode configuration

Configuring port IP and MAC bindingSwitch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC

Delete port IP and MAC binding

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Display configuration

Displays the bound entries of all ports

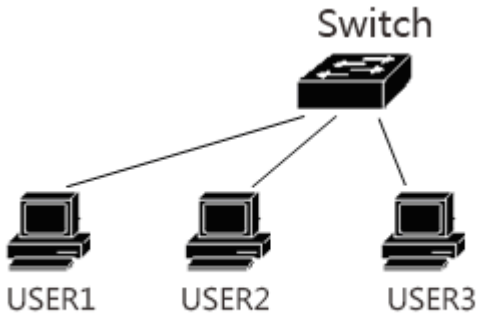
show ip mac-bind

Displays the binding table entry of an interfaceshow ip mac-bind IFNAME

5.3 Configuration example

There are 1 users, 2 users and 3 users in the network, and the IP and MAC of the user are bound at the port, which can defend against the ARP attack。

SEC.RU | Короткий путь к информации
Скачано с sec.ru




```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end
Switch#show ip mac-bind
[ge1/1] sum: 1
        MAC                     IP
        0011.5b34.42ad  192.168.1.100
[ge1/2] sum: 1
        MAC                     IP
        0011.6452.135d  192.168.1.101
[ge1/3] sum: 1
        MAC                     IP
        0011.804d.a246  192.168.1.102
Switch#show ip mac-bind ge1/1
[ge1/1] sum: 1
        MAC                     IP
        0011.5b34.42ad  192.168.1.100
Switch#show running-config
!
spanning-tree mst configuration
!
Interface vlan1
  ip address 192.168.0.1/24
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
!
interface ge1/1
 ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2
 ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3
 ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
end
```

5.4 Configuration misarrangement

If the IP MAC binding configuration fails, it may be caused by the following reasons：

1、System CFP resource exhaustion。

2、The current interface is configured with the ACL filter function。

3、The configured interface is a three layer interface or a TRUNK interface。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

OSNOVO
cable transmission

Sixth chapters

VLAN configuration

VLAN is an important concept in the switch, and it is used very much in practical applications. It is the basis of internal division of multiple networks。VLAN is the abbreviation of virtual local area network (LAN). It is a network that logically connects multiple devices, regardless of the physical location of the device。Each VLAN is a logical network, which has all the functions and attributes of the traditional physical network. Each VLAN is a broadcast domain, broadcast packets can only be forwarded within a VLAN, can not cross the VLAN, VLAN data communication must be transmitted through three layers。

The main contents of this chapter are as follows：

- VLAN introduce
- VLAN configuration
- VLAN configuration example
- MAC, IP subnet, protocol VLAN
- VOICE VLAN
- VLAN mapping
- QINQ

6.1 VLAN introduce

This section gives a detailed introduction to VLAN, including the following contents：

- The benefits of VLAN
- VLAN ID
- VLAN port member type
- Default VLAN of port
- Port VLAN mode
- VLAN relay
- Data flow is forwarded in VLAN

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1.1 The benefits of VLAN

VLAN greatly extends the scale of physical networks. The traditional physical network can only have a very small scale, which can accommodate thousands of devices, and the physical network using VLAN can accommodate tens of thousands or even hundreds of thousands of devices。VLAN has the same function and attribute as the traditional physical network。

The use of VLAN has the following advantages：

- VLAN can effectively control the traffic in the network。

In traditional networks, regardless of the need, all broadcast packets are transmitted to all devices, increasing the load of the network and equipment. And VLAN can organize the device in a logical network according to the need, a VLAN is a broadcast domain, broadcast packets are only transmitted within the VLAN, not across the VLAN 。By dividing the VLAN, the traffic in the network can be effectively controlled。

- VLAN can improve the security of network。

VLAN equipment only with a VLAN of two layer communication equipment, and if you want another VLAN communication, must be forwarded through the three layer, three layer forwarding between the VLAN if not established, no communication between VLAN, can play the role of isolation, to ensure that each VLAN data security。For example, a company's R & D department does not want to share with the data of the marketing department, can R & D department to establish a VLAN, the marketing department to build a VLAN, two VLAN do not establish three layers of communication channel。

- VLAN makes the device easy to move。

In the traditional network, if the device moves from one location to another, and belongs to different networks, it is necessary to modify the network configuration of the mobile device, which is very inconvenient for the user. VLAN is a logical network, can be put in the same physical location of the equipment designated in the same network, when the mobile device can also make the equipment belonging to the VLAN, so the mobile device does not need to modify any configuration。

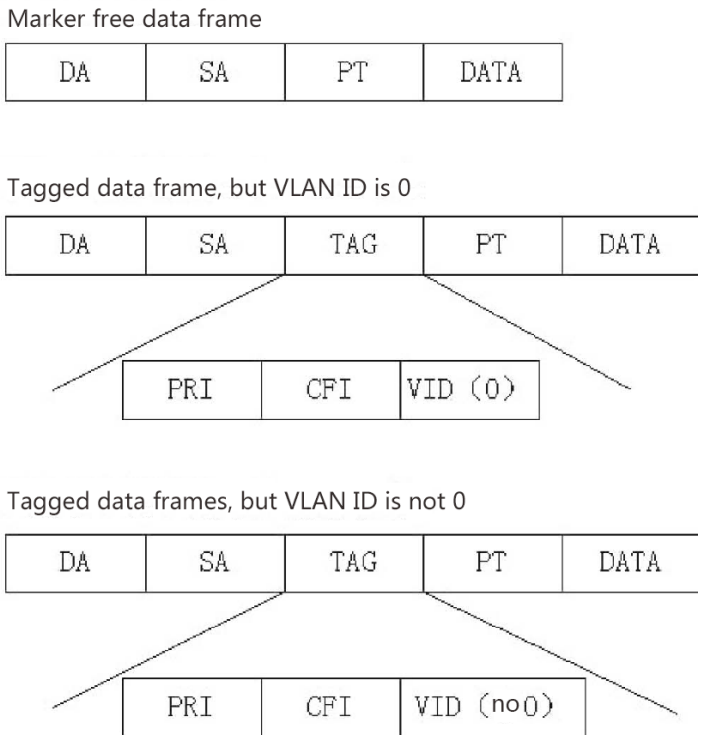
SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1.2 VLAN ID

Each VLAN has an identification number, called VLAN ID. The range of VLAN ID ranges from 0 to 4095, of which 0 and 4095 are not used, and the actual efficiency is only 1 to 4094 。VLAN ID uniquely identifies a VLAN 。

The switch supports 4094 VLAN, and when you create VLAN, you choose a VLAN ID, ranging from 2 to 4094。Switches create VLAN1 by default, and VLAN1 cannot be deleted。

There are three kinds of data frames transmitted in a VLAN network：A data frame without tags, a data frame with VID 0, a data frame with VID 0 Non marked。As shown below, there are three different formats of data frames。



All data frames within a switch are marked。If a marker free data frame is entered into the switch, the switch adds a tag to the data frame, and selects a VLAN ID value to fill in the marked VID。If a data frame with VID 0 is entered into the switch, the switch selects a VLAN ID value to fill in the marked VID。If a data frame with VID non 0 tag is input to the switch, the frame remains unchanged。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1.3 VLAN port member type

Switches support port based VLAN and 802.1Q based VLAN 。A VLAN consists of two port member types: untagged members and tagged members。A VLAN can include both a untagged port member and a tagged port member。

A VLAN can have no port member, and can also have one or more port members。When a port belongs to a VLAN, it can be a member of VLAN or a member of tagged in untagged。

A port can belong to one or more VLAN tagged or untagged members. If a port belongs to two or more tagged members of VLAN, this port is also called the VLAN relay port。A port can also belong to one or more untagged members of VLAN and to tagged members belonging to another or more VLAN。

6.1.4 Default VLAN of port

The port has only one default VLAN, and the default VLAN is used to determine the VLAN that is not labeled or marked with a VID 0 input from the port。The default VLAN is also referred to as port VID or PVID. By default, the default VLAN of the port is 1。

6.1.5 Port VLAN mode

There are three VLAN modes in port: ACCESS mode, TRUNK mode and HYBRID mode. When the user configured the port VLAN, the VLAN mode of the port must first be specified。

The port of the ACCESS mode is an access port, which is directly oriented to the user. The port can only belong to a VLAN member of the untagged, and the default VLAN is the user specified VLAN. When the port only belongs to a VLAN member of untagged, the VLAN mode of the port can be specified as the ACCESS mode。

TRUNK port is a trunk port, and the switch directly connected, the port can belong to one or more VLAN members of the tagged, but does not belong to any VLAN member of the untagged, the default VLAN port is 1, can not be changed。

The port of the HYBRID mode is a relay port, which is directly connected to the switch. The port can belong to one or more tagged members of the VLAN and / or one or more untagged members of the VLAN. The default VLAN of this port can be changed。

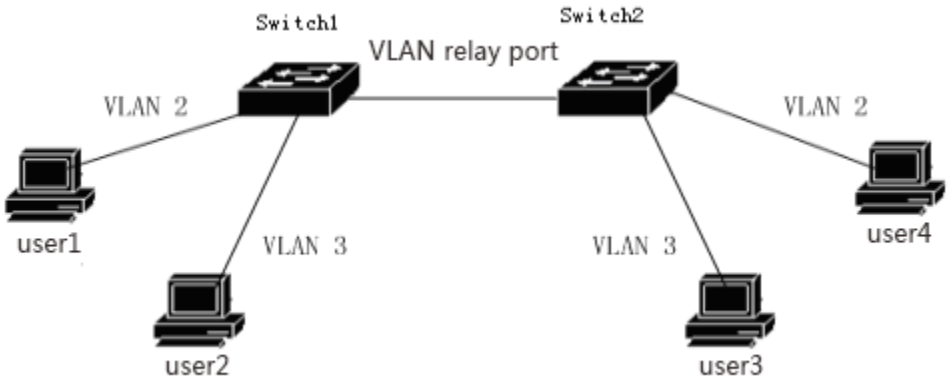
In practical application, the user can select the VLAN mode of the port according to the specific situation。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1.6 VLAN relay

If a port belongs to two or more tagged members of VLAN, then this port is also called the VLAN relay port. The two switches can be connected to the VLAN relay port, so that the two switches can be divided into two or more common VLAN。

Below is a VLAN relay for example, between two switches connected to VLAN relay port, VLAN 2 and VLAN 3 relay port, each switch is divided into two VLAN, respectively, VLAN 2 and VLAN 3, each VLAN has a user. In this way, the user 1 can communicate with the user 3, and the user 2 can communicate with the user 4, and the user 1 and the user 3 can not communicate with the user 2 and the user 4。



6.1.7 Data flow is forwarded in VLAN

When the switch receives a packet from one port, the two step is forwarded according to the following steps：

- Determines the VLAN to which the packet belongs 。
- Determine whether the packet is broadcast data packet, multicast packet or unicast packet。
- According to different packets to determine the output port (can be zero, one or more output ports), if there is no output port, discard the packet。
- According to different packets to determine the output port (can be zero, one or more output ports), if there is no output port, discard the packet。
- Send out from the output port。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1) How to determine the VLAN of a packet：

If the data packet label is received and the VID field in the tag is not 0, the VLAN to which the packet belongs is the V I D value in the tag。

If the received packet is not marked or marked, but the VID value in the tag is 0, the VLAN of the packet belongs to the default VLAN of the port。

2) How to determine the type of packets：

If the destination MAC address of the received packet is FF:FF:FF:FF:FF:FF, the packet is a broadcast packet。

If the received packets are not broadcast packets and the fortieth bits of their destination MAC addresses are 1, then the packets are multicast packets。

If it is neither a broadcast packet nor a multicast packet, the packet is a unicast packet。

3) How to determine the output port of a packet：

If the input packet is a broadcast packet, all the member ports of the VLAN to which the packet belongs is the output port of the packet。

If the input data packet is multicast data packets, according to the purpose of multicast MAC address and the VLAN for the two layer hardware multicast forwarding table entries, if found, is multicast, multicast entries in the output port and an VLAN member of the port in the common port (and operation) as the output port packet and if there is no common port, the packet is discarded。If the two hardware multicast forwarding multicast, find no entries in the table, according to the two layer multicast forwarding mode hardware forwarding decision output port, if it is not registered in the multicast forwarding mode, multicast packets as radio treatment, the VLAN of all members of the port is packet output port, if the forwarding mode is registered no, the output port, data packet discard。

If the input data packet is unicast packets, according to the VLAN to find the two hardware destination MAC address and the forwarding table, if it finds a match, then the output port of entry and the members of the VLAN port in the common port (and operation) for the data packet output port, if not the common port, the packet is discarded. If no matching entries are found in the two layer hardware forwarding table, the packet is treated as a broadcast packet, and all the member ports of the VLAN belong to the output port of the packet。

4) Send data packet：

The output port of the input packet is decided to send the packet out from all the output ports。

If an output port is a untagged member of the VLAN that belongs to the packet, the packet is

SEC.RU | Короткий путь к информации
Скачано с sec.ru

not marked when it is sent from the output port。

If an output port is a tagged member of the VLAN that belongs to the packet, the packet is tagged when it is sent out of the output port, and the VID value in the tag is the value of the VLAN to which the packet belongs。

6.2 VLAN configuration

This section gives a detailed introduction to the configuration of VLAN, including the following：

- Creating and deleting VLAN
- Configuring port VLAN mode
- VLAN configuration of ACCESS mode
- VLAN configuration of TRUNK mode
- HYBRID mode VLAN configuration
- View VLAN information

6.2.1 Creating and deleting VLAN

Before creating and deleting VLAN, users need to use the VLAN database command in the global configuration mode to enter the VLAN configuration mode, and create and delete VLAN in this mode。

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by the user. The commands for creating and deleting VLAN are as follows：

command	describe	CLI mode
vlan <vlan-id>	Create a VLAN。If the VLAN already exists, it does not do the processing, otherwise the VLAN is created。Parameters range from 2 to 4094。	VLAN configuration mode
no vlan <vlan-id>	Delete a VLAN, if the VLAN does not exist, do not do processing, otherwise delete the VLAN。Parameters range from 2 to 4094。	VLAN configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.2.2 Configuring port VLAN mode

Before configuring the port VLAN, you need to specify the VLAN mode of the port. By default, the VLAN mode of the port is ACCESS mode。The VLAN mode command of the specified port follows the table：

command	describe	CLI mode
switchport mode access	The VLAN mode of the specified port is ACCESS mode。After executing this command, the port is the untagged member of VLAN1, and the default VLAN of the port is 1。	Interface configuration mode
switchport mode trunk	The VLAN mode of the specified port is TRUNK mode. After executing this command, the port is the tagged member of VLAN1, and the default VLAN of the port is 1。	Interface configuration mode
no switchport trunk	The VLAN mode of the port is no longer TRUNK mode, back to the default, that is, the ACCESS mode。	Interface configuration mode
switchport mode hybrid	The VLAN mode of the specified port is HYBRID mode. After executing this command, the port is the untagged member of VLAN1, and the default VLAN of the port is 1。	Interface configuration mode
no switchport hybrid	The VLAN mode of the port is no longer HYBRID mode, back to the default, that is, the ACCESS mode。	Interface configuration mode

6.2.3 VLAN configuration of ACCESS mode

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the ACCESS mode。In this VLAN mode, the port defaults to the VLAN1 member of untagged, and the default VLAN of the port is 1。The VLAN configuration command of ACCESS mode is as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
switchport access vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. Parameters range from 2 to 4094。	Interface configuration mode
no switchport access vlan	The VLAN configuration of the port goes back to the default, that is, the port is the untagged member of VLAN1, and the default VLAN of the port is 1。	Interface configuration mode

6.2.4 VLAN configuration of TRUNK mode

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the TRUNK mode。In this VLAN mode, the port defaults to the VLAN1 member of tagged, and the default VLAN of the port is 1。The VLAN configuration command of TRUNK mode is as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
switchport trunk allowed vlan all	The configuration port is the tagged member of all VLAN. For the newly created VLAN, the port is also the tagged member of these VLAN。	Interface configuration mode
switchport trunk allowed vlan none	Except for VLAN1, the port is no longer a member of all other VLAN tagged。	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configure the port to be the tagged member of the specified one or more VLAN。The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN。For example, the parameters can be "1", "2-4" or "1,3,5"。	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLAN and is no longer the tagged member of these VLAN。The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN。For example, the parameters can be "1", "2-4" or "1,3,5"。	Interface configuration mode

6.2.5 HYBRID mode VLAN configuration

Before the port is configured for VLAN, the VLAN mode of the port should be specified as the HYBRID mode。In this VLAN mode, the port defaults to the VLAN1 member of untagged, and the default VLAN of the port is 1。The VLAN configuration command of HYBRID mode is as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
switchport hybrid vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN。Parameters range from 2 to 4094。	Interface configuration mode
no switchport hybrid vlan	The port is cleared from the default VLAN, no longer the default VLAN's tagged or untagged member, and the default VLAN of the port returns to 1。	Interface configuration mode
switchport hybrid allowed vlan all	Configuration ports are all tagged members except VLAN (except VLAN1). For the newly created VLAN, the port is also the tagged member of these VLAN。	Interface configuration mode
switchport hybrid allowed vlan none	Except for VLAN1, the port is no longer a member of all other VLAN's tagged or untagged, and the default VLAN of the port returns to 1。	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Configure the port to be the tagged member of the specified one or more VLAN。The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN。For example, the parameters can be "1", "2-4" or "1,3,5"。	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configure the port to be the untagged member of the specified one or more VLAN。	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	The parameter <vlan-list> can be a VLAN, a VLAN range or a plurality of VLAN。For example, the parameters can be "1", "2-4" or "1,3,5"。	
switchport hybrid allowed vlan remove <vlan-list>	The port is cleared from the specified one or more VLAN and is no longer the tagged or untagged member of these VLAN。If the default VLAN of the port belongs to the specified VLAN, then the default VLAN is returned to 1。	Interface configuration mode

6.2.6 View VLAN information

The commands for viewing VLAN information are listed below：

command	describe	CLI mode
show vlan [vlan-id]	If you don't input parameters, display all the VLAN information, if you input parameters, display a specified VLAN information. Parameters range from 1 to 4094。	Normal mode, privileged mode
show interface switchport	Display the VLAN related information of all ports of the system, such as VLAN mode, default VLAN and so on。	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the VLAN。	privileged mode

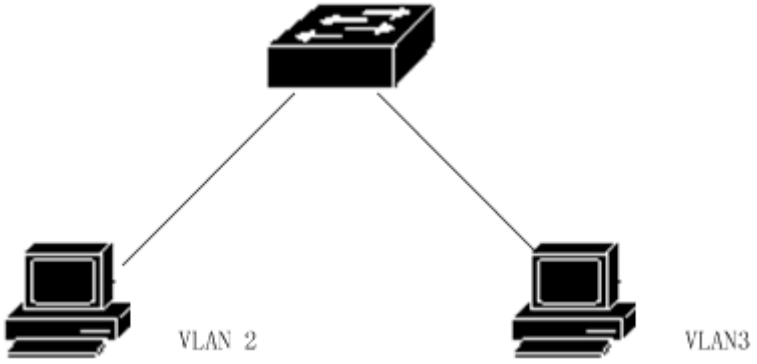
SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.3VLAN configuration example

6.3.1 VLAN based on PORT

1) Configuration

There are two users, 1 users and 2 users. Two users need to be in different VLAN because of the different network functions and environments。The user 1 belongs to the VLAN2, connects the switch port ge1/1, the user 2 belongs to VLAN3, connects the switch port ge1/2。



The configuration of the switch is as follows：

Creating VLAN

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Assigning ports to VLAN

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 2

Switch(config-ge1/1)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 3

2) Troubleshooting

SEC.RU | Короткий путь к информации
Скачано с sec.ru

If the configuration, it is found that the PC between different VLAN can not communicate, which is a normal phenomenon, because different VLAN to communicate, must go through three layers of routing forwarding。If the PC in the same VLAN cannot communicate with each other, the following verification must be made：

show vlan

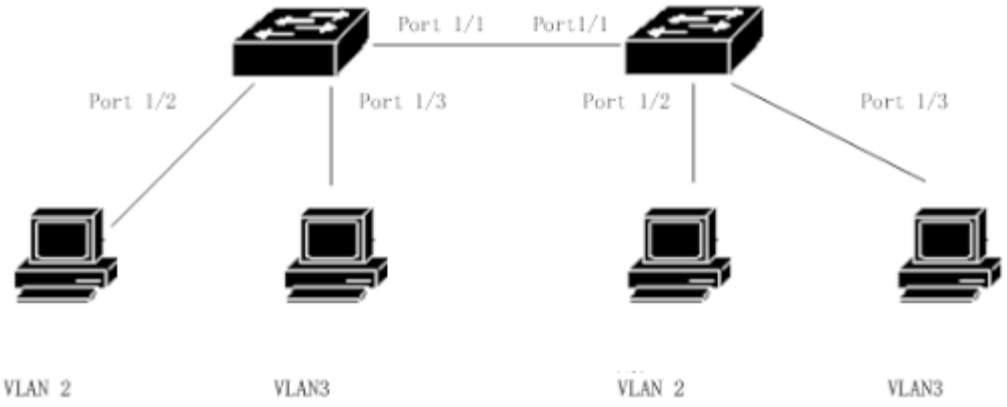
See all the VLAN member ports

show vlan <vlan-id>

See if the port connecting a particular PC machine is within the specified VLAN

6.3.2 VLAN based on 802.1Q

1) Configuration



There are two switches connected to two users：

user	VLAN belongs to	Connection port	Owned switch	cascade port
User 1	2	1/2	Switch 1	1/1
User 2	3	1/3	Switch 1	1/1
User 3	2	1/2	Switch 2	1/1
User 4	3	1/3	Switch 2	1/1

You need to configure on two switches。

Switch 1 configuration：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-vlan)#vlan 3

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 2

Switch(config-ge1/1)#switchport trunk allowed vlan add 3

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 3

Switch 2 configuration：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk allowed vlan add 2

Switch(config-ge1/1)#switchport trunk allowed vlan add 3

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 2

Switch(config-ge1/2)#exit

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 3

2) Troubleshooting

Inter switch VLAN, within the same VLAN PC can communicate, if not. Must see below：

- Connect the PC port is belong to the corresponding VLAN, and the application of ACCESS model to join the VLAN。
- The cascade port 1/1 is added to each VLAN, and port 1/1 is TRUNK mode。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.4 MAC, IP subnet, protocol VLAN

VLAN based on MAC is based on the source text MAC address to be divided。After receiving the untagged (or tag 0) message from the port, the VLAN of the message is determined according to the source MAC address of the message, and then the message is automatically divided into the designated VLAN transmission;

VLAN based on IP subnet is divided according to IP address and subnet mask of newspaper source。After receiving the untagged message from the port, the VLAN of the message is determined according to the source address of the message, and then the message is automatically divided into the designated VLAN transmission。This feature is mainly used to send messages from designated network segments or IP addresses in specified VLAN;

Protocol based VLAN assigns different VLAN ID to the message according to the protocol type of the message received by the port。The protocols that can be used to divide VLAN are IP, IPV6, IPX, etc.。

Before configuring VLAN based on MAC, IP subnet and protocol, the corresponding VLAN must be created first。

command	describe	CLI mode
mac-vlan mac WORD vlan <1-4094>	Create a VLAN based on the source MAC address	Interface configuration mode
no mac-vlan mac WORD	Deleting a VLAN based on the source MAC address	Interface configuration mode
no mac-vlan	Delete all VLAN based on the source MAC address	Interface configuration mode
show mac-vlan	Displays all VLAN based on the source MAC address	Privileged mode
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Creating a VLAN based on source IP subnet	Interface configuration mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Deleting a VLAN based on the source IP subnet	Interface configuration mode
no ip-subnet-vlan	Delete all VLAN based on source IP subnet	Interface configuration mode
show ip-subnet-vlan	Display all VLAN based on source IP subnet	Privileged mode
protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>) vlan <1-4094>	Creating a protocol based VLAN	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

no protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>)	Deleting a protocol based VLAN	Interface configuration mode
no protocol-vlan	Delete all protocol based VLAN	Interface configuration mode
show protocol-vlan	Show all protocol based VLAN	Privileged mode
show vlan-partition interface IFNAME	The display interface enables VLAN based on MAC, IP subnet, protocol	Privileged mode

6.5 Voice VLAN

Voice VLAN is a specialized VLAN for voice data streams of users。 By the division of Voice VLAN and the voice connection port of the device to join Voice VLAN, for voice data configuration of QoS (Quality of Service, to improve the quality of service) parameters, voice data message priority, ensure the quality of communication。

The device can determine whether the data stream is a voice data stream according to the source MAC address OUI field in the data packet entering the port。The source MAC address conforms to the system settings of the voice device OUI address of the packet is considered to be voice data stream, is divided into Voice VLAN transmission。

The user can preset the OUI address or use the default OUI address as the judgment standard, as follows

Serial number	OUI address	Manufacturer
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Manually add IP access port to Voice VLAN。Then, by identifying the source MAC of the message and matching the OUI address, after the match is successful, the system will send priority to the ACL rules and configuration messages。

Voice VLAN security mode and common mode, safe mode：Only OUI matched language streams are allowed to be transmitted in Voice VLAN, while OUI mismatched data streams are not allowed to be transmitted in Voice VLAN；Normal mode: All data streams can be transmitted in the voice VLAN。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Before configuring Voice VLAN, you must first create the corresponding VLAN。

command	describe	CLI mode
voice-vlan security (enable|disable)	Voice VLAN security mode enable	Global configuration mode
voice-vlan oui WORD mask WORD	Configuring user OUI	Global configuration mode
voice-vlan oui WORD mask WORD description WORD	Configure user OUI and name	Global configuration mode
no voice-vlan oui WORD mask WORD	Deleting user OUI configuration through OUI address and mask	Global configuration mode
no voice-vlan oui description WORD	Delete user OUI configuration by name	Global configuration mode
no voice-vlan oui	Delete all user OUI configuration	Global configuration mode
no voice-vlan default-oui WORD mask WORD	Deleting defualt OUI configuration through OUI address and mask	Global configuration mode
no voice-vlan default-oui description WORD	Delete defualt OUI configuration by name	Global configuration mode
no voice-vlan default-oui	Delete all defualt OUI configurations	Global configuration mode
voice-vlan default-oui resume	Restore all defualt OUI configurations	Global configuration mode
show voice-vlan oui	Display all defualt and user OUI configuration	Privileged mode
voice vlan <1-4094> (enable|disable)	Interface enable Voice VLAN	Interface configuration mode
voice vlan qos map-queue <0-7> remark-dscp <0-63>	The interface configuration QoS priority, default queue is 6, DSCP is 46	Interface configuration mode
no voice vlan qos	Restore interface QoS priority default configuration	Interface configuration mode
no voice vlan	Delete interface configuration Voice VLAN	Interface configuration mode
show voice-vlan state	Display all interfaces configured with Voice VLAN	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.6 VLAN mapping

The VLAN mapping (i.e., VLAN Mapping) function can modify the message carried VLAN Tag, providing the following mapping relationship: 1:1 VLAN mapping: the message carrying VLAN Tag in VLAN ID is modified to another VLAN ID。

Before configuring the VLAN map, the corresponding VLAN must be created first。

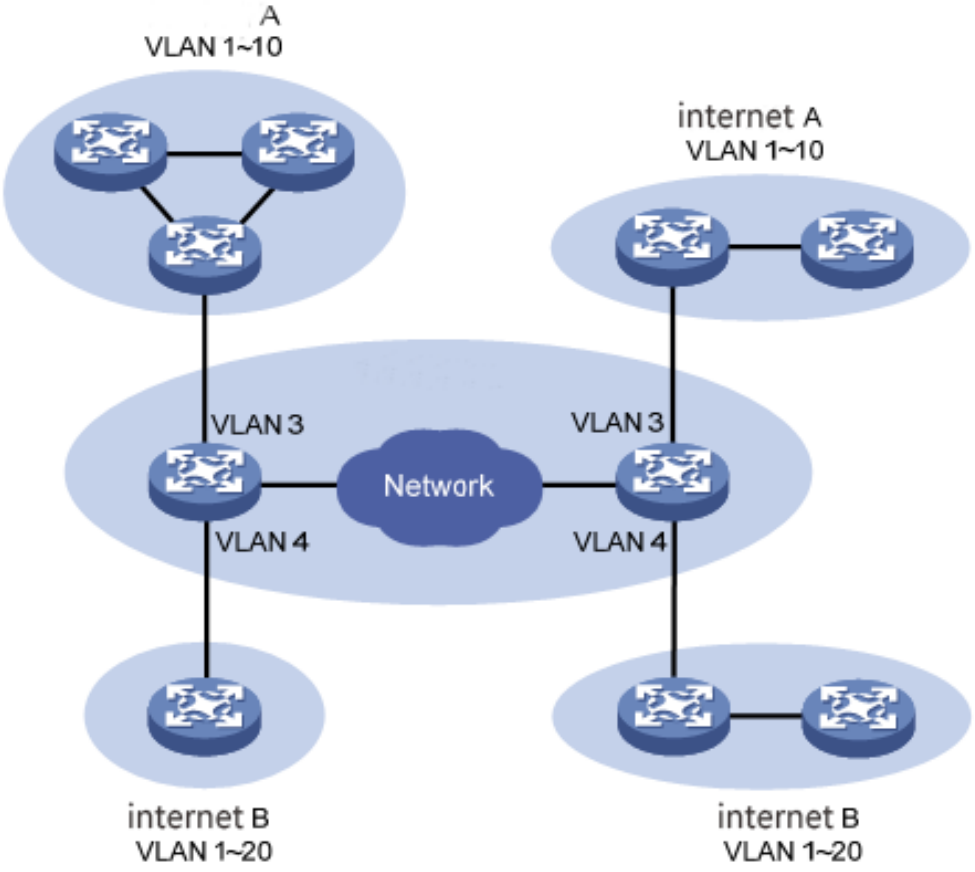
command	describe	CLI mode
vlan-mapping vlan <1-4094> map-vlan <1-4094>	A VLAN mapping relation for configuring ports	Interface configuration mode
no vlan-mapping vlan <1-4094>	A VLAN mapping relation for deleting ports	Interface configuration mode
no vlan-mapping	All VLAN mapping relationships for deleting ports	Interface configuration mode
show vlan-mapping	Display the VLAN mapping of all configurations	Privileged mode

6.7 QinQ

The characteristics of QinQ port device is provided with a simple and flexible two layer VPN technology, it through the operator's network edge device for users on the private network packet encapsulation layer VLAN Tag backbone network, messages that carry two layer VLAN Tag traversal operators (public)。In the public network, only according to the outer VLAN Tag equipment to transmit the message, and the message of the source MAC address table to study the outer Tag where the VLAN MAC address table, and private network VLAN Tag users in the transmission process will be as part of the data packets to be transmitted。

The QinQ feature enables an operator to use a VLAN to serve a network of users with multiple VLAN。As shown below, the user network A private network VLAN is VLAN 1~10, the user network B private network VLAN is VLAN 1~20。The A allocated by the operator to the user network VLAN is VLAN 3, and the VLAN allocated for the user network B is VLAN 4。When the user A network with VLAN Tag packets in the network operators, the message will be outside the package on a layer of VLAN ID 3 VLAN Tag; when the user B network with VLAN Tag packets in the network operators, the message will be outside the package on a layer of VLAN ID 4 VLAN Tag。In this way, packets of different user networks are completely separated from each other in public network transmission. Even if the VLAN range of two user networks overlaps, there is no confusion in the public network transmission。

SEC.RU | Короткий путь к информации
Скачано с sec.ru



QinQ features enable the network to provide 4094X4094 VLAN at most, and meet the requirement of VLAN in metropolitan area network， It mainly solves the following problems：

(1) Alleviate the increasingly shortage of public network VLAN ID resources。

(2) Users can plan their own private network VLAN ID, and will not lead to conflict with the public network VLAN ID。

(3) Provide a relatively simple two layer VPN solution for small metropolitan area network or enterprise network。

QinQ can be divided into two types: basic QinQ and flexible QinQ。

(1) Basic QinQ: basic QinQ is implemented on port mode。After opening the basic QinQ function of the port, when the port receives the message, the device will send the message default VLAN VLAN Tag for this message。If the received message is already VLAN Tag, the message becomes a double Tag message; if the received message is not VLAN Tag, the message becomes a message with port default VLAN Tag。

(2) Flexible QinQ: flexible QinQ is a more flexible implementation of QinQ, which is based on the combination of port and VLAN。In addition to all the basic functions of the QinQ, the message received by the same port can also do different actions according to the different VLAN, so as to add different external VLAN Tag for packets with different inner layer VLAN ID。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
qinq tpid WORD	Configure the TPID value carried in port VLAN Tag, default to 0x8100	Interface configuration mode
no qinq tpid	Recovery port default TPID	Interface configuration mode
qinq uplink	Configuration port is uplink port	Interface configuration mode
no qinq uplink	Uplink configuration for canceling ports	Interface configuration mode
qinq customer	Configuration port is customer port	Interface configuration mode
no qinq customer	Customer configuration for canceling ports	Interface configuration mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	A VLAN conversion for configuring interfaces	Interface configuration mode
no qinq inner-vid VLAN_ID	A VLAN conversion for deleting interfaces	Interface configuration mode
no qinq outer-vid <1-4094>	A VLAN conversion for deleting interfaces	Interface configuration mode
show qinq	Display all configured QinQ conditions	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Seventh chapters

QoS configuration

This chapter describes the QoS and its configuration, including the following：

- QoS introduce
- QoS configuration
- Example of basic QoS configuration
- Policy QoS configuration example

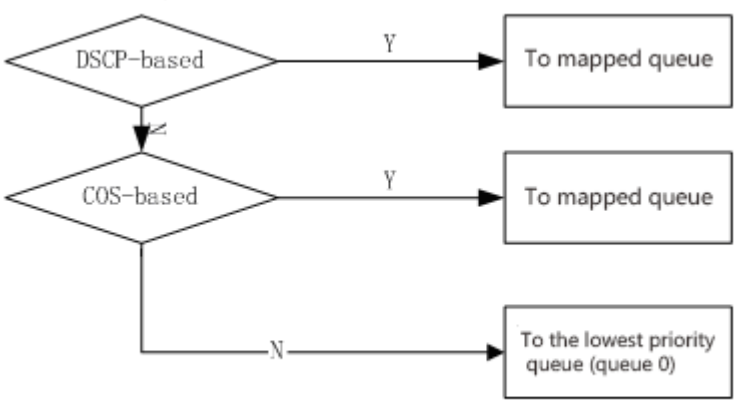
7.1 QoS introduce

Using the QoS function of the switch, you can make the important data stream forwarded by the switch get priority processing, make your network bandwidth utilization more reasonable, network performance become predictable。

In the packet is determined at the input end according to the priority information of the packet。

The switch implements QoS based on COS (802.1p), QoS based on DSCP (DiffServ) and QoS based on MAC. A DSCP based QoS can be configured on a physical port; the physical port defaults to start the QoS based COS。

The following is a QoS enabled packet forwarding flow：



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switches support 0~7 eight priority queues, queue 7 has the highest priority, and queue 0 has the lowest priority. There are three kinds of priority queue scheduling methods: SP, WRR, WFQ。SP is the strict priority scheduling, the priority queue is always forwarding 7 data packets, until the queue 7 packets forwarding is completed, began to queue 6 queue 6 packets, packet forwarding is completed before forwarding queue 5 packets, the packet forwarding queue 0. WRR is a weighted priority polling switch in forwarding packets, according to the distribution of the rights of the high priority queue to low priority queue polling packet forwarding, forwarding number first right from the high priority data packet forwarding in the right time the number of data packets with high priority and low priority queue forward until the end. From the high priority class began to push forward.。WFQ and WRR queue scheduling algorithm is similar, in the weight algorithm support byte-count and weight, also support SP packet, can replace each other. The difference is as follows: WRR supports a maximum delay, can guarantee the maximum delay of the configuration message in the queue from entering the queue to the maximum time to leave the queue does not exceed the set; WFQ supports guaranteed bandwidth, minimum queue bandwidth can guarantee the port traffic congestion when available。

In order to facilitate user configuration, we introduce the concept of QosProfile。QosProfile is an attribute of the mapping relationship configured with 802.1p and priority queues, which cannot be configured by the user。Their mapping relationships are as follows:

QosProfile	802.1p(CoS)	priority queuing
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp7	7	7

7.1.1 QoS based on COS

The port is enabled by default based on COS QoS. The exchange opportunity obtains the priority value of the VLAN TAG in the packet entering the port, and determines the output queue of the packet according to the mapping relationship between the user configured COS value and

SEC.RU | Короткий путь к информации
Скачано с sec.ru

the queue。If the data packet is not VLAN TAG or VLAN TAG VID is 0, then the switch will according to the user configuration of the port and the port of the VID default default priority fill the data package, and then according to the output queue of the packet determines the default priority。

7.1.2QoS based on DSCP

If a port is enabled DSCP based on QoS, then exchange the opportunity to acquire IP data packets into the port of the DSCP values in the output queue and decide the packet according to the mapping relation between the DSCP value and user configuration of the queue。

The cos-dscp type is an extension based on the DSCP type cos type, which is essentially a DSCP type or a cos type。If the cos-dscp type is used, the IP message system will automatically match the DSCP priority, and the non IP message system will be based on the cos priority。According to the priority type (dscp/cos), the corresponding scheduling is carried out。

7.1.3 Policy based QOS

The QoS policy includes classes and policy actions. The class is used to identify the stream, and the user can define a series of rules by the command to classify the packet; the policy action is used to define the QoS action of the message of the matching rule。If a port enabled strategy based on QoS, the switch will enter the port of packet classification, to meet the requirements of the classification of data packets, packet switch will according to the strategy of action processing of the port data corresponding to, does not meet the requirements of packet classification is not processed, then the output queue according to the priority mapping the relationship between decision of the packet。

7.2 QoS configuration

7.2.1 Default configuration for QoS

Configuration item	value	Whether it is configurable
Queue number	8	no
Dispatching mode	WRR	yes
Whether to enable SP scheduling	disable	yes
Whether to enable WFQ scheduling	disable	yes

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Queue weight	qp0[1],qp1[2],qp2[4],qp3[8],qp4[16] qp5[32],qp6[64],qp7[127]	yes
The mapping relation between COS and qosprofile	COS0[qp0] COS1[qp1] COS2[qp2] COS3[qp3] COS4[qp4] COS5[qp5] COS6[qp6] COS7[qp7]	no
The mapping relation between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP64[qp7]	yes
The attributes of Qosprofile	qp0 cos[0] 0 qp1 cos[1] 1 qp2 cos[2] 2 qp3 cos[3] 3 qp5 cos[4] 4 qp5 cos[5] 5 qp6 cos[6] 6 qp7 cos[7] 7	no
Whether the interface enables DSos based on DSCP	disable	no
Whether the interface enables COS-based qos	enable	no
Interface user priority (COS value)	0	**yes**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.2.2 Configuration scheduling mode

The default scheduling of switches is WRR. The configuration of SP and WFQ can be configured by command。

command	describe	CLI mode
qos sched { sp | wrr | wfq}	Configuring QoS scheduling	Interface configuration mode

7.2.3 Configuring queue weights

command	describe	CLI mode
qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight <1-127>	Configure the weight of each priority queue	Interface configuration mode
no qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight	The weight of the recovery queue is configured as the default configuration	Interface configuration mode

Queue weight is the number of packets forwarded by a priority queue when polling and forwarding. Therefore, when configuring the queue weight, it should be noted that the weight of the low priority queue does not exceed the weight of the high priority queue。

7.2.4 Configure the mapping relationship between DSCP and QosProfile

command	describe	CLI mode
qos dsc-map-qp <0-63> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7}	Mapping relations between DSCP and qosprofile。	Global configuration mode
no qos dscp-map-qp <0-63>	Restoring the mapping between DSCP and qosprofile is the default configuration。	Global configuration mode

7.2.5 Configuring port QoS

QoS policy configuration steps: define class, define policy action, application strategy。

Define a class and define a set of flow classification rules：

A total of 802.1p priority, DSCP, ACL three flow classification rules, a class can only use a

SEC.RU | Короткий путь к информации
Скачано с sec.ru

set of flow classification rules, a group of flow classification rules can be used by multiple class. The default configuration does not match any rules。

command	describe	CLI mode
qos class <1-256> name WORD	Naming a specified class	Global configuration mode
qos class <1-256> match cos <0-7> (<0-7>…)	Define a matching 802.1p priority rule, which can configure 8 rules at once	Global configuration mode
qos class <1-256> match dscp <0-63> (<0-63>…)	Defining matching DSCP rules allows you to configure 8 rules at once	Global configuration mode
qos class <1-256> match acl <1-99>|<100-199>…	Define matching ACL rules, only 1 groups of rules can be configured at one time	Global configuration mode
no qos class <1-256>	Restore default configuration	Global configuration mode
show qos class (<1-256>|)	Displays information about configured classes	Privileged mode

Define a strategy and define a set of QoS actions for matching rules：

There are six kinds of QoS actions, such as mapping message output queue, re marking DSCP, counting, copying to CPU, mirroring, speed limiting, in which copy to CPU and mirror can not be configured at the same time。 A policy can connect multiple class, and a class can be connected by multiple policy。A group of QoS actions can be used when a policy is connected to a class. In default configuration, policy does not connect to any class, nor does it use any QoS action。

command	describe	CLI mode
qos policy <1-256> name WORD	Naming the specified policy	Global configuration mode
qos policy <1-256> class <1-256> remark dscp <0-63>	Matching classification rules, marking the DSCP value of the message	Global configuration mode
no qos policy <1-256> class <1-256> remark	The action of removing the re marking message	Global configuration mode
qos policy <1-256> class <1-256> meter <1-1000000> <1-65535>	Matching classification rules restrict the bandwidth and burst traffic of packets	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

no qos policy <1-256> class <1-256> meter	Removal of restricted message bandwidth and burst traffic	Global configuration mode
qos policy <1-256> class <1-256> statistic-packets	Match the classification rules, and count the number of messages	Global configuration mode
no qos policy <1-256> class <1-256> statistic-packets	The action of removing the number of statistical messages	Global configuration mode
qos policy <1-256> class <1-256> mirror-to cpu	Matching classification rules, message mirroring to CPU	Global configuration mode
qos policy <1-256> class <1-256> mirror-to monitor-interface	Matching classification rules, message mirroring to mirror port (mirror port configuration is effective)	Global configuration mode
no qos policy <1-256> class <1-256> mirror	Remove the action of mirroring messages	Global configuration mode
no qos policy <1-256> (class <1-256>|)	Strategy deletes corresponding matching rules and actions	Global configuration mode
qos policy <1-256> class <1-256> map-queue <0-7>	Match the classification rules and assign messages to the corresponding output queue	Global configuration mode
no qos policy <1-256> class <1-256> map-queue	Match the classification rules and assign messages to the default output queue 0	Global configuration mode
clear interface IFNAME qos policy statistic-packets	Clear the statistical information of the interface QoS policy	Global configuration mode
show qos policy (<1-256>|)	Display information about configured policies	Privileged mode
show qos	Display the information of the configured QoS	Privileged mode

Apply policy and apply corresponding strategy to interface;

An interface only has one policy and only one policy can be used by multiple interfaces。

A port can only be enabled to select and enable a QoS. The QoS function can only be configured on the physical port and can not be configured in the TRUNK group or the three layer interface。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
qos {dscp-based| cos-based| dscpcos-based| apply-policy <1-256>}	Enable port QoS function。	Interface configuration mode
no qos	Restore default port-based。	Interface configuration mode
show qos	Display configuration information for all QoS	Privileged mode
show qos interface IFNAME	Display interface configuration of QoS information	Privileged mode
show qos interface	Display the QoS information of all interface configurations	Privileged mode

7.2.6 Configuring the port user priority (COS value)

command	describe	CLI mode
qos user-priority <0-7>	Configuring the user priority (COS value) of the port	Interface configuration mode
no qos user-priority	The user priority (COS value) of the recovery port is the default configuration。	Interface configuration mode

7.3 Example of basic QoS configuration

Configuring the ge1/3 user priority (COS value) is 3, and the COS based QoS function defaults to boot：

Switch#configure terminal

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos user-priority 3

Switch#(config-ge1/3)#end

Configure the interface ge1/3 to start the DSCP based QoS function and map the DSCP value 3 to the priority queue 2：

Switch#configure terminal

Switch#(config)#qos dscp-map-qp 3 qosprofile qp2

Switch#(config)#interface ge1/3

Switch#(config-ge1/3)#qos dscp-based

Switch#(config-ge1/3)#end

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.4 Policy QoS configuration example

Configure ACL to capture data streams of source MAC1, MAC2, MAC3, respectively（ACL rules can be modified according to requirements, but here are just a few examples）

access-list 700 permit host 0000.0000.1111 vid any ip any any

access-list 701 permit host 0000.0000.2222 vid any ip any any

access-list 702 permit host 0000.0000.3333 vid any ip any any

Configure the QOS class to match the data streams of source MAC1, MAC2, and MAC3, respectively（You can modify the matching rule cos or DSCP according to the requirement, which is just a simple example）

qos class 10 match acl 700

qos class 11 match acl 701

qos class 12 match acl 702

Configure the QOS policy to mark the 802.1p priority of the data streams of MAC1, MAC2, and MAC3, respectively

（You can modify policies according to requirements, but here are just a few examples）

qos policy 10 class 10 remark cos 7

qos policy 10 class 11 remark cos 5

qos policy 10 class 12 remark cos 3

Send QOS policy to port

interface ge1/23

qos apply-policy 10

Check the configuration information, the analysis of the test results in G1/24 portSwitch#show qos interface ge1/23

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Eighth chapters

MSTP configuration

This chapter describes the MSTP and its configuration, including the following：

- MSTP introduce
- MSTP configuration
- MSTP configuration example

8.1 MSTP introduce

switch supports IEEE802.1d, IEEE802.1w, IEEE802.1s standard STP protocol。

8.1.1 overview

MSTP uses RSTP to converge quickly so that multiple VLAN can be aggregated into a spanning tree instance, and each instance has a spanning tree topology that is independent of the other spanning tree instances. This architecture provides multiple forwarding paths for data streams, can load balance, and reduce the number of spanning tree instances that are required to support a large number of VLAN。

8.1.2 Multiple spanning tree domains

For instances involved in multiple spanning tree (MST) computations, the same MST configuration information must be configured in a consistent manner。A set of connected switches that have the same MST configuration form the MST domain。

The MST configuration determines the domain to which each switch belongs. The configuration includes domain name, revision number, and MST instance and VLAN assignment

SEC.RU | Короткий путь к информации
Скачано с sec.ru

mapping; this information generates a unique abstract (Digest) in the MST configuration。The summaries in the same domain are the same, and they must be the same. You can look at the information through the show spanning-tree MST config command。

One domain can have one or more members with the same MST configuration; each member must have the ability to process RSTP BPDU。There are no restrictions on the number of MST domains in a network, but each domain supports 16 instances at most. You can only assign one VLAN to one spanning tree instance at a time。

8.1.3 IST, CIST, and CST

The internal spanning tree (IST), the spanning tree running in the MST domain。

In each MST domain, MSTP maintains multiple instances of creation。Instance 0 is a special instance of a domain called IST。All other MST instances are numbers 1 to 15。

This IST is just a spanning tree instance of receiving and sending BPDU; all other spanning tree instance information is compressed in MSTI BPDU。Because MSTI BPDU carries all the instance information, it needs to be handled by a switch that supports multiple spanning tree instances, which means simplifying the number of BPDU。

All in the same domain MST instances share the same protocol timer, but each MST instance has its own topology parameters, such as a root switch ID, root path cost etc.。By default, all VLAN is assigned to IST。

The common and internal spanning tree (CIST) is a collection of all spanning trees in every MST domain, and the common spanning tree that connects the MST domain and the single spanning tree (IST)。

The spanning tree computed in a domain looks like a subtree of CST that contains all the switch domains。CIST is formed by the spanning tree computation results between switches that support 802.1W and 802.1D protocols。The CIST in MST domain is the same as that in CST domain。

Common spanning tree (CST), spanning spanning tree between MST domains。

8.1.4 Intra domain operation

IST connects all the MSTP switches in a domain. When IST converges, the root of IST becomes IST master, which is the minimum bridge ID in the domain and the path overhead of the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

switch to the CST root. If there is only one domain in the network, IST master is also the CST root. If the CST root is out of bounds, a MSTP switch at the domain boundary (boundary) is chosen as IST master。

When a MSTP switch is initialized, it sends BPDU to itself as the CST root and IST master, and the path cost to the CST root and IST master is set to 0. Switches also initialize all MST instances and require them to be their roots. If the switch receives MST root information than the current port information storage priority (low bridge ID, low cost and so on, it gives up the path) it became IST master requirements。

In initialization, a domain may have many sub domains, each of which has its own IST master. When the switch receives a more preferred IST information, it leaves its old sub domain and adds to the new sub domain that may contain the real IST master. Therefore, all sub domains are contracted, except for the real IST master subdomain。

In order to operate properly, all switches within the MST domain must recognize the same IST master. So, switches in any two domains synchronize the roles of the ports of one of their MST instances, only if they converge to a common IST master。

8.1.5 Inter-domain operation

If there are multiple domains or early 802.1D switches in the network, MSTP establishes and maintains CST, which contains all the MST domains in the network and all the early STP switches. MST instances join IST in domain boundaries (boundary) to become CST.

IST connects all switches in the MSTP domain and looks like a subtree of CST (surrounded by all switch domains), and the root of the subtree becomes IST master. The MST domain looks like a virtual switch adjacent to the STP switch and the MST domain。

Only CST instances send and receive BPDU, and MST instances increase their spanning tree information to BPDU to interact with neighbor switches and compute the last spanning tree topology. Because of this, the spanning tree parameters involved in BPDU transfers (such as hello time, forward time, max-age and max-hops) are configured only in CST instances, but not all MST instances. Parameters involved in the spanning tree topology (e.g., switch priority, port VLAN cost, port VLAN priority) can be configured in CST instances and MST instances。

MSTP switches use version 3 RSTP BPDU or 802.1D BPDU and 802.1D switch communication. MSTP switches communicate by using MSTP BPDU and MSTP switches。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.1.6 Hop count

The IST and MST instances do not use message-age and maximum-age information in the BPDU that configure the spanning tree topology。Instead, use the path to the root and spend the equivalent of IP TTL hop-count mechanism。

You can configure the maximum number of hops for that domain and apply it to that domain IST and all MST instances. The number of hops calculations is the same as the message-age result (decided after initiating a reconfiguration). The instance root switch always sends a BPDU (or-M-record) with cost 0 and hop-count as the maximum. When a switch receives a BPDU, it decrements the remaining hops and propagates the remaining hops in the BPDU it generates. When the count reaches 0, the switch drops the BPDU and age the information for that port。

In a domain, the Message-age and maximum-age information in the RSTP BPDU section is consistent, and the same value is spread over the specified port of the domain (boundary)。

8.1.7 Boundary port

A boundary is a spanning tree domain that connects an MST region to a single RSTP, or a spanning tree domain of 801.1D alone, or a different MST region. A border port is also connected to a LAN, and the designated switch for this LAN is either a single spanning tree switch or a switch with a different MST region configuration。

At boundary ports, the MST port roles are not important, and their states are forced to be the same as the IST port state (when the IST port is forwarding, the MST port at the boundary is forwarding). A IST port on the boundary can have any role other than the backup port。

In a shared boundary connection, the MST port waits for the forward-delay time expiration in the blocking state before it is converted to the learning state. The MST port waits for another forward-delay time to expire before it is converted to forwarding。

If the boundary port is a point-to-point connection and is the IST root port, the IST port is converted to the forwarding state, and the MST port is converted to the forwarding state。

If a boundary port is converted to an forwarding state in an instance, it is forwarding in all instances, and a topology change is triggered. If a boundary port with a IST root or a specified port role receives a topology change notification, the MSTP switch triggers a topology change on the active port of the IST instance and all the MST instances。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.1.8 MSTP 802.1d and STP interoperability

A switch running MSTP supports a built-in protocol migration mechanism that enables him to coordinate with 802.1D. If the switch receives an 802.1D-configured BPDU from a port, it sends an 802.1D BPDU on that port. When a boundary port of a domain receives an 802.1D BPDU or a different MSTP BPDU or RSTP BPDU, the MSTP switch can detect。

However, if the switch is no longer receiving 802.1D BPDU, it will not automatically revert to the MSTP mode because it cannot determine whether the exchange of the other party has been deleted from the connection unless the other switch is the designated switch. Similarly, when a switch connected to this switch has been added to this domain, the switch may continue to assign a boundary port role to a port. Migration processing of restart protocol (mandatory and neighbor switch negotiation)。

If all of the switches on the other side are RSTP switches, they can handle MSTP BPDU and handle RSTP BPDU. Therefore, the MSTP switch is sent to the border port or to send a version 0 configuration and TCN BPDU or version 3 MSTP BPDU. A boundary port that connects to the LAN. His designated switch is either a separate tree switch or a switch with different MST configurations。

8.1.9 Port role

Fast convergence algorithm for MSTP using RSTP. This paper briefly introduces MSTP port role and fast convergence in combination with RSTP。

RSTP provides fast convergence of specified port roles and decision activity topologies. RSTP, based on IEEE802.1D STP, selects high priority switches as root switches. When RSTP specifies a port role to a port：

Root port — When forwarding packets to the root switch switch provides the optimal path cost。

Designated port — Connection specified switch。When forwarding packets from the LAN to the root switch have the lowest cost path. Specifies that the port through which the switch connects to the LAN is called a specified port。

Alternate port— Provides a replacement path to the root switch of the current root por。

Backup port—Backup of a path that plays a specified port to the spanning tree leaf。A Backup port exists only when the two ports are connected together in a point-to-point loop, or when a switch has two or more connections to a shared LAN segment。

Disable port—There is no port role in the spanning tree operation。

Master port — On the shortest path of the domain root or the total root, it is the port

SEC.RU | Короткий путь к информации
Скачано с sec.ru

connecting the domain to the total root。

The root port or the specified port role is included in the active topology. The replacement port or backup port role is not included in the active topology。

In a stable topology and fixed port role of the entire network, RSTP to ensure that every root port and the designated port immediately moved to the forwarding state when all the replacement port and backup port is always in the state of discarding. Port state control forwarding and learning processing。

Fast convergence

In the following case, RSTP provides fast recovery: switch failure, port failure, or LAN fault, which provides fast restoration for edge ports, new root ports, and connections to a point-to-point connection：

Edge ports — If you configure a port as an edge port, the edge port is immediately migrated to the forwarding state. You can open it as a boundary port only when this port is connected to a single terminal or to determine the device that does not need to compute the spanning tree。

Root ports — If RSTP selects a new root port. It blocks an old root port and immediately moves the new root port to the forwarding state。

Point-to-point links — If you connect a port to other ports through a point-to-point connection and local port into a designated port and other ports, it passes through the proposal-agreement handshake negotiation a rapid migration to determine a fast convergence without loop topology (loop-free)。

Topological change

This section describes the differences between RSTP and 802.1D in dealing with topological changes in spanning-tree。

Detection — Any transfer between blocking and 802.1D as the forwarding state will cause topology changes, only to migrate from blocking to forwarding to RSTP (state topology change just to increase the connectivity of the considered topology change). The state changes at one edge of the port (edge port) does not cause topology changes. When a RSTP switch investigates a topology modification, it is flooding it to learn information to all non edge ports (nonedge ports), in addition to receiving ports of TC information。

Notification — Unlike 802.1D, using TCN BPDU, RSTP doesn't use it. However, in order to 802.1D and interoperability, RSTP switch and TCP BPDU treatment。

Acknowledgement — When an RSTP switch receives a TCN message from a 802.1D switch at a specified port, it responds with a 802.1D BPDU and sets the TCA flag bit. However, if

SEC.RU | Короткий путь к информации
Скачано с sec.ru

TC-while timer (the same as 802.1D topology-change timer) is active, it connects to the 802.1D switch at the root port and receives a configuration BPDU with TCA, TC-while timer restart (reset). This behavior is only required to support the 802.1D switch. RSTP BPDU never has a TCA flag bit。

Propagation — When a RSTP switch receives a TC message from another switch through a specified port or root port, it propagates to all non edge ports, designated ports and root ports (except for the receiving port). All of these ports start TC-while timer and flood the information they learn。

Protocol migration — In order to backward compatible 802.1D switches, RSTP selectively sends 802.1D configuration BPDU and TCN BPDU based on each port。

When one is initialized and migrate-delay timer starts (the specified minimum value is sent during RSTP BPDU), the RSTP BPDU is sent. When this timer is active, the switch handles all the BPDU received from the port and ignores the protocol type。

After the port migration-delay timer has stopped, if the switch receives a 802.1D BPDU, it assumes that it is connected to a 802.1D switch and starts using the 802.1D protocol BPDU. However, if the RSTP switch is using 802.1D BPDU on a port, after receiving timer, a RSTP BPDU is received, which restarts the timer and starts using RSTP BPDU。

8.1.10 A brief introduction to 802.1D spanning tree

The spanning tree protocol is based on the following points：

1）There is a unique group address (01-80-C2-00-00-00) that identifies all switches on a particular LAN. This group of addresses can be identified by all switches；

2）Each switch has a unique identifier (Brideg Identifier)；

3）The port of each switch has a unique port identifier (Port Identifier). Spanning tree configuration management also requires: for each switch tuning a relative priority; each port of each switch is a relative priority of each port; take a path of coordination。

The switch with the highest priority is called the root (root) switch. Each switch port has a root path cost, and the root path cost is the sum of the cost of each segment of the switch to the root switch. The minimum value of the root path in a switch is called the root port, and if there are multiple ports with the same root path cost, the port with the highest priority is the root port。

In each LAN, there is a switch called the designated (designated) switch, which belongs to the least cost switch in the root path of the LAN. The port that connects the LAN to the specified switch is the designated port of the LAN (designated port). If more than two ports in the specified

SEC.RU | Короткий путь к информации
Скачано с sec.ru

switch are connected to this LAN, the port with the highest priority is selected as the specified port。

The essential factors that determine the formation of a spanning tree：

1）Decision root switch

a、At first, all switches considered themselves to be root switches；

b、The switch sends the configuration BPDU to the connected LAN broadcast, whose root_id is the same as the bridge_id；

c、When the switch receives another switch configuration BPDU, if it is found that the root_id field is received in the configuration BPDU value is greater than the value in the root_id parameter of the switch, the frame is discarded, or root_id, update the switch takes root path parameters such as root_path_cost value, the switch will continue to broadcast to a new value the configuration of BPDU。

2）Decision root port

The minimum value of the root path in a switch is called the root port。

If multiple ports have the same minimum root path cost, the port with the highest priority is the root port。If two or more ports have the same minimum root path cost and the highest priority, the port with the smallest port number is the default root port。

3）Designated switch for LAN

a、At first, all switches consider themselves to be the designated switches of LAN。

b、When the switch receives the BPDU sent by other switches in the same LAN (the same) with a lower root path, the switch no longer claims that it is the designated switch. If there are two or more switches with the same root path cost in a LAN, the switches with the highest priority are selected as the designated switches。

c、If you specify a switch at a time one other LAN switch due to competition and sent to the specified switch configuration BPDU, the specified switch will send a response to the BPDU configuration, to re determine the designated switch。

4）Determining the specified port

The specified port in the specified switch of LAN is connected to the LAN port. If the specified switch has two or more ports connected to the LAN, then the port with the lowest identification port is the specified port。

In addition to the root port and the specified port, the other ports are blocked. In this way, the topology of a spanning tree is determined after deciding the root switch of the root switch, the switch, and the designated switch and designated port of each LAN。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.2 MSTP configuration

8.2.1 Default configuration

Command parameter	Default value
spanning-tree mst enable(Start MSTP)	Close
Spanning-tree mst priority(Switch CIST priority)	32768
spanning-tree mst hello-time(switch cist hello-time)	2 秒
spanning-tree mst forward-time(switch cist forward-time)	15 秒
spanning-tree mst max-age(switch cist max-age)	20 秒
spanning-tree mst max-hopsswitch cist max-hops)	20 秒
instance 1 priority (Instance priority)	32768
spanning-tree mst instance 1 priority(Port instance priority)	128
spanning-tree mst instance 1 path-cost(Port instance path-cost)	20000000
spanning-tree mst priority （port cist priority）	128
spanning-tree mst path-cost（port cist path-cost）	20000000

8.2.2 General configuration

Start MSTP

When the system is started, the default configuration MSTP is closed。

The configuration process for starting MSTP is：

Switch#configure terminal

Switch(config)#spanning-tree mst enable

The command to close MSTP is：

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configuration max-age

Configuring max-age is the configuration of all instances. Max-age is the number of seconds when the switch waits for the configuration information of the spanning tree before triggering a reconfiguration。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The default configuration is 20 seconds, and the configuration range is 6 to 40 seconds。

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Configuration max-hops

Max-hops is the number of hops specified before a BPDU is discarded in a domain。

The default value is 20, and the configuration range is 1 to 40。

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Configuration forward-time

Configuring forward-time is for all instances. Forward-time is the number of seconds that ports wait from discarding to learning and from learning to forwarding。

The default configuration is 15 seconds, and the configuration range is 4 to 30 seconds。According to the generation number protocol forward-time, the following conditions must be satisfied：2*(forward-time – 1) >= max-age。

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Configuration hello-time

Configuring hello-time is the configuration of all instances. Hello-time is the time interval for root switches to generate configuration information。

The default configuration time is 2 seconds, and the configuration range is 1 to 10 seconds. According to the generation number protocol hello-time, the following conditions must be satisfied：2*(hello-time + 1) =< max-age。

Configuration process：

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Configure the priority of CIST bridge (priority)

The default configuration 32768, the configuration range <0-61440>; the CIST priority value is only 4096 multiples。

Configuration process：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Configuration and CISCO compatibility

network switch uses MSTP protocol based on 802.1s, each MSTI message length is 16 bytes; and CISCO switch BPDU, each MSTI message length is 26 bytes. In order to interact with the CISCO switch, switches that configure the network need to start the CISCO compatible switch。

In the case of starting and CISCO compatible configuration, the same domain is considered as long as the domain name and the revision number are the same when judging whether the domain is the same。

The default system does not start this function。

Open and CISCO compatible：

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Close and CISCO compatible：

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Reset protocol checking task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the protocol of the other system running. Determine the protocol for the port running according to the protocol running by the other party。

In some cases reset protocols are required. For example, the system negotiated a port to run the STP protocol, and after a period of time, the other side of the device running STP protocol has been replaced by a host. When I need to configure the port for fast port, but the port has been running the STP protocol, and the protocol negotiation task has stopped; then need to reset this protocol negotiation task let it re negotiation between it and the host protocol。

Reset the protocol reconnaissance task of the whole device：

Switch#clear spanning-tree detected protocols

The protocol reconnaissance task of resetting a port：

Switch#clear spanning-tree detected protocols interface <if-name>

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.2.3 Domain configuration

Two or more devices in the same domain, they must have the same VLAN instance mapping relationship, the same modified version number and the same domain name。

One domain has one or more members with the same MST configuration, and each member can handle the RSTP BPDUS capability. There are no restrictions on the number of members in a network, but each domain can support up to 16 instances。

The configuration of the instance is explained in the instance configuration, which only introduces the domain name configuration and the revision version number configuration。

Configuring domain names：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#region <region-name>

Configuration revision number：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

8.2.4 Instance configuration

The system supports 16 instances, and the scope of the instance ID number is 0-15. A VLAN can only be assigned to a spanning tree instance at a time。

By default, there is only one instance 0, and all of the VLAN belong to this instance。

The process of configuring an instance：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Configure the priority of MSTI bridge (priority)

The default configuration 32768, the configuration range <0-61440>; the MSTI priority value is only 4096 multiples。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Configuration process：

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

8.2.5 port configuration

The port configuration information associated with MSTP is described below. Here only the simple configuration section, port fast and root guard, are introduced separately。

The process of configuring a port to join an instance：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id>

Configure the priority of the CIST port (priority)

The default configuration is 128, the configuration range is <0-240>, and the priority value of the CIST port is only multiples of 16。

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst priority <priority>

Configure the priority of the MSTI port (priority)

The default configuration is 128, the configuration range is <0-240>, and the priority value of the MSTI port is only multiples of 16。

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Configure the CIST port path cost (path-cost)

The default configuration is 20000000 and the configuration range is 1-200000000. The following is the bandwidth and path change mapping table：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

bandwidth(bps)	Path cost
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

Configure the MSTI port path cost (path-cost)

The default configuration is 20000000 and the configuration range is 1-200000000. Bandwidth and path and the above table costs。

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Configure the version number of the send protocol package

The default configuration sends the MSTP protocol package with a configuration range of 0-3 and a mapping relationship of 0-stp, 2-rstp, 3-mstp。

Configuration process：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)# spanning-tree mst force-version <version-id>

Configure connection type

If connected to the other port a port through the point-to-point mode, and become a local port (designated port, RSTP proposal-agreement through the designated port) (proposal agreement) negotiation a rapid migration of its connected ports become the root port to determine a loop free topology。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Here is a brief introduction to the negotiation process of proposal-agreement。

When the switch receives a proposal message on one of its ports and the port is selected as the new root port, RSTP forces all other ports to synchronize the new root port information。

If all other ports are synchronized with the better (superior) root information received from the root port, the switches are synchronized。

When RSTP forces it to synchronize the new root information, if a specified port is in the forwarding state and is not configured as an edge port, it migrates to the blocking state. Typically, when the RSTP forces a port to synchronize a new root message and the port does not satisfy the above conditions, the port state is set to blocking。

When all ports are synchronized, the switch sends a agreement message to the corresponding port of the root port. When the switch is connected to a point-to-point connection in their port role of agreement, the RSTP immediately transfers the port state to forwarding。

If shared connection, the 802.1D port is calculated to determine the state of the port。

The default port connection type is point-to-point connection。

The connection type of the configuration port is point-to-point connection：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst link-type point-to-point

The connection type of configuration port is shared connection：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config-ge1/2)#spanning-tree mst link-type shared

8.2.6 PORTFAST related configuration

1) Port Fast

Port Fast immediately transfers a access or trunk port from the blocking state to the forwarding state, bypassing the listening and learning states. You can connect to a separate workstation and server using Port Fast, which allows these devices to connect to the network immediately without waiting for spanning tree to converge。

Configure a port for fast port：

Switch#configure terminal

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

2) BPDU Filtering

BPDU filtering can be opened globally based on switches or based on each port, but their characteristics are different。

In the global layer, you can use the spanning-tree MST portfast bpdu-filter command to start the BPDU filtering function on the port of the portfast bpdu-filter default state。

In the port layer, you can open BPDU filter on any port with spanning-tree MST portfast bpdu-filter enable。

This function prevents port fast ports from receiving or sending BPDU。

Configuring BPDU Filtering

In global configuration mode：

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

Under the interface configuration mode：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

BPDU protection features can be opened globally or based on each port, but their characteristics are different。

In the global layer, you can use the spanning-tree MST portfast bpdu-guard to open the BPDU guard function on the port of the portfast bpdu-gurad default state。

In the port layer, you can open BPDU guard on any port。

When the port configured with BPDU gurad receives BPDU, spanning tree will port the shutdown. In an efficient configuration, the port of Port Fast-enabled does not receive BPDU. A BPDU is received at an Port Fast-enabled port to represent an invalid configuration, for example, a connection to an unauthorized device, and BPDU guard enters a error-disabled state。

Error-disabled is when the port of starting BPDU gurad receives BPDU, if the system configured error-disable mechanism, it will start error-disable timer. Error-disable restarts the port after the timeout time of the system configuration。

In global configuration mode：

Switch#configure terminal

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)# spanning-tree mst portfast bpdu-guard

Under the interface configuration mode：

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-guard enable

Configuration of error-disable

Start error-disable mechanism

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout enable

Configuring timeout time for error-disable

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

8.2.7 Root Guard configuration

A two tier network of SP can contain many switches that are not connected to their own. In such a topology, the spanning tree can reconfigure itself and select a client switch as the root switch. You can avoid this by configuring root guard in the SP switch to the port of the switch in the client network. If the spanning tree calculation causes the port in the client network to be chosen as root port, the root guard configured the port as root-inconsistent (blocked) state to prevent the customer switch from becoming a root switch or to the root path。

If a switch outside the SP network becomes a root switch, the port is blocked (root-inconsistent STAT) and the spanning tree selects a new root switch. The client's switch does not become a root switch and there is no path to the root。

If the switch operates in MST mode, the root guard mandatory port becomes the specified port. If a boundary port, because root guard is in the blocked state in the IST instance, this port is block in all MST instances. A boundary port is a port connected to a LAN, which specifies that the switch is either a 802.1D switch or a switch configured in different MST domains。

When a port is opened, the Root guard is applied to all the VLAN that this port belongs to. VLAN can be aggregated and mapped to a MST instance。

Configuration process

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst guard root

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8.3 MSTP configuration example

(1)Configuration

The three switches are connected into a circle, and the spanning tree protocol of each switch is needed to avoid the occurrence of the loop. Perform configuration on each switch separately。

Configuration of switch 1：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

Configuration of switch 2：

Switch>en

Switch#configure terminal

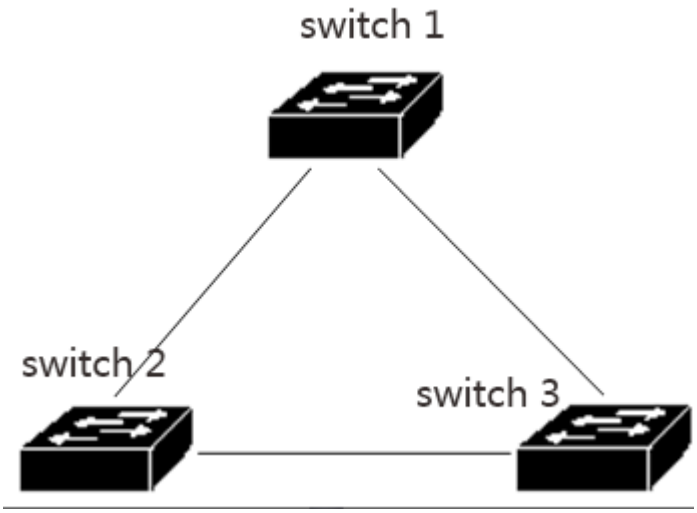
Switch(config)#spanning mst enable

Configuration of switch 3：

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2)Troubleshooting：

See which switch is selected as root bridge：

Show spanning-tree MST is executed, and the value of CISTRoot is observed as the least one

SEC.RU | Короткий путь к информации
Скачано с sec.ru

of the three MAC addresses in the exchange, that is, the root result is correct。

Switch#show spanning-tree mst

View the port state of the switches in the spanning tree：

Execute the instruction of show spanning-tree MST interface ge1/1, and observe the State value of PORT ge1/1 in instance 0

Switch#show spanning-tree mst interface ge1/1

Ninth chapters

EAPS configuration

This chapter describes the EAPS and its configuration, including the following：

- EAPS brief introduction
- Basic concepts of EAPS
- EAPS protocol introduction
- EAPS configuration
- Restrictive conditions
- A brief introduction to the EAPS command
- Single - loop configuration example
- Example of cross ring data forwarding configuration

9.1 EAPS brief introduction

EAPS is the abbreviation of Ethernet Automatic Protecting Switching。EAPS uses standard Ethernet and VLAN technology to provide loop topology and loop recovery mechanism。When a fault occurs in the loop, EAPS has the ability to recover data communication within a second. The EAPS running is not limited by the number of nodes, and the recovery time of the loop is not limited by the number of nodes. EAPS does not rely on other devices, that is, EAPS rings can have devices that do not support the EAPS protocol。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

9.2 Basic concepts of EAPS

Here are some of the basic concepts involved in EAPS：

1、EAPS Domain, in a network, a EAPS Domain is running in a single loop. It is a series of node devices that consist of a single loop, and a EAPS Domain contains one Master Node and one or more Transit Node。

2、Master Node, a EAPS switch, or EAPS node device, has a EAPS Domain with only one Master Node。

3、Transit Node, a switch that runs EAPS, or EAPS node device, in a EAPS Domain, other nodes except Master Node。

4、Primary Port, a port for connecting EAPS node devices in EAPS Domain. A node device has only one Primary Port connected to this loop in a EAPS Domain。

5、Secondary Port, a port for connecting EAPS node devices in EAPS Domain. A node device has only one Secondary Port connected to this loop in a EAPS Domain。

6、Control VLAN, control VLAN, responsible for EAPS Domain protocol packet transmission of VLAN, a EAPS Domain has only one Control VLAN。

7、Protected VLAN, protected VLAN, transfers VLAN of business data in EAPS Domain, a EAPS Domain must have a Protected VLAN, or more than one Protected VLAN。

9.3 EAPS protocol introduction

A EAPS Domain runs on a EAPS ring. A EAPS Domain contains a Master Node with one or more Transit Node EAPS; each node contains the same Control VLAN and multiple Protected VLAN; each EAPS node contains a Primary Port and a Secondary Port in a EAPS Domain, the two ports belong to this ring Control VLAN and Protected VLAN all. Through the Primary Port and Secondary Port connections of each EAPS node device, all nodes in the EAPS Domain compose a EAPS ring。

Under normal circumstances, when EAPS Domain and Secondary Port all Primary Port LINK UP, Master Node Secondary Port (blocking the Secondary Port port state Blocking), cancellation of business data EAPS in the Domain. When EAPS Domain fails, the Secondary port of Master Node is opened immediately (the state of the Secondary Port is Forwarding), allowing it to forward the business data and resume the normal forwarding of the service data。

Transit Node doesn't make any difference to Primary Port and Secondary Port processing。

Two fault checks and loop recovery of EAPS are described below：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

9.3.1Link-Down alarm

When Transit Node finds that its Primary Port or Secondary Port port appears LINK DOWN, it will send a LINK-DOWN protocol package to Master Node via another LINK UP port immediately from Control VLAN

When Master Node receives this LINK-DOWN protocol package：

Master Node Complete Failed immediately by the state to enter the state, open the Secondary Port (the Secondary Port state Forwarding), refresh two or three own forwarding, send a notification to the EAPS RING-DOWN-FLUSH-FDB Domain other Transit to refresh its forwarding table, re learning the two or three layer forwarding。

When Master Node finds that the local Primary Port occurs LINK DOWN, its operation is the same as that of the LINK-DOWN protocol packet。

When the Master Node Secondary Port found that the local LINK DOWN, Master Node Complete Failed immediately by the state to enter the state, refresh two or three own forwarding, sending RING-DOWN-FLUSH-FDB packets, EAPS Domain notify the other Transit to refresh its forwarding table, re learning the two or three layer forwarding。

9.3.2 Loop inspection

Master Node periodically sends HEALTH protocol packages from Primary Port. If the loop is complete, Master Node can receive the HEALTH protocol package in its own Secondary Port, when Master Node restarts its Fail-period timer, and the Master Node state is Complete。

If the fail-period is not received before the expiration of their HEALTH packets, Master Node will leave the Complete state into the Failed state Port (Secondary open Secondary Port state Forwarding), refresh two or three own forwarding, send RING-DsOWN-FLUSH-FDB EAPS Domain notify the other Transit to refresh its forwarding table, to learn the two or three layer forwarding。

9.3.3 Ring restoration

Master Node sends HEALTH packets from its Primary Port, regardless of the ring Complete or Failed or otherwise. When Master Node is in the Failed state, once the HEALTH protocol packet is received from its Secondary Port, the loop will revert to the Complete state. Then Master Node will set the Secondary Port state to blocking state, refresh two or three own forwarding, and sending a RING-UP-FLUSH-FDB packet, notify other equipment refresh two or three own forwarding, to learn two or three layer forwarding。

In the Transit Node port, from LINK DOWN back to LINK UP and Master Node, it is found

SEC.RU | Короткий путь к информации
Скачано с sec.ru

that Master Node Secondary Port may still be in the Forwarding state during loop restoration, in which case a temporary ring will be created. Therefore, in the Transit Node in a port is LINK UP, another LINK DOWN port has become LINK UP, Transit Node to enter into a "Forwarding" (PRE-FORWARDING), in this state behind the LINK UP port will be in the Pre-forwarding state, not transmit business data, interrupt the possible data loop. Wait until the Master Node recovery and send RING-UP-FLUSH-FDB, Transit Node received the packet after the node state transition to the LINK-UP state, Pre-forwarding state of the port is set to the Forwarding state, restore the normal transmission of business data。

If Transit Node does not receive the RING-UP-FLUSH-FDB protocol packet, it will be set to the Forwarding state by the port of the Pre-forwarding state after doubling the fail-time time。

9.3.4 Extreme compatible with EAPS

The product of Extreme company is the first to support EAPS manufacturers, series devices support EAPS protocol is to follow the RFC3619 standard; and EAPS protocol and RFC3619 Extreme protocol equipment package definition there are some differences. The EAPS protocol supported by the device of the network can be fully compatible with the Extreme device, and the compatible switch is open under default。

9.3.5 Multi EAPS Domain

series devices can support multiple EAPS Domain, which supports 16。

9.4EAPS configuration

The basic configuration of the EAPS protocol includes the following basic elements: Control VLAN, node mode (mode), Primary Port, Secondary Port, Protected VLAN, Hello Time and Fail Time. Hello Time and Fail Time have the default configuration, Hello Time is 1 second, Fail Timer is 3 seconds。

9.5 Restrictive conditions

1、Primary Port must belong to a EAPS Domain Control VLAN and all Protected VLAN TRUNK schema members。

2、EAPS protocol cannot run with MSTP protocol at the same time. EAPS protocol can not be started if MSTP is started or MSTP instance is configured。

3、A VLAN starts the VLLP protocol and cannot be configured as VLAN Control VLAN or Protected EAPS。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4、EAPS VLAN Control can only contain Primary Port and Secondary Port, and can only be the TRUNK mode of VLAN。

5、If a VLAN is configured as Control Domain of EAPS VLAN, and this Domain has been started, then the VLAN cannot be deleted, and its port members cannot be modified or deleted. Control VLAN cannot configure three layer interface。

6、In Protected VLAN, Primary Port and Secondary Port can only be TRUNK modes. Other member ports are not limited。

7、A port can only be configured as either a EAPS Domain Primary Port or a Secondary Port。

8、The same VLAN can only belong to a EAPS Domain Control VLAN or Protected VLAN。

9、The control VLAN of all nodes in a EAPS Domain must be the same。

9.6 A brief introduction to the EAPS command

To create a EAPS Domain, first of all, make sure that the configuration of the VLAN and port conforms to the above conditions。

Configuration EAPS has certain order requirements, first to create a EAPS Domain, before starting EAPS Domain, in accordance with the requirements of the previous configuration of other parameters; otherwise, the start will not succeed. If you want to change the Hello time to the value of the current fail time, you must first modify the fail time to a larger number; otherwise it will not be configured successfully. Other configuration sequences do not require special requirements。

Control-vlan, mode, primary-port, secondary-port cannot be modified when a EAPS Domain has been started; protected-vlan, fail-timer, hello-time, and extreme-interoperability can be modified。

Primary-port and secondary-port support LACP ports (that is, TRUNK groups)。

9.6.1 EAPS configuration command

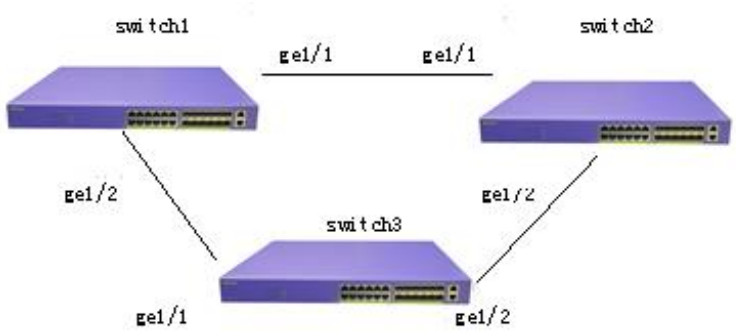
command	describe	mode
eaps create <ring-id>	Create a EAPS Domain	Global configuration mode
eaps control-vlan <ring-id> <vlan-id>	Configuring a EAPS Domain control VLAN。	Global configuration mode
eaps protected-vlan <ring-id> <vlan-id>	Add a protected VLAN for EAPS Domain。	Global configuration mode
eaps mode <ring-id> <master|transit>	Configure a run node mode of EAPS Domain。	Global configuration mode
eaps primary-port <ring-id> <ifname>	Configure a EAPS Domain Primary Port。	Global configuration mode
eaps secondary-port <ring-id> <ifname>	Configure a EAPS Domain Secondary Port。	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

eaps data-span <ring-id>	Configuring EAPS ring data trans ring forwarding	Global configuration mode
eaps fail-time <ring-id> <secs>	Configure the timeout time of a EAPS Domain fail-period timer. The default is 3 seconds. Units are seconds。	Global configuration mode
eaps hello-time <ring-id> <secs>	Configuring a EAPS Domain to send HEALTH packets at regular intervals. The default is 1 second. Units are seconds. Hello-timer must be less than fail-time。	Global configuration mode
eaps extreme-interoperability <ring-id> <enable|disable>	Boot or shutdown compatible with Extreme device, default is startup compatibility。	Global configuration mode
eaps enable <ring-id>	Start a EAPS Domain	Global configuration mode
eaps disable <ring-id>	Close a EAPS Domain	Global configuration mode
show eaps	The EAPS Domain information is displayed in the display system	Normal mode / privilege mode
Show eaps <ring-id>	Displays detailed information about a EAPSDomain	Normal mode / privilege mode

9.7 Single - loop configuration example

There are three sets of equipment Switch1, switch2, switch3, through the EAPS protocol VLAN 1 protection in traffic forwarding does not form a loop, while ensuring that when Switch1, switch2, there is a link off the standby link between switch3。According to the above requirements, you can configure Switch1 to master mode; configure switch2 and switch3 to transit mode. Add a protocol packet control VLAN VLAN 2。



Configuration of Switch1：

Switch1 is configured as EAPS Domain ring 1 master, control VLAN is VLAN 2, protected VLAN is VLAN 1, primary-port is ge1/1, secondary-port is ge1/2, other configurations use default values。

Switch#configure terminal

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#Adding VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit

#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12
2	vlan2	active	[t]ge1/1 [t]ge1/2

Switch#configure terminal

#Create a EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN
Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN
Switch(config)#eaps protected-vlan 1 1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#Configure Switch1 to be a master node
Switch(config)#eaps mode 1 master

#Configure ge1/1 to primary-port
Switch(config)#eaps primary-port 1 ge1/1

#Configure ge1/2 to secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1
Switch(config)#eaps enable 1

Configuration of Switch2

Switch2 is configured as EAPS Domain ring 1 transit, control VLAN is VLAN 2, protected VLAN is VLAN 1, primary-port is ge1/1, secondary-port is ge1/2, other configurations use default values。

Switch#configure terminal

#Adding VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit

#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit

SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
Switch#show vlan
 VLAN    Name          State         Member ports ([u]-Untagged, [t]-Tagged)
 ----    --------    ---------    -------------------------------------------------
 1         vlan1         active         [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                            [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
 2         vlan2         active         [t]ge1/1 [t]ge1/2
```

```
Switch#configure terminal

#Create a EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN
Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN
Switch(config)#eaps protected-vlan 1 1

#Configure switch to be a transit node
Switch(config)#eaps mode 1 transit

#Configure ge1/1 to primary-port
Switch(config)#eaps primary-port 1 ge1/1

#Configure ge1/2 to secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1
Switch(config)#eaps enable 1
```

Configuration of Switch3

Switch3 is configured as EAPS Domain ring 1 transit, control VLAN is VLAN 2, protected VLAN is VLAN 1, primary-port is ge1/1, secondary-port is ge1/2, other configurations use default values。

```
Switch#configure terminal
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

#Adding VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit

#Configure ge1/1 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Configure ge1/2 to be a trunk member of VLAN 1 and VLAN 2。
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10 [u]ge1/11 [u]ge1/12
2	vlan2	active	[t]ge1/1 [t]ge1/2

Switch#configure terminal

#Create a EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 to control VLAN
Switch(config)#eaps control-vlan 1 2

#Configuring VLAN 1 to be protected VLAN
Switch(config)#eaps protected-vlan 1 1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

#Configure switch3 to be a transit node
Switch(config)#eaps mode 1 transit

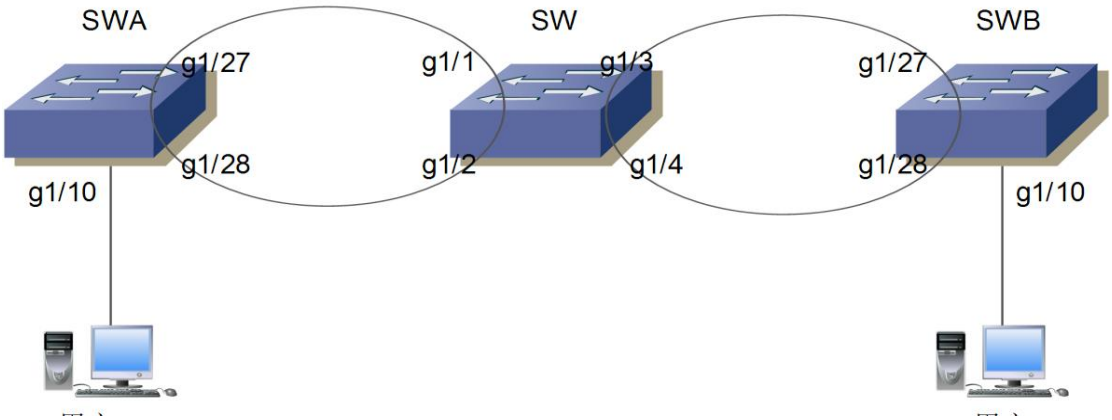
#Configure ge1/1 to primary-port
Switch(config)#eaps primary-port 1 ge1/1

#Configure ge1/2 to secondary -port
Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1
Switch(config)#eaps enable 1

9.8 Example of cross ring data forwarding configuration

There are three devices SWA, SW, SWB, through the EAPS protocol inter ring to achieve vlan1 vlan2 interworking。Topology as follows：



SWA loop 1 controls vlan111, protects vlan1, 2, configured as follows：

```
vlan database
  vlan 2
  vlan 111

interface ge1/10
  switchport access vlan 2
interface ge1/27
  switchport mode trunk
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
  switchport trunk allowed vlan add 2
  switchport trunk allowed vlan add 111
interface ge1/28
  switchport mode trunk
  switchport trunk allowed vlan add 2
  switchport trunk allowed vlan add 111

eaps create 1
eaps mode 1 Transit
eaps primary-port 1 ge1/27
eaps secondary-port 1 ge1/28
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps enable 1
```

SW loop 1 and SWA docking, control vlan111, protect vlan1, 2. Ring 2 and SWB docking, control vlan222, protect vlan3333 (virtual VLAN, while the interface need to add). If you want to achieve ring 1 and ring 2 data trans ring forwarding, you need to configure the command EAPs data-span。

Configuration is as follows：

```
vlan database
  vlan 2
  vlan 111
  vlan 222
  vlan 3333

interface ge1/1
  switchport mode trunk
  switchport trunk allowed vlan add 2
  switchport trunk allowed vlan add 111
interface ge1/2
  switchport mode trunk
  switchport trunk allowed vlan add 2
  switchport trunk allowed vlan add 111
interface ge1/3
  switchport mode trunk
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual VLAN 3333
interface ge1/4
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual VLAN 3333

eaps create 1
eaps mode 1 Master
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1

eaps create 2
eaps mode 2 Transit
eaps primary-port 2 ge1/3
eaps secondary-port 2 ge1/4
eaps control-vlan 2 222
eaps protected-vlan 2 3333                      ###Here is the virtual protection VLAN
eaps data-span 2
eaps enable 2
```

SWB ring 2 and SW ring 2 butt, control vlan222, protect vlan1, 2。Configuration is as follows：

```
vlan database
 vlan 2
 vlan 222

interface ge1/10
 switchport access vlan 2

interface ge1/27
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

interface ge1/28
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

eaps create 2
eaps mode 2 Master
eaps primary-port 2 ge1/27
eaps secondary-port 2 ge1/28
eaps control-vlan 2 222
eaps protected-vlan 2 1
eaps protected-vlan 2 2
eaps enable 2
```

After this configuration is completed, the user 1 and user 2 interworking, vlan1 data is also interoperability. Eaps node mode can be modified according to requirement。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Tenth chapters

ERPS configuration

10.1 ERPS overview

ERPS (Ethernet Ring Protection Switching) is a ring network protection protocol developed by ITU, also known as G.8032。It is a link layer protocol specially used in Ethernet ring network. It can prevent the broadcast storm caused by the data loop when the Ethernet loop is complete, and can quickly recover the communication between the nodes on the Ethernet ring when a link is disconnected. The ERPS protocol provides a fast Ethernet ring protection mechanism, which can quickly restore network transmission when the ring network fails, thus ensuring high availability and high reliability of the switch under the condition of the ring network topology。

10.2 Introduction of ERPS Technology

10.2.1 ERPS ring

ERPS rings are based on the minimization of rings, each ring must be the smallest ring, divided into the main ring and the sub ring: the main ring is a closed ring; the ring is a non closed ring or a closed ring; and all of them need to be configured by command。

Each ERPS ring (whether the main ring or ring) has five states: (1) Idle state: ring of each physical link is connected to the state; (2) Protection state: the state of one or multiple physical links open loop network; (3) Manual switch hand: change ring state; (4) Forced switch state: the forced change ring state; (5) Pending state: intermediate state in suspense.。

10.2.2 ERPS node

The two layer switching device that joins the ERPS ring is called a node. Each node cannot be more than two ports to join the same ERPS ring, one port is RPL port, and the other is common ring port。

For the overall situation, the role of the nodes are divided into two types as follows: (1) the intersection node: in the intersection of ERPS loop, nodes belong to multiple rings called the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

intersection node; (2) non intersection nodes: the intersection of the ERPS ring, the node only belongs to a ERPS ring is called non intersection node。

There are three types of node modes in ERPS protocol: RPL owner node, RPL neighbour node and common ring node。(1) RPL owner nodes: a ERPS ring is only a RPL owner node, determined by user configuration, to prevent loop in the ERPS ring by blocking the RPL port, when the RPL owner node receives a fault message that other node or link failure on the ERPS ring, will automatically open RPL port, the port receiving recovery and send traffic, ensure the flow will not be interrupted; (2) RPL neighbour node: node is directly connected with the RPL owner node RPL port, under normal circumstances, the RPL owner node RPL port and RPL neighbour node RPL port will be blocked, in order to prevent the loop from occurring. When the ERPS ring failure, RPL owner node RPL port and RPL neighbour node RPL port will be released; (3): ordinary ring node in the ERPS ring, the nodes except RPL owner nodes and RPL neighbour nodes are ordinary ring node, RPL port and port of ordinary ordinary ring ring node there is no difference between ordinary port link state ring ring node responsible for monitoring their direct ERPS protocol, and to change the message link state timely notify other nodes；

10.2.3 Link and channel

(1) RPL (Ring Protection Link): each ERPS ring has only one RPL, that is, the RPL port of the RPL owner node is located at the link. When the Ethernet ring is in the Idle state, the RPL link is in a blocking state and does not forward the data packet to avoid forming the loop；

(2) Sub loop link: in the intersection ring, belonging to the sub ring, link by loop control；

(3) RAPS (Ring Auto Protection Switch) virtual channel: in the intersection ring, the intersection nodes are used to transfer the ring protocol message, but the path not belonging to the sub ring is called the RAPS virtual channel of the ring。

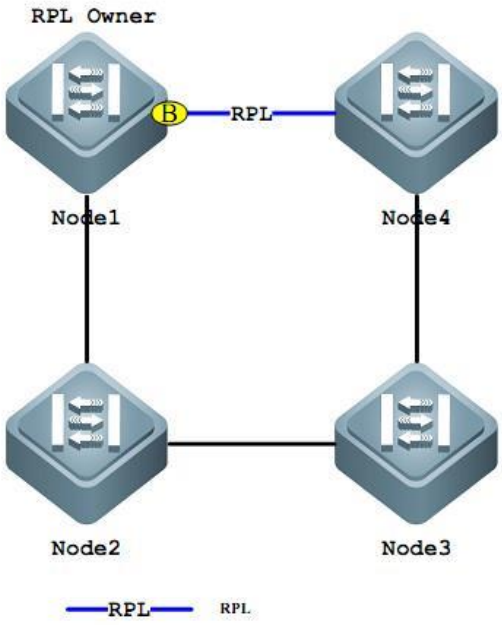
10.2.4 ERPS VLAN

There are two types of VLAN: (1) RAPS VLAN in ERPS, which are used to transfer ERPS protocol packets, and the ports that access the ERPS ring on the device belong to the RAPS VLAN, and only the ports accessing the ERP ring can join the VLAN. RAPS VLAN of different rings must be different. RAPS VLAN interface is not allowed to configure IP address; (2) data VLAN: relative to RAPS VLAN, data VLAN is used to transmit data packets, data VLAN can include ERP ring port, also can include non ERP ring port。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.3 ERPS Working principle

10.3.1 Normal state

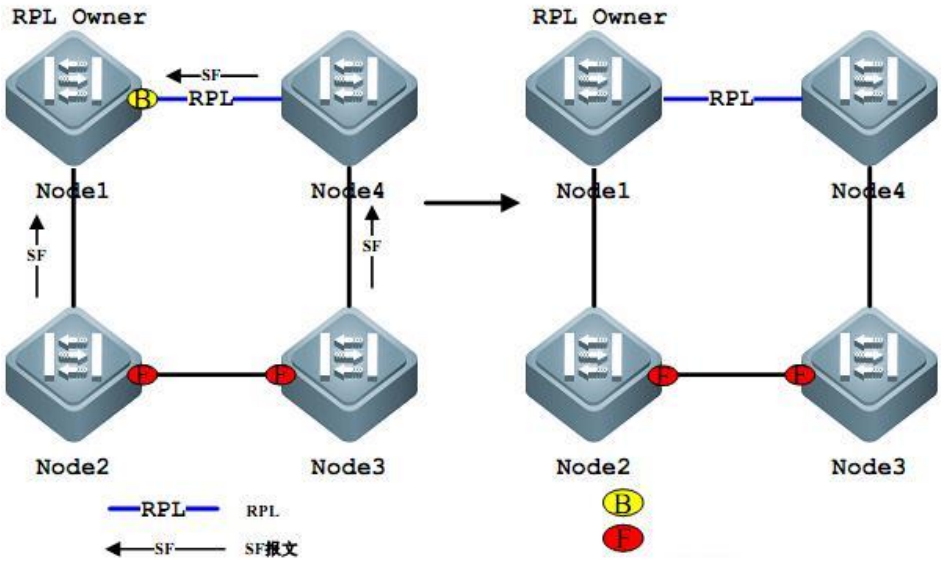


(1) All nodes are connected in a ring by physical topology;

(2) Loop protection protocols ensure that loops are not blocked by blocking the RPL link. As shown in the figure above, the link between Node1 and Node4 is RPL link;

(3) Fault detection is performed for each link between adjacent nodes。

10.3.2 Link failures

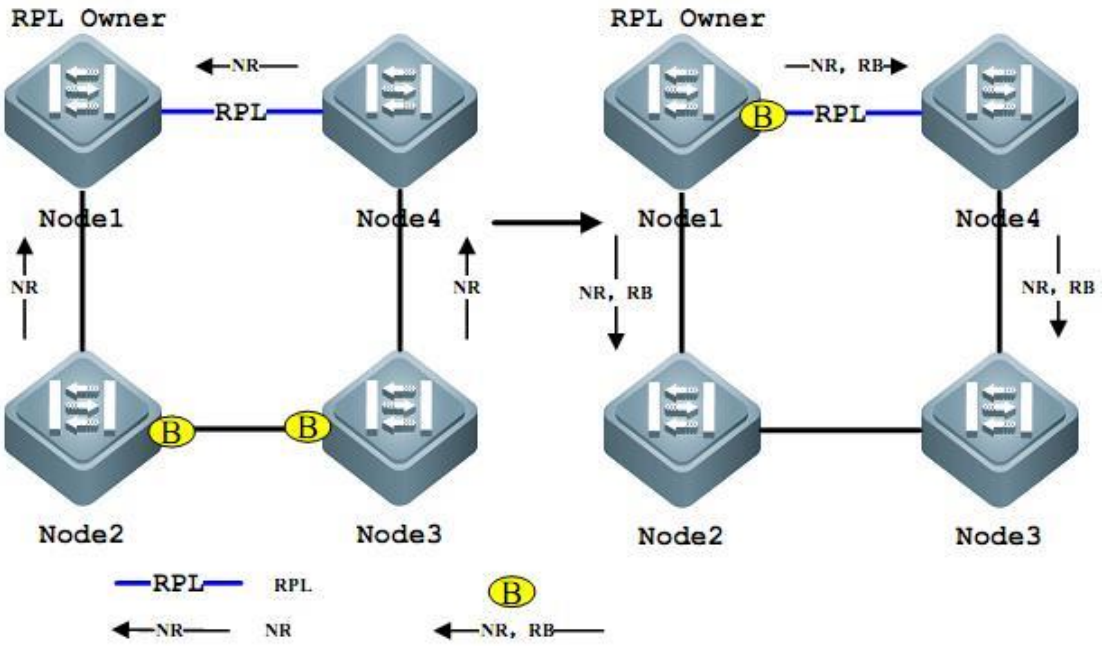


SEC.RU | Короткий путь к информации
Скачано с sec.ru

(1) The nodes adjacent to the fault and fault link link congestion, and the use of RAPS (SF) message to the other nodes report the fault on the ring, as shown above, assuming Node2, Node3 between Node2 and Node3 link failure, waiting for the holdoff timer after a timeout, it will block the link fault, respectively to ring network nodes send the RAPS message (SF);

(2) RAPS (SF) message trigger RPL has the node to open the RPL port. The RAPS (SF) message also triggers all nodes to update their respective MAC table entries, and then the nodes enter the protection state。

10.3.3 Link recovery



(1) When the fault is resumed, the neighboring nodes of the fault continue to block and send RAPS (NR) messages to indicate that there is no local fault;

(2) After the guard timer runs out, the RPL Owner node starts the WTR timer after the first RAPS (NR) message is received;

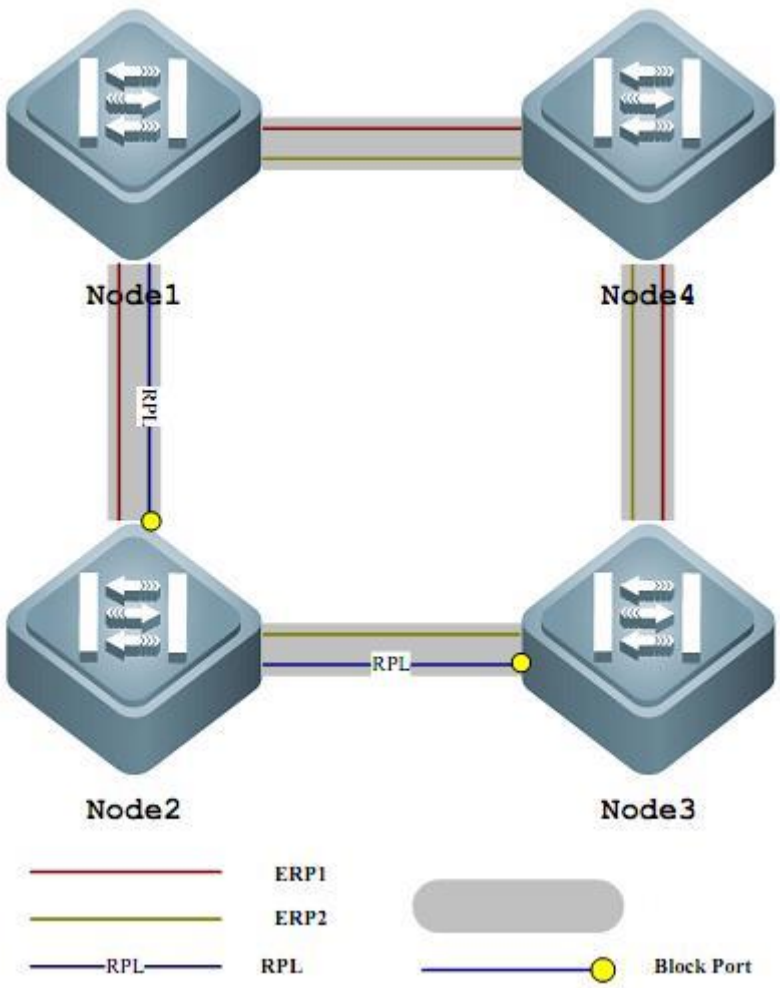
(3) When the WTR timer runs out, the RPL Owner node blocks the RPL and sends RAPS (NR, RB) messages;

(4) When other nodes receive this message, they update their respective MAC table entries, and the node that sends the RAPS (NR) message stops sending messages periodically and opens the previously blocked ports. The ring network has returned to its original normal state。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.4 Technical features of ERPS

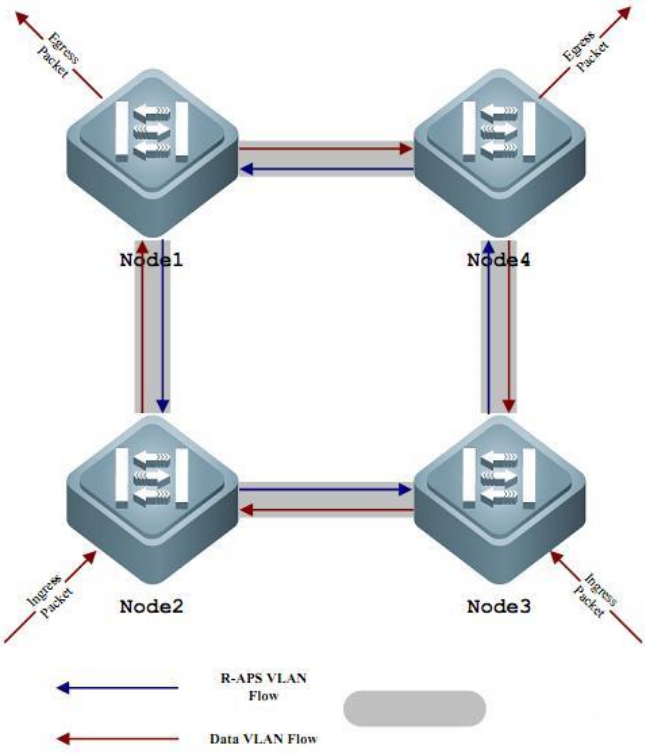
10.4.1 ERPS load balancing



Through the Internet in the same physical ring configuration of multiple instances of ERPS ring, ERPS ring VLAN send different different (called VLAN protection) traffic, the realization of topological data traffic with different VLAN in the ring network is different, so as to achieve the purpose of load sharing。 As shown in the figure above, a physical ring network corresponds to two instances of two ERPS rings, and two ERPS rings protect VLAN differently, Node2 is the RPL owner node of ERP1, and Node3 is ERP2 RPL owner node. By configuring, different VLAN can be used to block different links, so as to realize the load sharing of single loop。

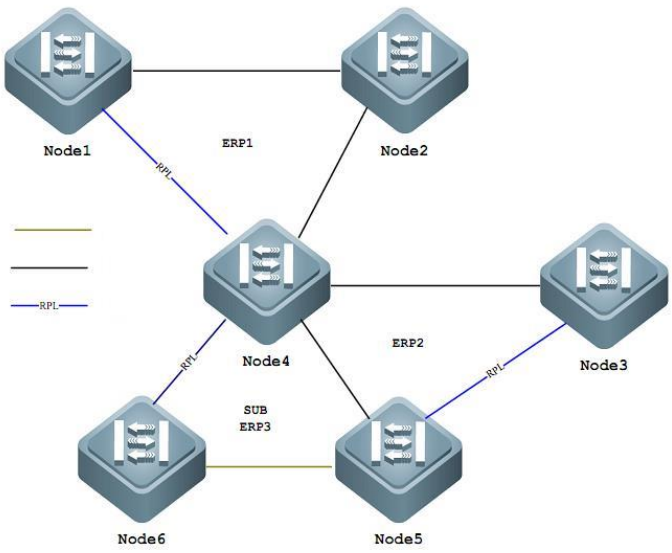
SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.4.2 Good safety



There are two types of ERPS in VLAN, one is RAPS VLAN, and the other is data VLAN. RAPS VLAN is only used for transmitting ERPS protocol packets; ERPS also only deals with protocol packets from RAPS VLAN, does not handle any protocol attack packets from data VLAN, and improves the security of ERPS。

10.4.3 Multi-loop intersecting is supported



SEC.RU | Короткий путь к информации
Скачано с sec.ru

As shown in the figure above, ERPS supports the addition of multiple rings in the same node (Node4) as tangent or intersection, greatly increasing the flexibility of networking。

10.5 ERPS protocol command

command	describe	CLI mode
erps <1-8>	Create an instance of ERPS	Global configuration mode
no erps <1-8>	Deleting an instance of ERPS	Global configuration mode
node-role (interconnection | none-interconnection)	The role of the configuration node in the ERPS loop, the interconnect node or the non interconnect node	ERPS mode
ring <1-32>	Create a ERPS ring	ERPS mode
no ring <1-32>	Deleting a ERPS ring	ERPS mode
ring <1-32> ring-mode (major-ring | sub-ring)	Configure the ERPS ring pattern, the main ring or the child ring	ERPS mode
ring <1-32> node-mode (rpl-owner-node | rpl-neighbor-node | ring-node)	Configure ERPS ring node pattern, RPL owner node, RPL neighbor node or common ring node	ERPS mode
ring <1-32> raps-vlan <2-4094>	Configuring ERPS ring protocol VLAN	ERPS mode
no ring <1-32> raps-vlan	Deleting ERPS ring protocol VLAN	ERPS mode
ring <1-32> traffic-vlan <1-4094>	Configuring ERPS ring data VLAN	ERPS mode
no ring <1-32> traffic-vlan <1-4094>	Deleting ERPS ring data VLAN	ERPS mode
ring <1-32> (rpl-port|rl-port) IFNAME	Configure ERPS ring port, RPL port or common ring port	ERPS mode
no ring <1-32> (rpl-port|rl-port)	Delete ERPS ring port	ERPS mode
ring <1-32> revertive-behaviour (revertive|non-revertive)	Configuring ERPS loops to restore behavior can be recoverable or not recoverable	ERPS mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

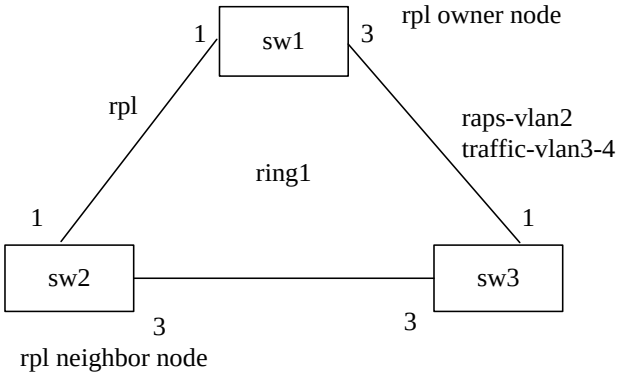
ring <1-32> hold-off-time <0-10000>	Configuring ERPS ring hold-off time	ERPS mode
no ring <1-32> hold-off-time	Restore ERPS ring hold-off default time	ERPS mode
ring <1-32> guard-time <10-2000>	Configuring ERPS ring guard time	ERPS mode
no ring <1-32> guard-time	Restore ERPS ring guard default time	ERPS mode
ring <1-32> wtr-time <1-12>	Configuring ERPS ring WTR time	ERPS mode
no ring <1-32> wtr-time	Restore ERPS ring WTR default time	ERPS mode
ring <1-32> wtb-time <1-10>	Configuring ERPS ring WTB time	ERPS mode
no ring <1-32> wtb-time	Restore ERPS ring WTB default time	ERPS mode
ring <1-32> raps-send-time <1-10>	Configuring ERPS ring protocol packet delivery time	ERPS mode
no ring <1-32> raps-send-time	Restore ERPS ring protocol message default sending time	ERPS mode
ring <1-32> (enable|disable)	Turn on or off the ERPS ring	ERPS mode
ring <1-32> forced-switch IFNAME	Forced switching ERPS ring port	ERPS mode
ring <1-32> clear forced-switch	Forced handoff of clear ERPS ring	ERPS mode
ring <1-32> manual-switch IFNAME	Manually switch the ERPS ring port	ERPS mode
ring <1-32> clear manual-switch	Manual switching to clear ERPS ring	ERPS mode
ring <1-32> clear recovery	Manual restoration of ERPS loop's non recoverable behavior or manual recovery prior to WTR/WTB expiration	ERPS mode
show erps	Display all the ERPS instances and loops in the device	Privileged mode
show erps <1-8>	Display device single ERPS instance and loop details	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.6 Typical use of ERPS

10.6.1 Example of single ring

The following diagram, SW1, SW2 and SW3 nodes constitute a single ERPs ring ring1, 1, 3 ports of each node as the ERPs ring ring port, protocol VLAN is 2, 3, 4 VLAN data, the SW1 node is RPL owner node, SW2 node to the RPL node of neighbor, SW1 and SW2 between the link RPL link。



(1) Configuring SW1：

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

(2) Configuring sw2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

(3) Configuring SW3:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

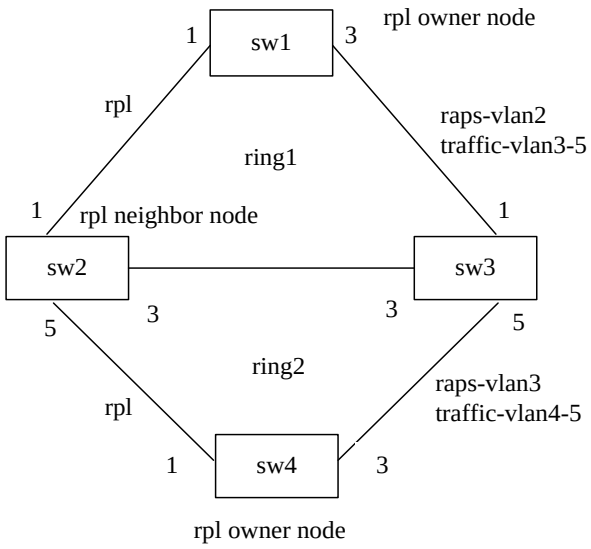
SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

10.6.2 Multi ring example

The following diagram, SW1, SW2 and SW3 nodes constitute a ERPs main ring ring1, SW1, SW2 and SW3 nodes 1, 3 port as the main ring a ring1 port, the main ring of the ring1 protocol of VLAN is 2, 3, 4, VLAN 5, SW1 ring1 RPL owner main ring node node, SW2 node the main loop ring1 neighbor node RPL, SW1 link between SW2 and ring1 based RPL link ring。

SW2, SW3 and SW4 nodes constitute a ERPs ring RING2, SW2, SW3 nodes and SW4 nodes 5 port 1, port 3 as a sub ring ring ring RING2 port, RING2 protocol VLAN 3, data is 4 VLAN, 5, SW4 RING2 RPL owner is a sub ring node node, link SW2 between SW4 and sub ring RING2 RPL link。



(1) Configuring SW1：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs main ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 traffic-vlan 5

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

SEC.RU | Короткий путь к информации
Скачано с sec.ru

(2) Configuring SW2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Switch(config)# interface xe1/5

Switch(config-xe1/5)# switchport mode trunk

Switch(config-xe1/5)# switchport trunk allowed vlan add 3

Switch(config-xe1/5)# switchport trunk allowed vlan add 4

Switch(config-xe1/5)# switchport trunk allowed vlan add 5

Switch(config-xe1/5)# switchport trunk allowed vlan remove 1

Switch(config-xe1/5)#exit

Configure ERPs instance 1, ERPs main ring 1, sub ring 2

Switch(config)#erps 1

Switch(config-erps-1)# node-role interconnection

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

(3) Configuring SW3:
Switch>enable
Switch#configure terminal
Creating ERPs protocol and data VLAN
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Switch(config)# interface xe1/5

Switch(config-xe1/5)# switchport mode trunk

Switch(config-xe1/5)# switchport trunk allowed vlan add 3

Switch(config-xe1/5)# switchport trunk allowed vlan add 4

Switch(config-xe1/5)# switchport trunk allowed vlan add 5

Switch(config-xe1/5)# switchport trunk allowed vlan remove 1

Switch(config-xe1/5)#exit

Configure ERPs instance 1, ERPs main ring 1, sub ring 2

Switch(config)#erps 1

Switch(config-erps-1)# node-role interconnection

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode ring-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 traffic-vlan 5

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#ring 2

Switch(config-erps-1)# ring 2 ring-mode sub-ring

Switch(config-erps-1)# ring 2 node-mode ring-node

Switch(config-erps-1)# ring 2 raps-vlan 3

Switch(config-erps-1)# ring 2 traffic-vlan 4

Switch(config-erps-1)# ring 2 traffic-vlan 5

Switch(config-erps-1)# ring 2 rpl-port xe1/5

Switch(config-erps-1)# ring 2 enable

Switch(config-erps-1)#exit

(4) Configuring SW4：

Switch>enable

Switch#configure terminal

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 3-5

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs sub ring 2

Switch(config)#erps 1

Switch(config-erps-1)#ring 2

Switch(config-erps-1)# ring 2 ring-mode sub-ring

Switch(config-erps-1)# ring 2 node-mode rpl-owner-node

Switch(config-erps-1)# ring 2 raps-vlan 3

Switch(config-erps-1)# ring 2 traffic-vlan 4

Switch(config-erps-1)# ring 2 traffic-vlan 5

Switch(config-erps-1)# ring 2 rpl-port xe1/1

Switch(config-erps-1)# ring 2 rl-port xe1/3

Switch(config-erps-1)# ring 2 enable

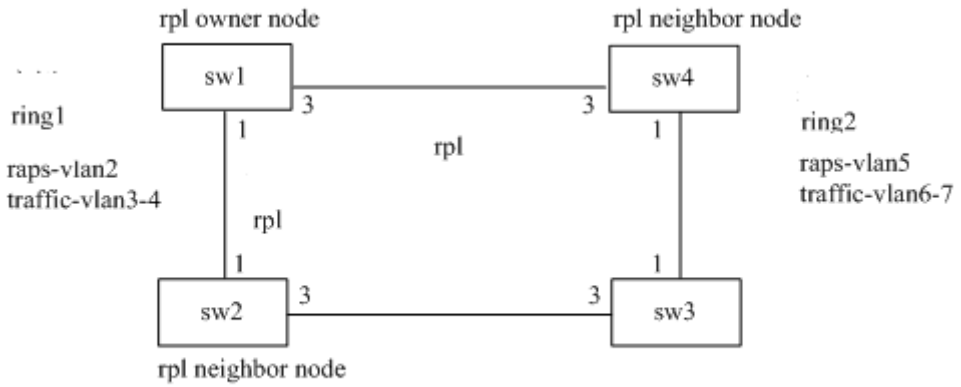
Switch(config-erps-1)#exit

SEC.RU | Короткий путь к информации
Скачано с sec.ru

10.6.3 Multi instance load balancing example

The following diagram, SW1, SW2, SW3 and SW4 nodes constitute a ERPs instance 1 single loop ring1, 1, 3 ports of each node as the ERPs ring ring port, protocol VLAN is 2, 3, 4 VLAN data, the SW1 node is RPL owner node, SW2 node is RPL neighbor node, link and SW1 SW2 for RPL link。

SW1, SW2, SW3 and SW4 nodes constitute a ERPs instance 2 single loop RING2, 1, 3 ports of each node as the ERPs ring ring port, protocol VLAN is 5, 6, 7 VLAN data, the SW1 node is RPL owner node, SW4 node is RPL neighbor node, link between SW4 and SW1 for the RPL link。



(1) Configuration instance 1：

Configuring SW1：

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-owner-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

Configuring SW2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

Configuring SW3:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

Switch(config-erps-1)# ring 1 node-mode ring-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

Configuring SW4:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 1, ERPs single ring 1

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

Switch(config-erps-1)# ring 1 ring-mode major-ring

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-1)# ring 1 node-mode ring-node

Switch(config-erps-1)# ring 1 raps-vlan 2

Switch(config-erps-1)# ring 1 traffic-vlan 3

Switch(config-erps-1)# ring 1 traffic-vlan 4

Switch(config-erps-1)# ring 1 rpl-port xe1/1

Switch(config-erps-1)# ring 1 rl-port xe1/3

Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

(2) Configuration instance 2：

Configuring SW1：

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan add 6

Switch(config-xe1/1)# switchport trunk allowed vlan add 7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan add 6

Switch(config-xe1/3)# switchport trunk allowed vlan add 7

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 2, ERPs single ring 2

Switch(config)#erps 2

Switch(config-erps-2)#ring 2

Switch(config-erps-2)# ring 2 ring-mode major-ring

Switch(config-erps-2)# ring 2 node-mode rpl-owner-node

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-2)# ring 2 raps-vlan 5

Switch(config-erps-2)# ring 2 traffic-vlan 6

Switch(config-erps-2)# ring 2 traffic-vlan 7

Switch(config-erps-2)# ring 2 rpl-port xe1/3

Switch(config-erps-2)# ring 2 rl-port xe1/1

Switch(config-erps-2)# ring 2 enable

Switch(config-erps-2)#exit

Configuring SW2:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan add 6

Switch(config-xe1/1)# switchport trunk allowed vlan add 7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan add 6

Switch(config-xe1/3)# switchport trunk allowed vlan add 7

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 2, ERPs single ring 2

Switch(config)#erps 2

Switch(config-erps-2)#ring 2

Switch(config-erps-2)# ring 2 ring-mode major-ring

Switch(config-erps-2)# ring 2 node-mode ring-node

Switch(config-erps-2)# ring 2 raps-vlan 5

Switch(config-erps-2)# ring 2 traffic-vlan 6

Switch(config-erps-2)# ring 2 traffic-vlan 7

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-2)# ring 2 rpl-port xe1/1

Switch(config-erps-2)# ring 2 rl-port xe1/3

Switch(config-erps-2)# ring 2 enable

Switch(config-erps-2)#exit

Configuring SW3:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan add 6

Switch(config-xe1/1)# switchport trunk allowed vlan add 7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan add 6

Switch(config-xe1/3)# switchport trunk allowed vlan add 7

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 2, ERPs single ring 2

Switch(config)#erps 2

Switch(config-erps-2)#ring 2

Switch(config-erps-2)# ring 2 ring-mode major-ring

Switch(config-erps-2)# ring 2 node-mode ring-node

Switch(config-erps-2)# ring 2 raps-vlan 5

Switch(config-erps-2)# ring 2 traffic-vlan 6

Switch(config-erps-2)# ring 2 traffic-vlan 7

Switch(config-erps-2)# ring 2 rpl-port xe1/1

Switch(config-erps-2)# ring 2 rl-port xe1/3

Switch(config-erps-2)# ring 2 enable

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-erps-2)#exit

Configuring SW4:

Switch>enable

Switch#configure terminal

Creating ERPs protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 5-7

Switch(config-vlan)#exit

Configure ring port VLAN mode as trunk, join ERPs protocol and data VLAN

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 5-7

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 5-7

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure ERPs instance 2, ERPs single ring 2

Switch(config)#erps 2

Switch(config-erps-2)#ring 2

Switch(config-erps-2)# ring 2 ring-mode major-ring

Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node

Switch(config-erps-2)# ring 2 raps-vlan 5

Switch(config-erps-2)# ring 2 traffic-vlan 6

Switch(config-erps-2)# ring 2 traffic-vlan 7

Switch(config-erps-2)# ring 2 rpl-port xe1/3

Switch(config-erps-2)# ring 2 rl-port xe1/1

Switch(config-erps-2)# ring 2 enable

Switch(config-erps-2)#exit

SEC.RU | Короткий путь к информации
Скачано с sec.ru

OSNOVO
cable transmission

Eleventh chapters

AAA configuration

This chapter describes how to configure the 802.1x and RADIUS of switches to prevent unauthorized users from accessing the network. For the use of the 802.1x client and HyperBoss, see the respective operating manuals. The main contents of this chapter are as follows：

- 802.1x introduce
- RADIUS introduce
- Configuring 802.1x
- configuration RADIUS

AAA is the abbreviation of authentication, authorization and Authentication (Authorization, and, Accounting). It provides a consistent framework for configuring authentication, authorization, and billing for these three security functions. The configuration of AAA is actually a management of network security, where network security mainly refers to access control. Which users can access the network? What services can users get access to? How to account for the users who are using the network resources?

Authentication (Authentication): verify whether the user can access access。

Authorization (Authorization): what services can authorized users use?。

Accounting (Accounting): recording the user's use of network resources。

network company launched a set of AAA solutions, the product has 802.1x client, a variety of supporting authentication switches and authentication billing system HyperBoss. The 802.1x client is installed on the PC which users access to the Internet. When the user needs to access the network, it needs to use the 802.1x client to authenticate. Only the authenticated user can use the network。

is an authentication exchange, which receives the authentication request of client, transfers the username and password to the authentication and billing system HyperBoss, and the switch itself doesn't do the actual authentication work. HyperBoss receives the authentication request sent by the switch and carries out the actual authentication, and carries on the billing processing to the successful authentication user。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The 802.1x protocol is used between the 802.1x client and the switch to communicate, and the RADIUS protocol is used between the switch and the HyperBoss。

11.1 802.1x introduce

The 802.1x protocol is based on access control and authentication protocol port, the port is here refers to the logical port, can be a physical port, MAC address or Vlan ID, network switch realization is based on MAC address and port based on 802.1x Protocol。

802.1x is a two layer protocol, the authenticated switch and the user's PC must be in the same subnet, and the protocol packet cannot cross the network segment. 802.1x authentication uses the model of client server, and must have a server to authenticate all users。

In MAC mode, the user through the authentication before, only authentication flow can through the switch port, after succeeding in authentication, data can flow through the switch port, which means that users must access the network after the adoption of the certification to. Port mode, you can open the Guest Vlan function, the default is closed. Turn off Guest Vlan, and MAC data through the same pattern, but after authentication is to open the port, not registered MAC address; open the Guest Vlan when the user is authenticated before data by Guest Vlan, the authentication succeeds, by Auth Vlan, this method can be used to specify the scope of limited access limited user authentication before, after the public network access authentication。

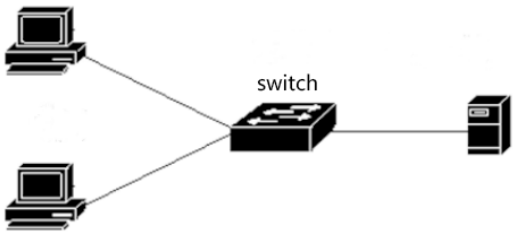
The main contents of this section are as follows：

- 802.1x device composition
- Brief introduction of protocol package
- Protocol flow interaction
- 802.1x port state

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11.1.1 802.1x device composition

802.1x device consists of three parts: client (Supplicant System), authentication system (Authenticator System) and authentication server (Authentication Server System). As shown in the following picture。



802.1x

Refers to the client requests access to network equipment, general user terminal system, such as PC users, the user terminal system must install a 802.1x client software, the software realization of 802.1x protocol in the client part. The client initiates the 802.1x authentication request and requests the authentication server to verify its user name and password. If the authentication is successful, the user can access the network。

Authentication systems refer to authenticated devices, such as switches. The user authentication system by logical port (refer to the MAC address) state control whether a user can access the network, if the user is non logical port state authority, the user can not access the network, if the user is authorized to logical port state, the user can access the network。

Authentication system is a relay between the client and the authentication server. The authentication system requests the identity information of the user, and forwards the identity information of the user to the authentication server, and forwards the authentication result sent by the authentication server to the client. The server part authentication system to implement the 802.1x protocol in the near end users, the client part near the authentication server to implement the RADIUS protocol, RADIUS protocol client authentication system 802.1x client sent EAP information package sent to the authentication server in RADIUS, and from the authentication server to the RAIDUS protocol in the EAP information solution package out and sent by the 802.1x server to 802.1x client。

Authentication server refers to the device that actually authenticates the user. Identity authentication server to receive user authentication system and verify if authentication is successful, the authentication server authorization authentication system allows the user to access the network, if authentication fails, the authentication server authentication system tells the user authentication failure, the user can not access the network. Communication between authentication server and authentication system through EAP extended RADIUS protocol. network provides authentication and billing system, HyperBoss authentication and billing for users。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11.1.2 Brief introduction of protocol package

The 802.1x protocol authentication data transmission on the network flow is EAPOL (EAP Over LAN) frame format, all the user identity information (including user name and password) encapsulated in EAP (Extensible Authentication Protocol), EAP encapsulated in EAPOL frames. The user name exists in the form of plaintext in the EAP, and the password exists in the form of MD5 encryption in the EAP。

The frame format of EAPOL is as follows. PAE Ethernet Type is the Ethernet protocol type number of EAPOL, and the value is 0x888E. Protocol Version is the EAPOL version number, which is 1. Packet Type refers to the type of EAPOL frame. Packet Body Length is the length of the EAPOL frame content. Packet Body refers to the content of the EAPOL frame。

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

EAPOL frame format

switches use three EAPOL protocol frames, respectively：

The value of EAPOL-Start:Packet Type is 1, the authentication frame is initiated, and when the user needs authentication, the frame is first launched, and the client is sent to the switch。

The value of EAPOL-Logoff:Packet Type is 2. The request frame is exited and the frame is notified when the user does not need to use the network。

The value of EAP-Packet:Packet Type is 0, and the authentication information frame is used to bear authentication information。

EAP package format as follows. Code refers to the type of EAP package, including Request, Response, Success and Failure. Identifier refers to identifiers, which are used to match Response and Request. Length refers to the length of the EAP packet, including Baotou. Data refers to the EAP packet data。

The EAP package consists of the following four types：

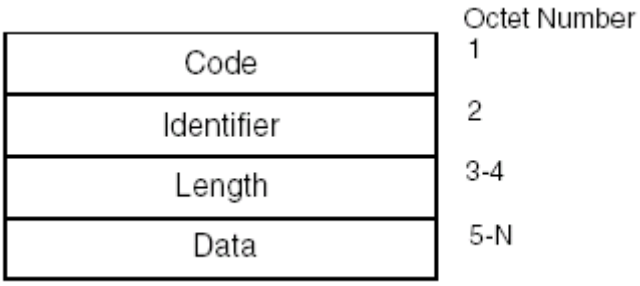
The EAP-Request:Code value is 1, the EAP requests the packet and requests the user name and / or password from the switch to the client。

The EAP-Response:Code value is 2, the EAP response packet is sent from the client to the switch, and the user name and / or password are sent to the switch。

EAP-Success:Code value is 3, EAP is successfully packaged, sent from the switch to the client, told the client user authentication success。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

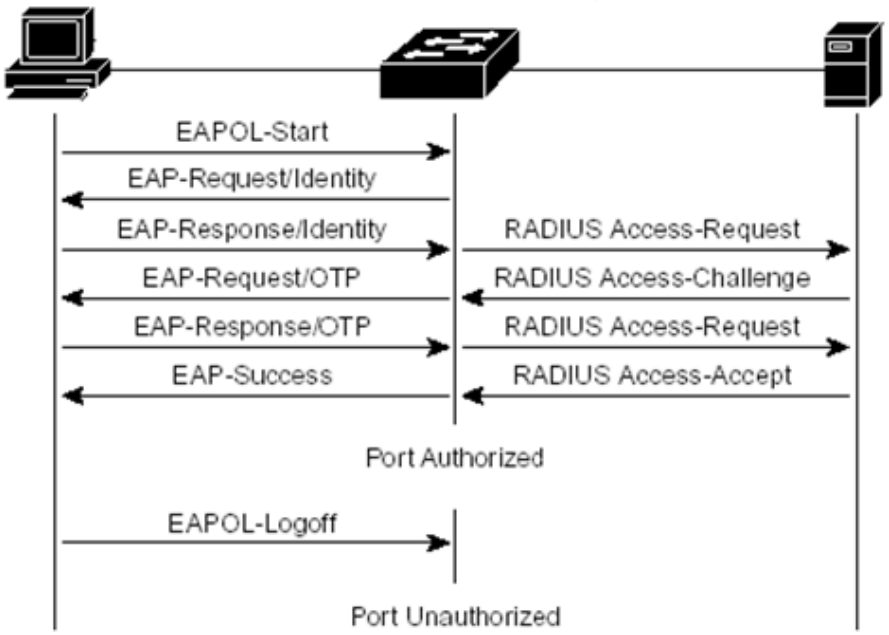
The EAP-Failure:Code value is 4, the EAP failure packet is sent from the switch to the client, and the client is told that the authentication failed。



EAP packet format

11.1.3 Protocol flow interaction

When the switch enables the 802.1x and the port state is Auto, all access users under the port must pass authentication to access the network. Protocol interaction as shown below。



Client initiated authentication protocol interaction

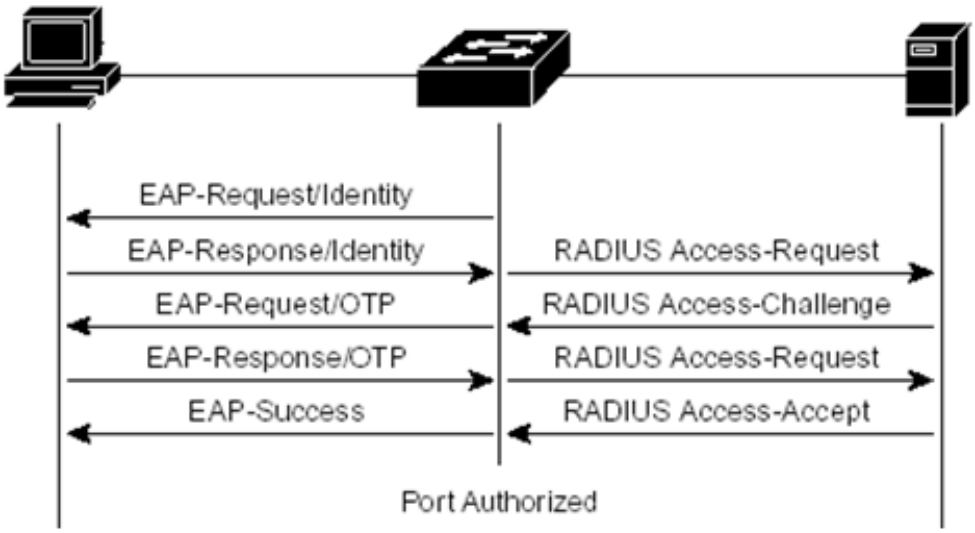
When users need to access the network, the client sends the first EAPOL-Start to exchange requests received after the authentication request authentication, the switch sends the EAP-Request request user name, the client send EAP-Response, switch EAP information extracted from the package in the RADIUS package sent to the authentication server, the authentication server requests the user password, switch to send EAP-Request to the client request user password the client EAP-Response, echo switch, EAP information is encapsulated in the RADIUS authentication server to send packets, according to the authentication server

SEC.RU | Короткий путь к информации
Скачано с sec.ru

authenticates the user name and password. If the authentication is successful, the authentication server notifies the switch, the switch sends EAP-Success to the client and the user's logical port is in the authorized state. When the client receives EAP-Success, the authentication is successful, and the user can access the network。

When the user no longer needs to use the network, the client sends EAPOL-Logoff to the switch, and the switch transfers the user's logical port state to an unauthorized state, when the user can not access the network。

In order to prevent the abnormal client offline, switch provides a mechanism for re certification, the time interval can be set in the re certification on the switch, when the authentication time arrives, the switch initiated re certification, if authentication is successful, the user can continue to use the network, if authentication fails, the user will not use the network. Protocol interaction as shown below。



Authenticated protocol interaction

11.1.4 802.1x port state

The port state is the physical port state of the switch. There are four states in the physical port of the switch: N/A state, Auto state, Force-authorized state, and Force-unauthorized state. When the switch does not open the 802.1x, all ports are in the N/A state. When the switch port is to be set into Auto state, Force-authorized state or Force-unauthorized state, the 802.1x of the enable switch must be first。

When the port of the switch is in the N/A state, all the users under the port can access the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

network without authentication. When the switch receives the 802.1x protocol packet from the port, the protocol packets are discarded。

When the port of the switch is in the Force-authorized state, all the users under the port can access the network without authentication. When the switch receives the EAPOL-Start packet from the port, the switch sends the EAP-Success packet. When the switch receives the other 802.1x protocol packets from the port, the protocol packets are discarded。

When the port of the switch is in the Force-unauthorized state, all users under the port can not access the network all the time, and the authentication request will never pass. When the switch receives the 802.1x protocol packet from the port, the protocol packets are discarded。

When the port of the switch is in the Auto state, the authentication mode should be distinguished. Port mode, if Guest Vlan is not configured, the port of the user must can access the network through the certification, closing the port is not certified; if the configuration of the Guest Vlan port, the user can access Auth Vlan through certification, not certified can access the Guest Vlan. All users under the port must be authenticated to access the network. The interaction of the 802.1x protocol is shown in the diagram. If the user needs authentication, the port is generally set to the Auto state。

When the switch port is set to the Auto state, and enable the anti spoofing ARP function; anti spoofing ARP function can only control the IP package MAC source and source IP are consistent with the information provided by the client authentication data packet and ARP packet's sender IP and MAC are in line with the sender authentication client provides information packets to is this port forwarding, otherwise it will be discarded. This function must be static configuration client configuration IP address, if it is to obtain IP address through the DHCP protocol dynamic circumstances to achieve this function to enable the DHCP SNOOPING protocol; if you need more details please refer to the IP MAC binding configuration。

11.2 RADIUS introduce

When the user authenticates, the exchange and the authentication server interact with the RADIUS protocol that supports the EAP extension. RADIUS protocol uses client / server model, switches need to implement RADIUS client, and authentication server needs to implement RADIUS server。

In order to ensure the security of the interaction between the switch and the authentication server, and to prevent the interaction between illegal switches or illegal authentication servers, mutual authentication between the switch and the authentication server is needed. The switch and the authentication server need a same key, when the switch or the authentication server sends the RADIUS protocol packets, all packets according to the key using the HMAC algorithm to

SEC.RU | Короткий путь к информации
Скачано с sec.ru

generate a message digest, when the switch and the authentication server receives the RADIUS protocol packet, all protocol packets to verify the message digest using the key, if verified by that is, the legal RADIUS, otherwise it is illegal RADIUS packets discarded。

The main contents of this section are as follows：

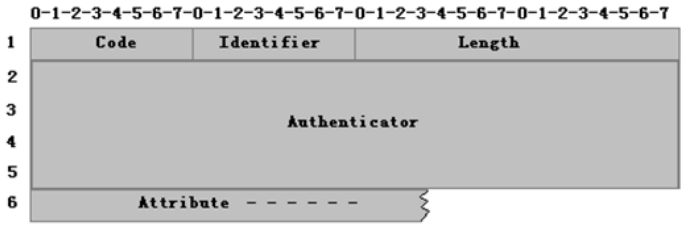
- Brief introduction of protocol package
- Protocol flow interaction
- User authentication method

11.2.1 Brief introduction of protocol package

RADIUS is a protocol based on UDP, and RADIUS can encapsulate authentication information and billing information. The early RADIUS authentication port is 1645, the current use port 1812, the early RADIUS billing port is 1646, the current use port 1813。

Because RADIUS is hosted on UDP, RADIUS has a timeout retransmission mechanism. At the same time, in order to improve the reliability of communication between authentication system and RADIUS server, two RADIUS server schemes are adopted, that is to say, the standby server mechanism is adopted。

The RADIUS message format is as follows. Code refers to the type of RADIUS protocol message. Identifier index identifier for matching requests and responses. Length refers to the length of the entire message (including the header). Authenticator is a 16 byte string, a random number for the request packet, and a message digest for the response packet that is generated by MD5. Attribute refers to the attributes in the RADIUS protocol package。



RADIUS message format

The network uses the following RADIUS protocol packages：

The Access-Request:Code value is 1, the authentication request packet is sent to the authentication server from the authentication system, and the user name and password are encapsulated on the package。

The Access-Accept:Code value is 2, from the authentication server to the response packet of the authentication system, which means the user authentication is successful。

The Access-Reject:Code value is 3, and the authentication packet is sent to the authentication

SEC.RU | Короткий путь к информации
Скачано с sec.ru

system from the authentication server, which indicates the failure of user authentication。

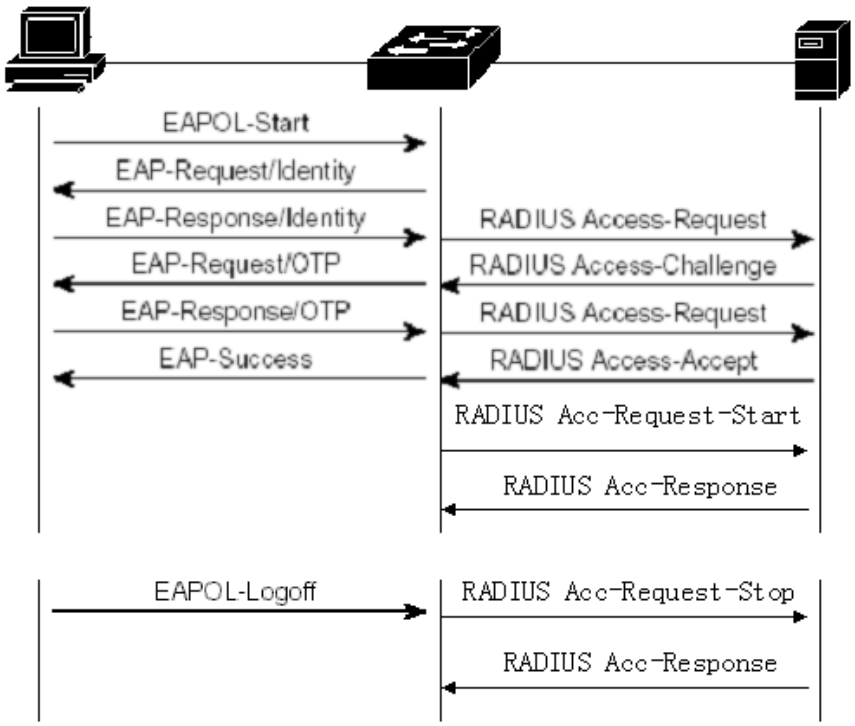
The Access-Challenge:Code value is 11, from the authentication server to the response packet of the authentication system, which indicates that the authentication server needs further information of the user, such as passwords。

The Accounting-Request:Code value is 4, and the billing request package from the authentication system is sent to the authentication server, including the start billing and the end billing package, and the billing information is encapsulated on the package。

The Accounting-Response:Code value is 5, from the authentication server to the billing response package of the authentication system, which indicates that the billing information has been received。

11.2.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact with each other through the RADIUS protocol. The authentication system does not send the protocol flow of the RADIUS billing package as the diagram below. Generally, when the user authentication is successful or the user is offline, the authentication system needs to send the RADIUS billing package to the authentication server, and the protocol flow interaction is shown in the following picture。



Authenticate user, switch package in the Access-Request message sent to the user name

SEC.RU | Короткий путь к информации
Скачано с sec.ru

authentication server, the server in response to Access-Challenge request user password switch request client user password, the password to the client in the EAP packaging, a switch gets to this EAP encapsulated in Access-Request to the authentication server authenticates the user authentication server, if authentication is successful, echo Access-Accept to the switch, the switch receives this message to inform the client authentication is successful, and sends the Accounting-Request notification authentication server to start billing, authentication server loopback Accounting-Response。

When the user does not want to use the Internet, notify the subscriber line, switch Accounting-Request notify the authentication server end of billing, billing information is encapsulated in this package, the authentication server to send Accounting-Response。

11.2.3 User authentication method

There are three kinds of user authentication methods for RADIUS：

- PAP (Password Authentication Protocol). The user passes the user name and his password to the switch in the form of plaintext. The switch passes the user name and password to the RADIUS server through the RADIUS protocol package, and the RADIUS server looks for the database. If there is the same user name and password, it indicates that the authentication is passed, otherwise it indicates that the authentication has not passed。
- CHAP (Challenge Handshake Authentication Protocol). When the user requests to access the Internet, the switch generates a 16 byte random code to the user. The user encrypts the random code, password, and other domains to generate a response, passing the user name and response to the switch. The switch passes the user name, the response, and the original 16 byte random code to the RADIUS server. According to the RADIU username in the switch side search database, and end users use the same password encryption, then encrypted based on random code to 16 bytes, and the results from the response comparison showed that if the same is verified, if not the same that validation failed。
- EAP (Extensible Authentication Protocol). With this verification method, the switch doesn't really participate in the verification, and only plays the role of forwarding between the user and the RADIUS server. When a user requests access, exchange requests the user's user name, the user name and forwarded to the RADIUS server, the RADIUS server generates a 16 byte random code to the user and stores the random code, users to generate a random code, response encryption password and other domain, the user name and the response to switch, switch forwarding to the RADIUS server.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

According to the RADIU username in the switch side search database, and end users use the same password encryption, and then encrypted according to random code stored 16 bytes, and the results from the response comparison showed that if the same is verified, if not the same that validation failed。

The authentication and billing solution of network adopts the method of EAP user authentication。

11.3 Configuring 802.1x

This section gives a detailed description of the configuration of 802.1x, including the following：

- 802.1x default configuration
- Start and close 802.1x
- Configuring 802.1x port status
- Configuring 802.1x port authentication
- Configuring 802.1x port guest VLAN
- Configuration re authentication mechanism
- Maximum number of configuration port access host
- Configure interval times and resend times
- Configuration port is the transport port
- Configuring the 802.1x client version number
- Configure whether to check the client version number
- Configuration authentication method
- Configure whether to check the client's timing packet
- Display 802.1x information

11.3.1 802.1x default configuration

switch 802.1x configuration defaults as follows：

- 802.1x is closed。
- The state of all ports is N/A。
- The authentication mechanism is closed, and the authentication interval is 3600 seconds。
- The maximum number of access hosts for all ports is 100。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- The timeout interval of EAP-Request retransmission is 30 seconds。
- The number of timeout retransmission EAP-Request is 3 times。
- The user authentication failed waiting for 60 seconds。
- The timeout interval of the server timeout is 10 seconds。

The switch provides a command in the global CONFIG mode to return all the configuration back to the default state. The commands are as follows：

Switch(config)#dot1x default

11.3.2 Start and close 802.1x

The first step in configuring 802.1x is to start 802.1x. In the global CONFIG mode, enter the following command to start 802.1x：

Switch(config)#dot1x

When the 802.1x is closed, all port States return to the N/A state. In global CONFIG mode, enter the following command to close 802.1x：

Switch(config)#no dot1x

11.3.3 Configuring 802.1x port status

You must start 802.1x before setting 802.1x port state. If all users under the port must be authenticated to access the network, the port must be set to the Auto state。

The following command sets port ge1/1 to Auto state in the interface configuration mode and enables anti ARP spoofing function：

Switch(config-ge1/1)dot1x control auto

If the configuration of anti ARP spoofing fails, it may be caused by the following reasons：

1、System CFP resource exhaustion。

2、The current interface is configured with the ACL filter function。

3、The current interface enables the DHCP SNOOPING function。

4、The configured interface is a three layer interface or a trunk interface。

The following command sets port ge1/1 to Force-authorized state in the interface

SEC.RU | Короткий путь к информации
Скачано с sec.ru

configuration mode：

Switch(config-ge1/1)dot1x control force-authorized

The following command sets port ge1/1 to Force-unauthorized state in the interface configuration mode：

Switch(config-ge1/1)dot1x control force-unauthorized

The following command sets port ge1/1 to N/A state in the interface configuration mode：

Switch(config-ge1/1)no dot1x control

Note: if a port has bound the MAC address, then the port cannot be set to Auto, Force-authorized or Force-unauthorized state。

11.3.4 Configuring 802.1x port authentication

You must start 802.1x before you set up the 802.1x port authentication method. If the port is only connected to a user who needs authentication, the port is opened by authentication, and the port must be set to portbase. If the authentication is based on the MAC address, it will be set to macbase. The default state is macbase。

The following command sets port ge1/1 to portbase state in the interface configuration mode：

Switch(config-ge1/1)dot1x method portbase

The following command sets port ge1/1 to macbase state in the interface configuration mode：

Switch(config-ge1/1)dot1x method macbase

11.3.5 Configuring 802.1x port guest VLAN

Before setting 802.1x port guest VLAN, you must start 802.1x, and configure ports for Auto state and portbase state. The guest VLAN can be accessed before the authentication of the user under the desired port. After the authentication, the configuration VLAN can be accessed, and then the port must be configured with guest VLAN。

It must be noted that guest VLAN only supports access mode, nor does it support trunk. Once

SEC.RU | Короткий путь к информации
Скачано с sec.ru

the port is configured with guest VLAN, its mode cannot be modified, and guest VLAN can not be configured in non access mode. When configuring guest VLAN, you must ensure that the VLAN has been created。

The following command sets the port guest VLAN to 2 in the interface configuration mode：

Switch(config-ge1/1)dot1x guest-vlan 2

11.3.6 Configuration re authentication mechanism

In order to prevent the client from being unaware of the switch and authentication server, the switch provides a re authentication mechanism that initiates authentication once every other time interval。

The following command starts the re authentication mechanism in the global CONFIG mode：

Switch(config)#dot1x reauthenticate

The following command closes the authentication mechanism in global CONFIG mode：

Switch(config)#no dot1x reauthenticate

The following command sets the time interval for re authentication in global CONFIG mode：

Switch(config)#dot1x timeout re-authperiod <interval>

Note: the interval between re authentication should not be too short, otherwise the network bandwidth and the CPU resource consumption of the switch will be too large。

11.3.7 Maximum number of configuration port access host

Each port of the switch can control the maximum number of access hosts. This function can restrict users to illegally access to the network by using multiple hosts. The maximum number of port access host defaults is 100, the maximum can be set to 100. If the maximum number of ports access host is set to 0, then the port rejects any user access。

The following command sets the maximum number of port ge1/1 access hosts in the interface configuration mode：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config-ge1/1)dot1x support-host <number>

11.3.8 Configure interval times and resend times

The 802.1x protocol standard protocol and protocol state machine some time interval and the number of retransmissions, switches using the standard time interval and the number of retransmissions, suggest that users in the use of these do not change the time interval and the number of retransmissions。

Tx-period said the switch time interval repeat EAP-Request protocol package; max-req said the number of retransmission switch EAP-Request; quiet-period represents the time interval of user authentication failure when waiting for re certification; server-timeout said the switch to the authentication server RADIUS packet retransmission time interval; supp-timeout said time interval of packet switches to the client EAP retransmission request。

The following command configures the interval and retransmission times in the global CONFIG mode：

Switch(config)#dot1x timeout tx-period <interval>

Switch(config)#dot1x max-req <number>

Switch(config)#dot1x timeout quiet-period <interval>

Switch(config)#dot1x timeout server-timeout <interval>

Switch(config)#dot1x timeout supp-timeout <interval>

11.3.9 Configuration port is the transport port

When the switch is not open 802.1x authentication, and subnet other switches to open the 802.1x certification, can configure the switch connection client and the authentication switch port for transmission port forwarding eapol authentication packets between the client and the authentication of 802.1x switches. So as to realize the 802.1x authentication of other switches to the client。

The following command sets port ge1/1 as the transport port in the interface configuration mode：

Switch(config-ge1/1)dot1x transmit-port

The following command sets port ge1/1 as non transport port in the interface configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

mode：

Switch(config-ge1/1)no dot1x transmit-port

11.3.10 Configuring the 802.1x client version number

Configure the version number of the 802.1x client, and only the client whose version is not less than the version number of the configuration can be authenticated, otherwise the authentication fails. The default client version number of the switch is 2。

The following command configures the client version number in global CONFIG mode：

Switch(config)# dot1x client-version <string>

11.3.11 Configure whether to check the client version number

Configure whether to check the version number of the 802.1x client. If configured to check, the switch first checks the client version number when authenticating. The default is configured to check。

The following command configures the global CONFIG mode to open the check of the client version number：

Switch(config)# dot1x check-version open

11.3.12 Configuration authentication method

The authentication method of configuration switch to 802.1x packet, the client initiated authentication method is divided into universal authentication and extended authentication, the switch can be configured as the first to which way authentication. If the client initiated authentication method is inconsistent with the authentication method of the switch configuration, the client will initiate authentication after another failure of authentication。

The following command configures the authentication method of the switch in the global CONFIG mode to extend the authentication mode：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)# dot1x extended

11.3.13 Configure whether to check the client's timing packet

Timing switch to check whether the package configuration of the client in the authentication succeeds, exchange the opportunity to ask the client regularly send 802.1x packets, but not all of the clients will regularly send 802.1x packets on certification through, this configuration through the command switch timing packet inspection of the client。

The following command is configured as a switch in the global CONFIG mode to check the client's timing packet：

Switch(config)# dot1x check-client

11.3.14 Display 802.1x information

The following command in the normal mode / privilege mode display 802.1x information, when the command is show dot1x, display 802.1x configuration information for all, including the configuration information for all ports; when the command is show dot1x interface, to display all the information user access port：

Switch#show dot1x

Switch#show dot1x interface

11.4 configuration RADIUS

This section gives a detailed description of the configuration of RADIUS, including the following：

- RADIUS Default configuration
- Configuring the IP address of the authentication server
- Configuring shared keys
- Start and close billing
- Configuring RADIUS ports and attribute information
- Configuring RADIUS roaming function
- Display RADIUS information

SEC.RU | Короткий путь к информации
Скачано с sec.ru

11.4.1 RADIUS Default configuration

switch RADIUS configuration defaults as follows：

- There is no IP address for the primary authentication server and the backup authentication server, that is, the IP address is 0.0.0.0。
- There is no configuration share key, that is, the shared key string is empty。
- Billing is initiated by default。
- RADIUS authentication UDP port is 1812, billing UDP port is 1813。
- The value of RADIUS attribute NASPort is 0xc353, the value of NASPortType is 0x0f, and the value of NASPortServer is 0x02。

11.4.2 Configuring the IP address of the authentication server

In order to communicate between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. RADIUS. In practical applications, you can use an authentication server, you can also use two authentication servers, one as the main authentication server, one as backup authentication server. If the switch is configured with two authentication server IP addresses, when the switch and the main authentication server interrupt communication, you can switch to the backup authentication server communication。

The following command configures the IP address of the master authentication server in the global CONFIG mode：

Switch(config)#radius-server host <ip-address>

The following command configures the IP address of the backup authentication server in the global CONFIG mode：

Switch(config)#radius-server option-host <ip-address>

11.4.3 Configuring shared keys

Mutual authentication is needed between the switch and authentication server, and the same shared key is needed on the switch and authentication server. Note that the shared key on the switch must be the same as the authentication server。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The following command configures the shared key of the switch in the global CONFIG mode：

Switch(config)#radius-server key <string>

11.4.4 Start and close billing

If the switch closes the billing, the switch will not send the RADIUS packet to the authentication server when the authentication is successful or the user is offline. In general, billing is open in practical applications。

The following command initiates billing in global CONFIG mode：

Switch(config)#radius-server accounting

The following command closes billing in global CONFIG mode：

Switch(config)#no radius-server accounting

11.4.5 Configuring RADIUS ports and attribute information

It is recommended that users do not modify the RADIUS port and attribute information configuration。

The following command modifies the RADIUS authentication UDP port in the global CONFIG mode：

Switch(config)#radius-server udp-port <port-number>

The following command modifies the RADIUS attribute information in global CONFIG mode：

Switch(config)#radius-server attribute nas-portnum <number>

Switch(config)#radius-server attribute nas-porttype <number>

Switch(config)#radius-server attribute service-type <number>

11.4.6 Configuring RADIUS roaming function

When MAC, IP or VLAN binding is made to the client, when the client is moved to other places, the binding client can not carry out 802.1x authentication because of the MAC address, IP address or VLAN change. Open the radius roaming function, will ignore the client's MAC, IP or

SEC.RU | Короткий путь к информации
Скачано с sec.ru

VLAN binding, so as to continue to achieve 802.1x authentication。

The following command configures the RADIUS roaming function in the global CONFIG mode：

Switch(config)#radius-server roam

The following command closes the RADIUS roaming function in global CONFIG mode：

Switch(config)#no radius-server roam

11.4.7 Display RADIUS information

The following command displays RADIUS configuration information in normal mode / privilege mode：

Switch#show radius-server

11.5 Configuration example

Open the 802.1x protocol, configure the port ge1/1 is Auto state, configure the main authentication server is 198.168.80.111, configure the switch shared secret key is ABCDEF。

Switch#

Switch# dot1x

Switch#config t

Switch(config)#radius-server host 198.168.80.111

Switch(config)#radius-server key abcdef

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dot1x control auto

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Twelfth chapters

GMRPconfiguration

The main contents of this chapter are as follows：

- GMRP introduce
- configuration GMRP
- Examples of typical GMRP configurations

12.1 GMRP introduce

At present, GMRP (GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, which is used to maintain the multicast registration information in the switch. All the support GMRP switch can receive the multicast registration information from other switches, and dynamically update the local multicast registration information, but also to the local multicast registration information spread to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP supported devices in the same switching network。

When a host wants to join a multicast group, it sends GMRP to join the message. The switch will receive the port of adding GMRP message to the multicast group, and broadcast the GMRP into the message in the VLAN where the receiving port is located. The multicast source in VLAN can know the existence of multicast members. When the multicast source sends multicast packets to the multicast group, the switch only forwards the multicast packets to the ports connected to the multicast group members, thus realizing the two layer multicast in the VLAN。

12.2 configuration GMRP

The main configuration of GMRP includes：
Open GMRP
View GMRP
In configuration tasks, you must first open the global GMRP to open the port GMRP。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

12.2.1 Open GMRP settings

command	describe	Configuration mode
set gmrp enable | disable	Enable / go global VLAN GMRP	Global configuration mode
set gmrp enable vlan <vlan-id>	Enabling globally specific VLAN GMRP	Global configuration mode
set gmrp registration{fixed | forbidden | normal} <if-name>	Configuring interface registration multicast mode	Global configuration mode
set gmrp timer {join | leave | nleaveall} <time-value>	The timing of configuring various timers	Global configuration mode
set port gmrp enable <if-name>	Enable port GMRP function	Global configuration mode
set port gmrp disable <if-name>	De enable port GMRP function	Global configuration mode

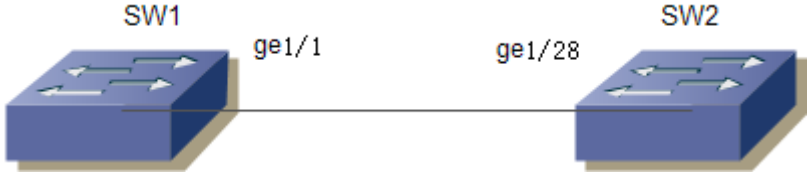
12.2.2 View GMRP information

After completing the above configuration, executing show command in any view can display the operation of GMRP after configuration, and verify the effect of configuration by checking the display information。

command	describe	Configuration mode
show gmrp configuration	View GMRP configuration information	Privileged mode
show gmrp machine	View GMRP state machine information	Privileged mode
show gmrp statistics vlanid	See the GMRP statistics of specific vlanid	Privileged mode
show gmrp timer <ifname>	View timer information for specific ports	Privileged mode

12.3 Examples of typical GMRP configurations

1. Networking requirement
In order to realize dynamic registration and update of multicast information between switches, it is necessary to start GMRP on the switch
2. Network diagram



GMRP example network diagram

3. Configuration steps
Configuring SW1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port ge1/1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Configuring SW2

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port ge1/28

Switch(config)# set port gmrp enable ge1/28

Switch(config)#

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Thirteenth chapters

SNOOPING configuration

In the metropolitan area network /Internet, using unicast sends the same packet to the network in many but not all recipients, because of the need to copy each packet to the receiving endpoint, with the increasing number of receivers, the number of packets will need a linear increase, which makes the host, exchange the overall burden of routing equipment and the network bandwidth increase, efficiency is greatly affected. With the increasing demand for multipoint video conferencing, video on demand and group communication applications, multicast has become the most popular mode of communication in order to improve resource utilization。

switch implements the function of IGMP SNOOPING for multicast application service. IGMP SNOOPING monitors IGMP packets on the network to realize dynamic learning of IP multicast MAC addresses。

This chapter describes the concept and configuration of IGMP SNOOPING, including the following contents：

- GMP SNOOPING introduce
- IGMP SNOOPING configuration
- The IGMP SNOOPING configuration example

13.1 IGMP SNOOPING introduce

Traditional network in a subnet multicast packets as broadcast processing, so easy to make network traffic, causing network congestion. When the switch is implemented on IGMP SNOOPING, IGMP SNOOPING can learn IP dynamic multicast MAC address, to maintain the output port list IP multicast MAC address, the multicast data flow only to the output port to send, it can reduce the network traffic.

The main contents of this section are as follows：

- IGMP SNOOPING processing
- Second layer dynamic multicast
- Join a group
- Leave a group

13.1.1 IGMP SNOOPING processing

SEC.RU | Короткий путь к информации
Скачано с sec.ru

IGMP SNOOPING is a two layer network protocol, the IGMP protocol packets through the switch monitoring, according to the receiving port these IGMP protocol package, VLAN ID and multicast address to maintain a multicast group, and then forwarded these IGMP protocol. Only multicast ports can be added to receive multicast data streams; thus, the network traffic is reduced and the network bandwidth is saved。

Multicast group includes multicast group address, member port, VLAN ID, Age time。

The formation of IGMP SNOOPING multicast group is a learning process. When one port of the switch receives the IGMP REPORT packet, IGMP SNOOPING generates a new multicast group, and the port that receives the IGMP REPORT packet is added to the multicast group. When a IGMP QUERY packet is received by the switch, if the multicast group already exists in the switch, then the port received the IGMP QUERY is added to the multicast group, otherwise it will only forward the IGMP QUERY packet. Leave SNOOPING also supports the IGMP mechanism of IGMP V2 IGMP SNOOPING; if the configuration of the fast-leave ENABLE in IGMP V2, received leave packet when it receives port can leave the multicast group immediately; if the configuration of the fast-leave left the waiting time (fast-leave-timeout), then the multicast group waiting for this time expires after leaving the multicast group。

There are two update mechanisms for IGMP SNOOPING. One is the leave mechanism described above. In most cases, IGMP SNOOPING deletes expired multicast groups through age time. When the multicast group joins the IGMP SNOOPING, the added time is recorded. When the multicast group has more than one configured age time in the switch, the exchange opportunity deletes the multicast group。

When a port to receive Leave packets, this port will immediately removed from the multicast group to which it belongs, this situation may affect the continuity of the network data stream; because this network equipment port below may be connected to a HUB or no IGMP SNOOPING function, the equipment connected to receive the multicast data under many of the current equipment. A device sends Leave, which may affect other devices and can not receive multicast data streams. Fast-leave-timeout mechanism can prevent the occurrence of this situation, through the Fast-leave-timeout configuration of a left waiting time, port leave packets received after waiting for Fast-leave-timeout long time and then removed from the multicast group to which it belongs, to guarantee the continuity of network multicast stream。

13.1.2 Second layer dynamic multicast

The multicast MAC address entries in the two layer hardware multicast forwarding table can be dynamically learned by IGMP SNOOPING. The IP multicast MAC address is dynamically learned through IGMP SNOOPING。

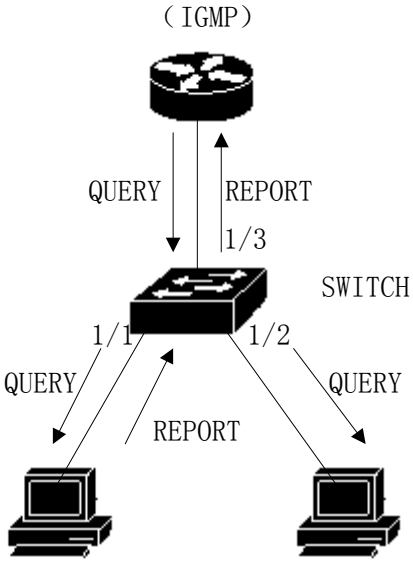
SEC.RU | Короткий путь к информации
Скачано с sec.ru

When the switch off IGMP SNOOPING, the two layer hardware multicast forwarding table in unregistered forwarding mode, multicast MAC address cannot be dynamically learned that two layer hardware multicast forwarding table no entries, two layer multicast data stream as all broadcast processing。

When the network multicast environment, in order to effectively control the multicast traffic network, the switch can open the IGMP SNOOPING, the two layer hardware multicast forwarding table in register forwarding mode, the switch can learn to multicast MAC address through the monitoring network on the IGMP protocol, and the two layer hardware multicast forwarding entries in the table, the two layer multicast to be able to flow forward。

13.1.3 Join a group

When a host wants to join a multicast group, the host sends a IGMP REPORT packet, which specifies the multicast group to which the host is to join. When the switch receives a IGMP QUERY packet, the packet forwarding will switch to the same VLAN all other ports, when the IGMP QUERY packet is received under the port to join a multicast group after the host return a IGMP REPORT package. When a IGMP REPORT packet is received, a two layer multicast entry is established, and the port of the IGMP QUERY packet and the port of the IGMP REPORT packet are added to the two layer multicast item to become its output port。

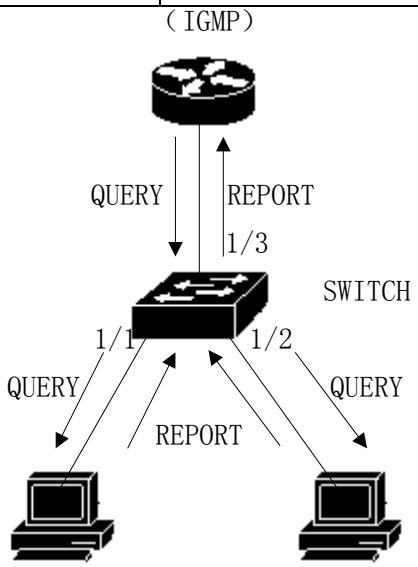


If all the devices in the picture are in a subnet, suppose that the subnet VLAN is 2. Router runs IGMPv2 protocol and sends IGMP QUERY packets regularly. Host 1 wants to join multicast group 224.1.1.1. After receiving the IGMP QUERY packet from the 1/3 port, the switch will

SEC.RU | Короткий путь к информации
Скачано с sec.ru

record the port and forward the packet to port 1/1 and 1/2. Host 1 sends a IGMP REPORT packet after receiving the IGMP QUERY packet, and host 2 does not send IGMP REPORT packets because it does not want to join the multicast group. After receiving the IGMP REPORT packet from the port 1/1, the switch forwards the packet from the query port 1/3 and creates a two layer multicast item (assuming that the item does not exist). The two layer multicast entry includes the following items：

Two layer multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/3



As shown in Figure 1, host 1 has added multicast group 224.1.1.1, and now host 2 wants to join multicast group 224.1.1.1. When the host 2 received IGMP QUERY packet after sending back a IGMP REPORT packet switch IGMP REPORT received from the 1/2 port will put the package from the 1/3 query port forwarded and make port 1/2 was added to the two layer multicast entry, the entry into the two layer multicast：

Two layer multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/2，1/3

SEC.RU | Короткий путь к информации
Скачано с sec.ru

13.1.4 Leave a group

In order to be able to form a stable multicast environment, IGMP devices (such as routers) send a IGMP QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or who wants to join the multicast group returns a IGMP REPORT after receiving the IGMP QUERY。

If the host wants to leave a multicast group, there are two ways: the active leave and the passive leave. The active departure is the host sends a IGMP LEAVE packet to the router, and the passive departure is when the host receives the IGMP QUERY sent by the router and does not send back the IGMP REPORT。

When the host leaves the multicast group, there are two ways to switch off the two layer multicast from the switch: leave out of time and receive the IGMP LEAVE packet。

When the switch over a certain time from one port to receive a multicast group IGMP REPORT packet, the port should be removed from the two layer multicast entry corresponding, if the two layer multicast entries without port, delete two layer multicast entries。

When the switch fast-leave is configured as a ENABLE, if a port receives a multicast group IGMP LEAVE packet, clear the port from the two layer multicast entry corresponding, if the two layer multicast no entry port, then delete the layer two multicast entries。

Fast-leave is generally used by one host in a port under the circumstances; if a port under more than one host, you can configure the fast-leave-timeout waiting time, so as to ensure the continuity and reliability of multicast flow。

13.2 IGMP SNOOPING configuration

13.2.1 IGMP SNOOPING default configuration

The default IGMP SNOOPING is closed, and the two layer hardware multicast forwarding table is in the unregistered forwarding mode。

Fast-leave is closed by default。

Fast-leave-timeout time is 300 seconds。

The age time of multicast group REPORT port defaults to 400 seconds。

The age time of multicast group QUERY port defaults to 300 seconds。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

13.2.2 Open and close IGMP SNOOPING

Open the IGMP SNOOPING protocol can be global open, you can also open part of the VLAN; only global open IGMP SNOOPING to open or close a VLAN IGMP SNOOPING。

Open global IGMP SNOOPING
Switch#configure terminal
Switch(config)#ip igmp snooping

Open a VLAN IGMP SNOOPING
Switch#configure terminal
Switch(config)#ip igmp snooping vlan <vlan-id>

Close global IGMP SNOOPING
Switch#configure terminal
Switch(config)#no ip igmp snooping

Close a VLAN IGMP SNOOPING
Switch#configure terminal
Switch(config)#no ip igmp snooping vlan <vlan-id>

13.2.3 Configuration survival time

Configuring the lifetime of multicast groups
Switch#configure terminal
Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds。

The lifetime of configuration query groups
Switch#configure terminal
Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

13.2.4 configuration fast-leave

Start a VLAN fast-leave
Switch#configure terminal
Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Close fast-leave
Switch#configure terminal
Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configuring fast-leave wait time
Switch#configure terminal
Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Recovery default fast-leave wait timeSwitch#configure terminal
Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

13.2.5 configuration MROUTER

Configuring a static query port
Switch#configure terminal
Switch#interface ge1/6
Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

13.2.6 display information

Display IGMP SNOOPING configuration information
Switch#show ip igmp snooping

Displays a configuration information for VLAN
Switch#show ip igmp snooping vlan <vlan-id>

Display aging information of REPORT multicast group
Switch#show ip igmp snooping age-table group-membership

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Display the aging information of QUERY

Switch#show ip igmp snooping age-table query-membership

Display forwarding information of multicast group

Switch#show ip igmp snooping forwarding-table

Display MROUTER information

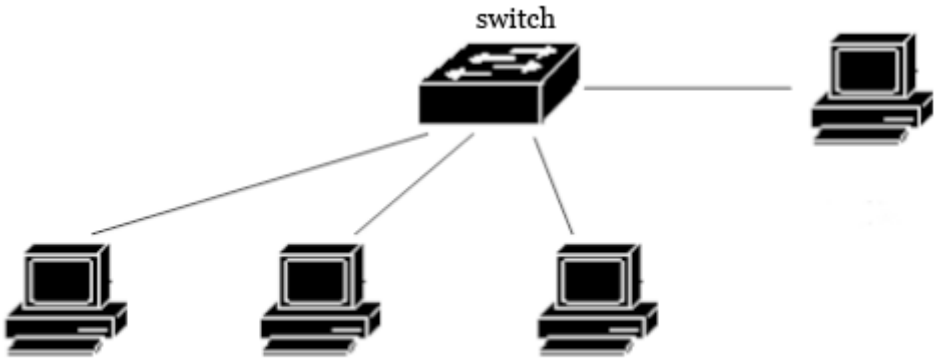
Switch#show ip igmp snooping mrouter

The display system is currently configured, including the configuration of IGMP SNOOPING

Switch#show running-config

13.3 The IGMP SNOOPING configuration example

The IGMP SNOOPING function is enabled on the switch. The user 1, the user 2, and the user 3 can be added to the particular multicast group。



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ip igmp snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

Fourteenth chapters

MVR configuration

The main contents of this chapter are as follows：

- MVR profile
- configuration MVR
- MVR configuration example

14.1 MVR profile

Multicast VLAN registration (MVR) is applied to multicast streaming applications in service provider networks, such as vod. MVR allows users to subscribe to or cancel multicast flows within the multicast VLAN, allowing a multicast VLAN to share data streams with other VLAN. MVR has two purposes: (1) through simple configuration, it can effectively and securely transfer multicast flows between VLAN; (2) support multicast groups dynamically join and leave；

MVR is similar to IGMP snooping in that two functions can be started at the same time, MVR only handles the joining and leaving of configured multicast groups, and the other groups

SEC.RU | Короткий путь к информации
Скачано с sec.ru

join and leave by IGMP snooping management. The difference between them is that multicast flows in IGMP snooping can only be forwarded within one VLAN, while MVR multicast streams can be forwarded in different VLAN。

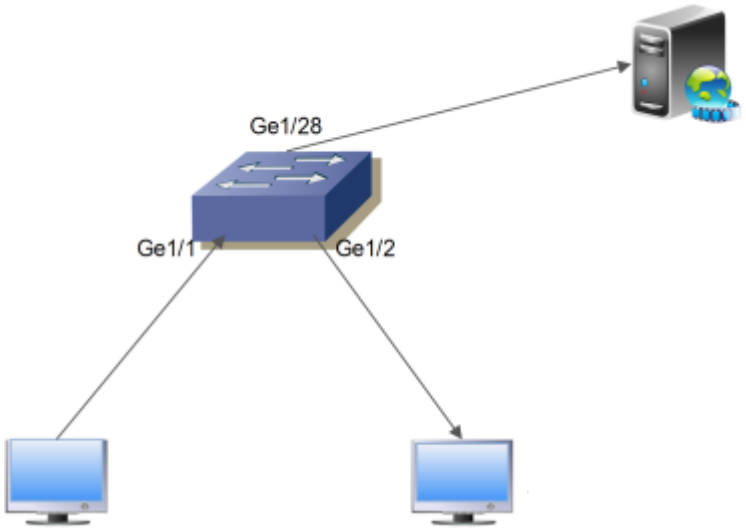
14.2 configuration MVR

command	describe	CLI mode
mvr (enable|disable)	Start global MVR	Global configuration mode
no mvr	Clear all MVR configurations	Global configuration mode
mvr group A.B.C.D	Configuring IP multicast address	Global configuration mode
no mvr group A.B.C.D	Delete IP multicast address	Global configuration mode
mvr group A.B.C.D <1-256>	Configure the IP multicast address and configure a continuous MVR group address	Global configuration mode
mvr vlan <1-4094>	Specifies the VLAN to receive multicast data	Global configuration mode
no mvr vlan	Restore default VLAN1 for receiving multicast data	Global configuration mode
mvr-interface (enable|disable)	Boot interface MVR	Interface configuration mode
show mvr	Display MVR configuration information	Privileged mode

14.3 MVR configuration example

Network topology as shown below, the user 1 and user 2 belong to vlan10 vlan20 respectively, user 1 and user 2 see the same program, program range 225.1.1.1~225.1.1.64, MVR VLAN is 100：

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Configure VLAN, start global IGMP snooping, configure MVR VLAN, MVR program group range, global enable MVR：

Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#

Configure switch user port Ge1/1 Ge1/2, and uplink Ge1/28：
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan add 10 egress-tagged disable
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable
Switch(config-ge1/1)#

Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 20 egress-tagged disable
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable
Switch(config-ge1/2)#

Switch#configure terminal
Switch(config)#interface ge1/28
Switch(config-ge1/28)#switchport mode trunk
Switch(config-ge1/28)#switchport trunk allowed vlan add 100
Switch(config-ge1/28)#

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Fifteenth chapters

DHCP SNOOPING configuration

In the dynamic access network environment, the host obtains the IP address and the network parameter through the DHCP server. DHCP SNOOPING is a kind of interception protocol for ARP attack. By listening to the DHCP message, dynamically binding the DHCP server to the client's IP address and the client's MAC address, so as to filter the ARP attack message on the switch。

switch support DHCP SNOOPING function, can effectively defend ARP attack. DHCP SNOOPING listens to the DHCP message on the network and binds the port ARP information。

You can configure four links to DHCP server physical ports, to some extent, to prevent unknown server interference networks。

When the switch power off restart, the binding table will be lost and need to be re learned; switch provides binding table uploading and downloading function, and the binding table can be stored in the TFTP server。

This chapter describes the concept and configuration of DHCP SNOOPING, including the following contents：

- DHCP SNOOPING introduce
- DHCP SNOOPING configuration
- DHCP SNOOPING configuration example
- DHCP SNOOPING configuration error

15.1 DHCP SNOOPING introduce

Because of the simple trust mechanism, the ARP protocol has caused a loophole to the network security. When a ARP attack message carrying a false MAC message arrives at the host, it will override the local ARP cache table directly without restriction, leading to the normal data flow to the attacker. Therefore, the ARP information binding of ports can be implemented on the network two layer switch, which can effectively filter the ARP attack packets and make the attack packets unable to reach the attack host. If the network has not foreseen into the DHCP server, IP address distribution will lead to confusion, DHCP SNOOPING protocol provides a physical port binding link server, physical port can not be non specified by the DHCP server forwarding DHCP packets, can reduce the unknown server into the network the opportunity。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The main contents of this section are as follows：

- DHCP SNOOPING processing
- DHCP SNOOPING binding table
- DHCP SNOOPING specifies the physical port of the linked server
- DHCP SNOOPING binding list is uploaded and downloaded

15.1.1 DHCP SNOOPING processing

The DHCP SNOOPING protocol listens only to DHCPrequest, DHCPack, DHCPrelease three kinds of messages, does not receive other types of DHCP packets, and binds the mapping relationship between IP and MAC according to these messages。

The global DHCP SNOOPING switch is responsible for opening the switch to receive DHCP packets, i.e., UDP ports are 67 and 68 IP packets。

15.1.2 DHCP SNOOPING binding table

The DHCP SNOOPING binding table entries are indexed by the MAC address, including item type, IP address, MAC address, interface information, delay timer, lease timer. The type of REQ and ACK in two, type REQ entry indicates that the DHCPrequest message is received, the DHCPack has not yet received the message, then start delay timer, the default time interval is 10 seconds, 10 seconds if it fails to receive an DHCPack message, the REQ type binding table entries are deleted; type ACK entry indicates that the DHCPack message is received and recorded the IP server address is assigned IP address, then start the lease timer, time interval is included in the DHCPack message DHCP server provides the lease contract value, the timer is restarted, the lease expires, the binding table entries are deleted. The interface information records the interface where the client is, that is, the interface between the IP address and the MAC address binding。

When the DHCPrequest message is received, the binding table entries are created, the entries type is REQ, the IP address, the MAC address, the interface information, and the 10 second delay timer are set up。

When the DHCPrequest message is received, the REQ type binding table entries already exist, the entries are updated, and the delay timers are restarted。

When the DHCPrequest message is received, the ACK type binding table entry already exists, then the interface information is recorded。

When receiving the DHCPack message, if there is a REQ type binding table entry, the IP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

address allocated by the server in the DHCPack message is recorded, the delay timer is closed, and the lease timer is started。

When receiving the DHCPack message, there is no REQ type binding table entry, and then the message is dropped。

When DHCPack packets are received, ACK type binding table entries already exist. If the interface has changed, the binding table entries of the original interface are deleted, and the entries are updated。

If the interface does not change, the IP address assigned by the server changes, deleting the binding table entries of the original interface and updating the entries。

If the interface does not change, the IP address has not changed, indicating that the renewal process, restart the lease timer can be。

When the timeout timer expires, the REQ type binding table entries are deleted。

When the lease timer timeout, the ACK type binding table entries are deleted。

15.1.3 DHCP SNOOPING specifies the physical port of the linked server

DHCP SNOOPING specifies the physical port of the linked server, and only the DHCP message can be received on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the server from the non specified port will be filtered, and the IP address can not be assigned to the client. Designated ports are conducive to the unified allocation of IP addresses in the network, to avoid the unknown server address pool is not in the IP planning, some clients can not normally connect to the network. To some extent, it reduces the probability of network communication anomalies caused by unauthorized access to the server。

15.1.4 DHCP SNOOPING binding list is uploaded and downloaded

DHCP SNOOPING records the binding relationship between IP and MAC by monitoring the DHCP message, and maintains its binding table. When the switch is switched off, restart or malfunction occurs, the binding table will be lost when the power is cut off unexpectedly, and the switch needs to learn the binding table entries after restarting. In the network topology, it is difficult to identify the network connection interruption and restart the DHCP discover process, unless the host is directly connected, and the switch will be difficult to re learn the binding information. For this reason, the binding table is saved on the TFTP server and the binding table is

SEC.RU | Короткий путь к информации
Скачано с sec.ru

downloaded after the switch is restarted, which can solve the transient memory gap when the switch is restarted. The switch provides the binding table upload and download function, the administrator can be ordered through the manual upload or download the binding table, can automatically upload configuration commands, uploaded the binding table; the binding table command in the starting process from the TFTP server to download the backup file and the binding table has the binding table into the DHCP SNOOPING protocol module automatically restart the download。

15.2 DHCP SNOOPING configuration

15.2.1 DHCP SNOOPING default configuration

DHCP SNOOPING is closed by default。

DHCP SNOOPING binding table type REQ entry delay timer default time interval is 10 seconds。

15.2.2 Global open and close DHCP SNOOPING

When the DHCP SNOOPING is opened globally, the DHCP SNOOPING of an interface can be turned on or off, and DHCP SNOOPING of all interfaces must be turned off before the global DHCP SNOOPING can be turned off。

Open global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

The parameter is the physical port list of the linked DHCP server that needs to be bound. A total of four ports can be specified, and the port list is separated by "", "ge1/1", "ge1/25", "ge1/26"

Close global DHCP SNOOPING

Switch#configure terminal

Switch(config)#no ip dhcp snooping

SEC.RU | Короткий путь к информации
Скачано с sec.ru

15.2.3 The interface opens and closes DHCP SNOOPING

Open an interface for DHCP SNOOPING

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

DHCP SNOOPING that closes an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

15.2.4 DHCP SNOOPING binding list is uploaded and downloaded

Upload the DHCP SNOOPING binding table to the TFTP server

Switch#configure terminal

Switch(config)#dhcp snooping upload A.B.C.D FILE_NAME

Parameters: the IP address of A.B.C.D TFTP server; the name of the binding table file that is saved on the TFTP server by FILE_NAME。

Download the DHCP SNOOPING binding table from the TFTP server

Switch#configure terminal

Switch(config)#dhcp snooping download A.B.C.D FILE_NAME

Configure timed upload DHCP SNOOPING binding table to TFTP server

Switch#configure terminal

Switch(config)#dhcp snooping auto-upload A.B.C.D FILE_NAME interval

Parameters: interval upload interval time, ranging from 1 minutes to one day。

Cancel the configuration of DHCP SNOOPING binding table to TFTP server regularly

Switch#configure terminal

Switch(config)#no dhcp snooping auto-upload

Automatically download the DHCP SNOOPING binding table from the TFTP server when configuration restarts

Switch#configure terminal

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)#dhcp snooping reset-download A.B.C.D FILE_NAME

Automatically configure the configuration of the DHCP SNOOPING binding table from the TFTP server when the restart is cancelled

Switch#configure terminal

Switch(config)#no dhcp snooping reset-download

15.2.5 display information

Display DHCP SNOOPING configuration information

Switch#show dhcp snooping

Display DHCP SNOOPING binding table information

Switch#show dhcp snooping binding-table

The display system is currently configured, including the DHCP SNOOPING configuration。

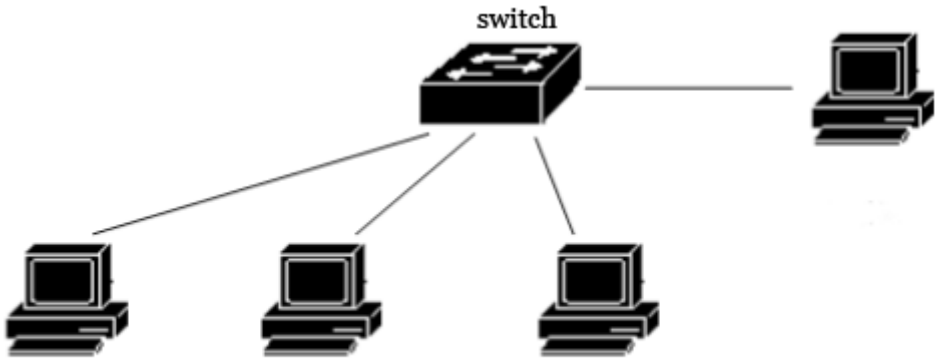
Switch#show running-config

15.3 DHCP SNOOPING configuration example

15.3.1 configuration

The DHCP SNOOPING function is enabled on the two layer switch, and the user 1, the user 2 and the user 3 obtain the IP address and network parameters dynamically through the DHCP server. User 1, user 2, user 3 interface start DHCP SNOOPING function, dynamically binding ARP information in the interface。

SEC.RU | Короткий путь к информации
Скачано с sec.ru




```
Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/9
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#end
Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface：ge1/9
Enable interface: ge1/1 ge1/2 ge1/3
Switch#show dhcp snooping binding-table
```

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	00:11:5b:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	00:11:64:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	00:11:80:4d:a2:46	ACK	ge1/3	20:34:45

```
Switch#show running-config
!
ip dhcp snooping ge1/9
!
spanning-tree mst configuration
!
interface vlan1
  Ip address 192.168.0.1/24
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
!
interface ge1/1
 dhcp snooping
!
interface 1/2
 dhcp snooping
!
interface 1/3
 dhcp snooping
!
line vty
!
End
Switch#
```

15.4 DHCP SNOOPING configuration error

If the DHCP snooping configuration fails, it may be caused by the following reasons：

1、System CFP resource exhaustion。

2、If the interface is configured, the ACL filtering function fails to open the DHCP SNOOPING globally

3、When the interface is configured with IP binding to MAC, the global open DHCP SNOOPING fails

4、The current interface is configured with the ACL filter function。

5、The current interface enables 802.1x anti ARP spoofing。

6、The configured interface is a three layer interface or a trunk interface。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Sixteenth Chapters

MLD SNOOPING configuration

In the metropolitan area network /Internet, using unicast sends the same packet to the network in many but not all recipients, because of the need to copy each packet to the receiving endpoint, with the increasing number of receivers, the number of packets will need a linear increase, which makes the host, exchange the overall burden of routing equipment and the network bandwidth increase, efficiency is greatly affected. With the increasing demand for multipoint video conferencing, video on demand and group communication applications, multicast has become the most popular mode of communication in order to improve resource utilization。

switch implements the function of MLD SNOOPING for multicast application service. MLD SNOOPING monitors MLD packets on the network to realize dynamic learning of IPV6 multicast MAC addresses。

This chapter describes the concept and configuration of MLD SNOOPING, including the following contents：

- MLD SNOOPING introduce
- MLD SNOOPING configuration
- MLD SNOOPING configuration example

16.1 MLD SNOOPING introduce

Traditional network in a subnet multicast packets as broadcast processing, so easy to make network traffic, causing network congestion. When the switch is implemented on MLD SNOOPING, MLD SNOOPING can learn IPV6 dynamic multicast MAC address, to maintain the output port list IPV6 multicast MAC address, the multicast data flow only to the output port to send, it can reduce the network traffic。

The main contents of this section are as follows：

- MLD SNOOPING processing
- Second layer dynamic multicast
- Join a group
- Leave a group

SEC.RU | Короткий путь к информации
Скачано с sec.ru

16.1.1 MLD SNOOPING processing

MLD SNOOPING is a two layer network protocol, the MLD protocol packets through the switch monitoring, according to the receiving port these MLD protocol package, VLAN ID and multicast address to maintain a multicast group, and then forwarded these MLD protocol. Only multicast ports can be added to receive multicast data streams; thus, the network traffic is reduced and the network bandwidth is saved。

Multicast group includes multicast group address, member port, VLAN ID, Age time。

The formation of MLD SNOOPING multicast group is a learning process. When one port of the switch receives the MLD REPORT packet, MLD SNOOPING generates a new multicast group, and the port that receives the MLD REPORT packet is added to the multicast group. When a MLD QUERY packet is received by the switch, if the multicast group already exists in the switch, then the port received the MLD QUERY is added to the multicast group, otherwise it will only forward the MLD QUERY packet. Done SNOOPING also supports the MLD mechanism of MLD V2 MLD SNOOPING; if the configuration of the fast-leave ENABLE in MLD V2, received Done packet when it receives port can leave the multicast group immediately; if the configuration of the fast-leave left the waiting time (fast-leave-timeout), then the multicast group waiting for this time expires after leaving the multicast group。

There are two update mechanisms for MLD SNOOPING. One is the Done mechanism described above. In most cases, MLD SNOOPING deletes expired multicast groups through age time. When the multicast group joins the MLD SNOOPING, the added time is recorded. When the multicast group has more than one configured age time in the switch, the exchange opportunity deletes the multicast group。

When a port to receive Done packets, this port will immediately removed from the multicast group to which it belongs, this situation may affect the continuity of the network data stream; because this network equipment port below may be connected to a HUB or no MLD SNOOPING function, the equipment connected to receive the multicast data under many of the current equipment. A device sends Done, which may affect other devices and can not receive multicast data streams. Fast-leave-timeout mechanism can prevent the occurrence of this situation, through the Fast-leave-timeout configuration of a left waiting time, port leave packets received after waiting for Fast-leave-timeout long time and then removed from the multicast group to which it belongs, to guarantee the continuity of network multicast stream。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

16.1.2 Second layer dynamic multicast

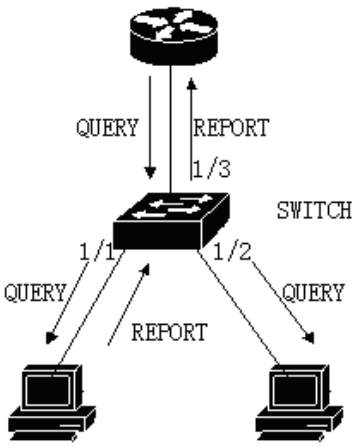
The multicast MAC address entries in the two layer hardware multicast forwarding table can be dynamically learned by MLD SNOOPING. The IPV6 multicast MAC address is dynamically learned through MLD SNOOPING。

When the switch off MLD SNOOPING, the two layer hardware multicast forwarding table in unregistered forwarding mode, multicast MAC address cannot be dynamically learned that two layer hardware multicast forwarding table no entries, two layer multicast data stream as all broadcast processing。

When the network multicast environment, in order to effectively control the multicast traffic network, the switch can open the MLD SNOOPING, the two layer hardware multicast forwarding table in register forwarding mode, the switch can learn to multicast MAC address through the monitoring network on the MLD protocol, and the two layer hardware multicast forwarding entries in the table, the two layer multicast to be able to flow forward。

16.1.3 Join a group

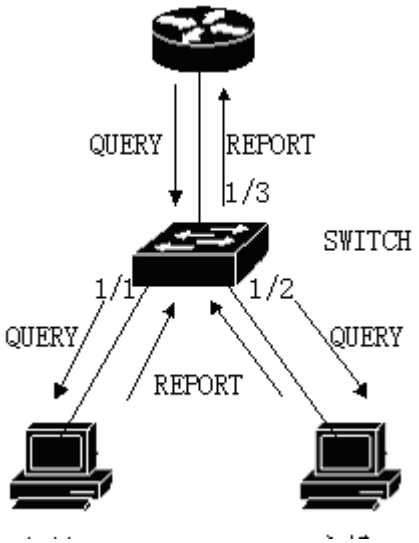
When a host wants to join a multicast group, the host sends a MLD REPORT packet, which specifies the multicast group to which the host is to join. When the switch receives a MLD QUERY packet, the packet forwarding will switch to the same VLAN all other ports, when the MLD QUERY packet is received under the port to join a multicast group after the host return a MLD REPORT package. When a MLD REPORT packet is received, a two layer multicast entry is established, and the port of the MLD QUERY packet and the port of the MLD REPORT packet are added to the two layer multicast item to become its output port。



SEC.RU | Короткий путь к информации
Скачано с sec.ru

If all the devices in the picture are in a subnet, suppose that the subnet VLAN is 2. Router runs MLDv2 protocol and sends MLD QUERY packets regularly. Host 1 wants to join multicast group ff15:: 1. After receiving the MLD QUERY packet from the 1/3 port, the switch will record the port and forward the packet to port 1/1 and 1/2. Host 1 sends a MLD REPORT packet after receiving the MLD QUERY packet, and host 2 does not send MLD REPORT packets because it does not want to join the multicast group. After receiving the MLD REPORT packet from the port 1/1, the switch forwards the packet from the query port 1/3 and creates a two layer multicast item (assuming that the item does not exist). The two layer multicast entry includes the following items：

Two layer multicast address	VLAN ID	Output port list
33:33:00:00:00:01	2	1/1，1/3



As shown in Figure 1, host 1 has added multicast group ff15:: 1, and now host 2 wants to join multicast group ff15:: 1. When the host 2 received MLD QUERY packet after sending back a MLD REPORT packet switch MLD REPORT received from the 1/2 port will put the package from the 1/3 port and forwarded the query packet port 1/2 was added to the two layer multicast entry, the entry into the two layer multicast：

Two layer multicast address	VLAN ID	Output port list
33:33:5e:00:00:01	2	1/1，1/2，1/3

SEC.RU | Короткий путь к информации
Скачано с sec.ru

16.1.4 Leave a group

In order to be able to form a stable multicast environment, MLD devices (such as routers) send a MLD QUERY packet to all hosts at regular intervals. The host that has joined the multicast group or who wants to join the multicast group returns a MLD REPORT after receiving the MLD QUERY。

If the host wants to leave a multicast group, there are two ways: the active leave and the passive leave. The active departure is the host sends a MLD LEAVE packet to the router, and the passive departure is when the host receives the MLD QUERY sent by the router and does not send back the MLD REPORT。

When the host leaves the multicast group, there are two ways to switch off the two layer multicast from the switch: leave out of time and receive the MLD DONE packet。

When the switch over a certain time from one port to receive a multicast group MLD REPORT packet, the port should be removed from the two layer multicast entry corresponding, if the two layer multicast entries without port, delete two layer multicast entries.

When the switch fast-leave is configured as a ENABLE, if a port receives a multicast group MLD LEAVE packet, clear the port from the two layer multicast entry corresponding, if the two layer multicast no entry port, then delete the layer two multicast entries。

Fast-leave is generally used by one host in a port under the circumstances; if a port under more than one host, you can configure the fast-leave-timeout waiting time, so as to ensure the continuity and reliability of multicast flow。

16.2 MLD SNOOPING configuration

16.2.1 MLD SNOOPING default configuration

The default MLD SNOOPING is closed, and the two layer hardware multicast forwarding table is in the unregistered forwarding mode。

Fast-leave is closed by default。

Fast-leave-timeout time is 300 seconds。

The age time of multicast group REPORT port defaults to 400 seconds。

The age time of multicast group QUERY port defaults to 300 seconds。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

16.2.2 Open and close MLD SNOOPING

Open the MLD SNOOPING protocol can be global open, you can also open part of the VLAN; only global open MLD SNOOPING to open or close a VLAN MLD SNOOPING。

Open global MLD SNOOPING
Switch#configure terminal
Switch(config)#ipv6 mld snooping

Open a VLAN MLD SNOOPING
Switch#configure terminal
Switch(config)#ipv6 mld snooping vlan <vlan-id>

Close global MLD SNOOPING
Switch#configure terminal
Switch(config)#no ipv6 mld snooping

Close a VLAN MLD SNOOPING
Switch#configure terminal
Switch(config)#no ipv6 mld snooping vlan <vlan-id>

16.2.3 Configuration survival time

Configuring the lifetime of multicast groups
Switch#configure terminal
Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds。

The lifetime of configuration query groups
Switch#configure terminal
Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>
The unit of Interval is milliseconds。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

16.2.4 configuration fast-leave

Start a VLAN fast-leave
Switch#configure terminal
Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Close fast-leave
Switch#configure terminal
Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>

Configuring fast-leave wait time
Switch#configure terminal
Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Recovery default fast-leave wait time
Switch#configure terminal
Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

16.2.5 configuration MROUTER

Configuring a static query port
Switch#configure terminal
Switch#interface ge1/6
Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]

16.2.6 display information

Display MLD SNOOPING configuration information
Switch#show ipv6 mld snooping

Displays a configuration information for VLAN
Switch#show ipv6 mld snooping vlan <vlan-id>

Display aging information of REPORT multicast group

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch#show ipv6 mld snooping age-table group-membership

Display the aging information of QUERY

Switch#show ipv6 mld snooping age-table query-membership

Display forwarding information of multicast group

Switch#show ipv6 mld snooping forwarding-table

Display MROUTER information

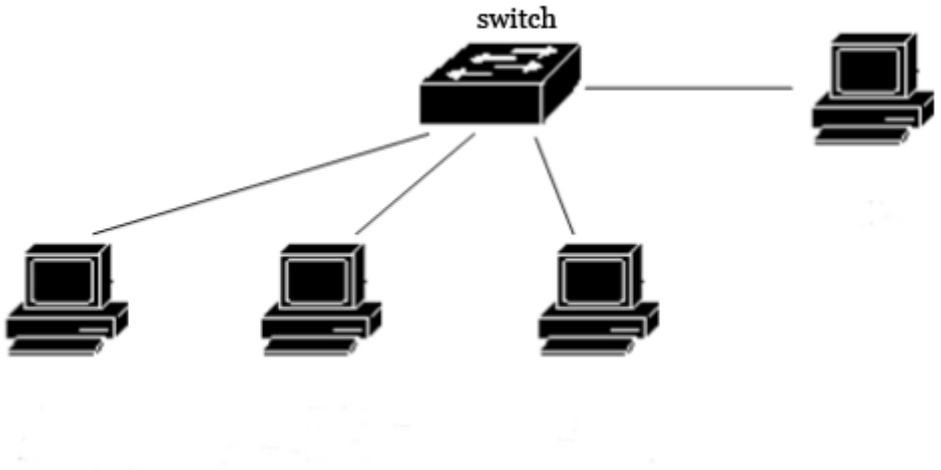
Switch#show ipv6 mld snooping mrouter

The display system is currently configured, including the configuration of MLD SNOOPING

Switch#show running-config

16.3 MLD SNOOPING configuration example

The MLD SNOOPING function is enabled on the switch. The user 1, the user 2, and the user 3 can be added to the particular multicast group。



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ipv6 mld snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200
```

Seventeenth chapters

ACL configuration

In the actual network, the access security of the network is the concern of the administrator. switches support ACL filtering to provide access security for the network. By configuring the ACL rules, the switches filter the input data stream according to these rules to realize the access security of the network。

This chapter describes how to configure ACL, including the following：

- Introduction of ACL resource library
- ACL filtering introduction
- ACL repository configuration
- ACL based on time interval
- ACL filter configuration
- ACL configuration example
- ACL configuration debugging

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.1 Introduction of ACL resource library

ACL (Access Control List) resource library is a set of multi group access rules. ACL resource library does not control the function of data forwarding, but only a set of rules sorted by conflict. When the ACL resource library is referenced, these applications control the forwarding of data according to the rules provided by the ACL resources. ACL can be applied to port access filtering, service access filtering and QoS, and so on。

The ACL resource group (group number 1 standard rules of IP ~ 991300 ~ 1999), IP group (group number 100 expansion rules ~ 1992000 ~ 2699), IP group MAC group ARP group (700~799> <, group 1100~1199)； Each group of rules is automatically prioritized by conflicting rules. When the user configured a ACL rule, the system inserts the rule into the corresponding location according to the collation。

In the application, when a data packet through a port, the switch will all fields corresponding to each rule in the field and in the data packet are compared; when appear at the same time a complete matching rules, a rule, the first fully effective; by this matching rule to determine data the package is forwarded or discarded. The so-called perfect match is that the value of the field in the rule is exactly equal to the value of the corresponding field in the packet. Only when a rule is fully matched with ACL, the rule can do the corresponding deny or permit operations。

In switches, the rules within the same group are automatically sorted. The automatic sorting of rules is relatively complicated. In the sorting process, a large range of rules is behind, and a small range is in front. The scope of the rule is determined by the constraint condition of the rule; the less the constraint condition of the rule is, the larger the range of the rule matching is; the more the rule constraints are, the smaller the range of the rule matching is. Constraint rules are mainly embodied in the number of wildcard addresses and some non address field. Wildcard is a bit string. The IP address is four bytes, and the MAC address is six bytes. Bits' 1 'means no matching, and bits' 0' means matching. Non address fields refer to protocol types, IP protocol types, protocol ports, and these fields also hide a wildcard. Their length is the byte length of the corresponding field, so the same field length is uniform, just counting the number of fields. The more bit the Wildcard is' 0 ', the more constraints。

Taking port access filtering as an example, the necessity of rule ranking and the advantages of automatic sorting are illustrated. If the user needs to reject the source address for the 192.168.0.0/16 segment address forwarding, allowing the source address for the 192.168.1.0/24 network address forwarding, you can configure the following two rules：

access-list 1 permit 192.168.1.0 0.0.0.255－Rule 1

access-list 1 deny 192.168.0.0 0.0.255.255 －Rule 2

Rule 1 and rule 2 are hereafter referred to as rule 2。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The two rules are conflicting; the address of rule 1 is contained in the address of rule 2, and one is deny and one is permit; according to the filtering principle of ACL, different orders have different results. If you want to achieve the above requirements, the order of the two rules above must be: Rule 1 is in front, rule 2 is behind. The switch automatically implements the above sorting function, regardless of the order in which the user configures the above rules, and the final order is the rule 1, which is in front of rule 2. When a source address is the 192.168.1.1 address of the packet forwarding up, first compare the first rule, then compare second rules, two rules are matched, in front of the force (forward); if the source address is 192.168.0.1, only the first match, then discarded (not forwarding)。

If no sorting is done, the user may configure rule 2 first, then configure rule 1, rule 1 behind, rule 2 in front。

access-list 1 deny 192.168.0.0 0.0.255.255－Rule 2

access-list 1 permit 192.168.1.0 0.0.0.255－Rule 1

Because rule 2 contains the following rule 1, which may lead to the fact that the packets that match rule 1 completely match rule 2, rule 2 will be effective every time, and cannot meet the application requirements。

In the switch, '0.0.255.255' is wildcard bits, bits' '1' means no matching, bits' '0' means to match. It can be seen wildcard bits rule 2 for '0.0.255.255', need to match two bytes (16 bits); wildcard bits in rule 1 as the '0 0.0.255', need to match three bytes (24 bits); so rule 2 of the rules' "bigger, so after the row in the face. In extended IP, sorting needs to consider more rule fields, such as IP protocol type, communication port and so on. Their ordering rules are the same, that is, the more the configuration limit, the smaller the scope of the rule, and the larger the scope. The ordering of the rules is implemented in the background, and the user commands can only be displayed in the order of user configuration。

The filter fields supported by ACL include source IP, destination IP, IP protocol type (such as: TCP, UDP, OSPF), source port (such as 161), destination port. Users can configure different rules to access control according to different needs。

In a switch, a set of rules can be used by multiple applications; for example, a set of rules are filtered by port access and service access filtering, and referenced by or accessed by ports of the two ports。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.2 ACL filtering introduction

ACL filtering is carried out at the input port of the switch, and the port is filtered by the rule matching of the data stream entering the port. The ACL filter is handled by the line speed of the switch, and does not affect the forwarding efficiency of the data stream。

When a port of a switch does not configure ACL filtering, all data flow through the port will not match the rules, and can be forwarded through the port. When a switch port configuration of the ACL filter, all the input data through the port flow rule matching, the matching rules of action if it is permit, the data flow allows the forwarding, if it is deny, the data stream is not allowed to discard forwarding.。

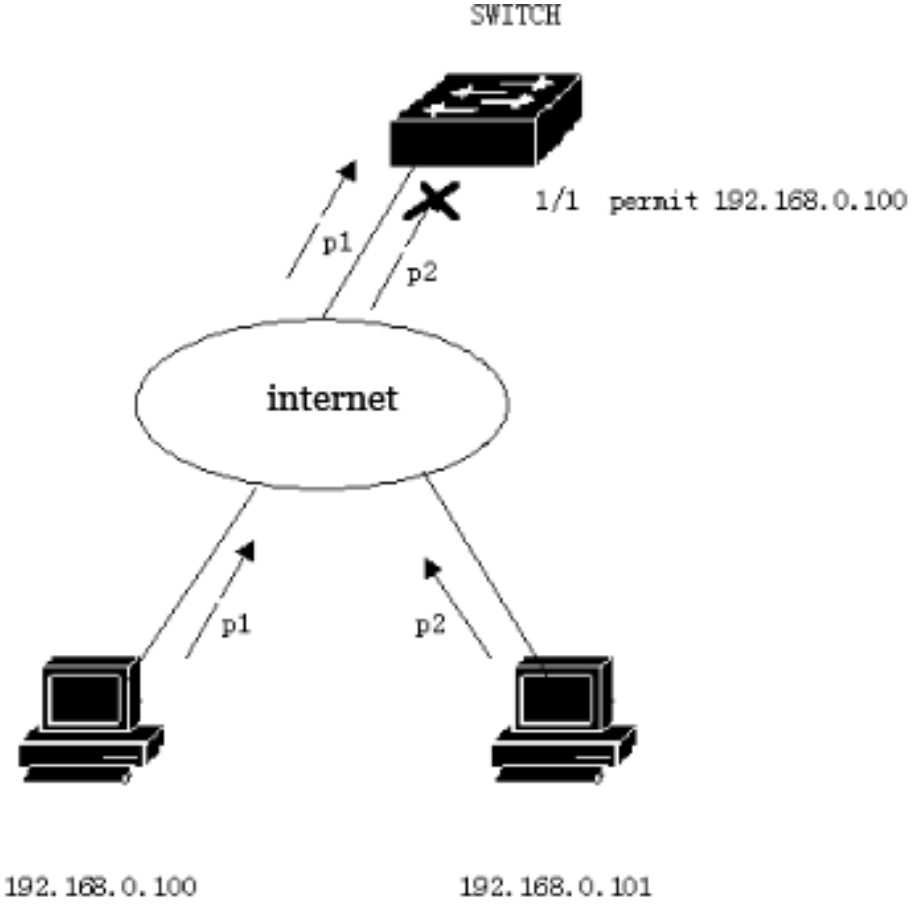
In the ACL filter configuration port, a port can select multiple ACL rules CFP group, the group rules into port selection, if not to deny or allow all the IP protocol. The rules set of rules in writing, CFP will add a rejection of all the rules of the IP agreement. When the rules of the ACL repository change, the rules written into the CFP automatically change。

For example, there is only one rule in a set of rules: access-list 1 permit 192.168.1.0 0.0.0.255, which defaults to a rule that rejects all IP protocol packets, and actually there are two rules imported into the port's CFP. When data flows through filters, only data flows from 192.168.1.0 to 192.168.1.255 can be forwarded through this port, and all other data streams are filtered out。

For example, there are two rules in a set of rules: access-list 1, deny 192.168.1.0 0.0.0.255, and access-list 1 permit any. At this point there is a rule that allows all IP protocol packages, and there are no hidden rules, and actually there are two rules imported into the port's CFP. When data flows through filters, only data streams with source addresses from 192.168.1.0 to 192.168.1.255 are filtered out, and all other data streams can be forwarded。

As shown below, an example of ACL filtering is given. The port 1/1 of the switch selects a ACL rule group 1. There is only one rule access-list 1 permit 192.168.0.100 in this set of rules. In the switch port 1/1, there are two users want to access the network from this port, the user's 1 IP address is 192.168.0.100, the user's 2 IP address is 192.168.0.101. Only the user 1 can access the network through the port 1/1 of the switch, and the user 2 can not access the network through the port 1/1 of the switch. The data stream P1 sent by the user can be forwarded through the port 1/1 of the switch, while the data stream P2 sent by the user 1 is discarded at the port 1/1 of the switch. 2。

SEC.RU | Короткий путь к информации
Скачано с sec.ru



When multiple ports are used for ACL filtering, the same ACL rule group can be used, and the same filtering rules are used。

Whether a set of rules or multi group rules are referenced by a port, they are automatically sorted, even if the order between the two sets of rules is crossed。

When a user refers to a set of rules, if the rules change, then the ports that refer to this set of rules will automatically respond to the user's configuration; there is no need to reconfigure the reference of this port。

17.3 ACL repository configuration

The switch defaults without any rules。

The resource library in the switch supports four types of ACL rules: Standard IP rules, extended IP rules, IP MAC groups, and ARP groups. Here are four rules to introduce the configuration of ACL。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Standard IP rule: the standard IP rule is to control the forwarding of data packets through the source IP address。

Command form：access-list <groupId> {deny | permit} <source>

Parameter description：

groupId：The access control list number, standard IP ACL support from 1 to 99 or 1300 to 1999。

deny/permit：If the match is complete, the packet is rejected or allowed to be forwarded。

source：Source IP has three input modes：

1)A.B.C.D wildcard You can control the IP address from a network segment；

2)any Amount to A.B.C.D 255.255.255.255

3)host A.B.C.D Amount to A.B.C.D 0.0.0.0

wildcard：Determine which bits needs to match, '0' indicates the need for matching, and '1' indicates no need for matching。

Extended IP rule: extending the IP rule is an extension of the standard IP rule. The packet forwarding can be controlled by source IP, destination IP, IP protocol type and service port。

Command form：access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Parameter description：

groupId：The access control list number, the extended IP ACL support from 100 to 199 or 2000 to 2699。

deny/permit：If the match is complete, the packet is rejected or allowed to be forwarded。

protocol：The protocol types over the IP layer, such as TCP, UDP, and so on, can also input the corresponding number 6 (TCP). If you don't need to control these protocols, you can enter IP or 0。

source：Source IP has three input modes：

1)A.B.C.D wildcard You can control the IP address from a network segment；

2)any Amount to A.B.C.D 255.255.255.255

3)host A.B.C.D Amount to A.B.C.D 0.0.0.0

srcPort：For the case of protocol TCP or UDP, you can control the source port of the packet, the input mode can be some familiar port service name, such as: www can also be digital, such as 80。

destination：Objective IP has three input modes：

1) A.B.C.D wildcard You can control the IP address from a network segment；

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2) any Amount to A.B.C.D 255.255.255.255

3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

destPort：For the case that protocol is TCP or UDP, the destination port of the packet can be controlled, and the input mode is the same as that of srcPort。

tcp-flag：For the case that protocol is tcp. The TCP field matching of data packets can be controlled, and the optional parameters are ACK, fin, PSH, RST, syn, urg。

IP MAC rule：The IP MAC group can control the source destination MAC address and the source destination IP address of the IP packet。

Command form：access-list <groupid> {deny | permit} <src-mac> vid <vlan-id|any> ip <src-ip> <dst-ip>

Parameter description：

groupId：The access control list number, the extended IP ACL support group from 700 to 799。

deny/permit：If the match is complete, the packet is rejected or allowed to be forwarded。

src-mac：source mac address。

The MAC address has three input modes：

1)HHHH.HHHH.HHHH wildcard You can control the MAC address from a segment；

2)any Amount to HHHH.HHHH.HHHH FFFF.FFFF.FFFF.

3)host A.B.C.D Amount to HHHH.HHHH.HHHH 0000.0000.0000

Vid：The outer vid can be either a vlan-id, or any any vlan-id

src-ip：Source IP address。

dst-ip：Destination IP address。

The IP address has three input modes：

1) A.B.C.D wildcard You can control the IP address from a network segment；

2) any Amount to A.B.C.D 255.255.255.255

3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

ARP rule：The ARP group can control the type of operation of the ARP packet, the sender MAC and the sender IP。

Command form：access-list <groupid> {deny | permit} arp <sender-mac> <sender-ip>

Parameter description：

groupId：The access control list number, the extended IP ACL support group from 1100 to 1199。

deny/permit：If the match is complete, the packet is rejected or allowed to be forwarded。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

sender-mac：The MAC address of the sender of the ARP packet。

The MAC address has three input modes：

1)HHHH.HHHH.HHHH wildcard You can control the MAC address from a segment；

2)any Amount to HHHH.HHHH.HHHH FFFF.FFFF.FFFF

3)host A.B.C.D Amount to HHHH.HHHH.HHHH 0000.0000.0000

sender-ip：Sender IP address of ARP packet。

The IP address has three input modes：

1) A.B.C.D wildcard You can control the IP address from a network segment；

2) any Amount to A.B.C.D 255.255.255.255

3) host A.B.C.D Amount to A.B.C.D 0.0.0.0

Other commands list：

show access-list [groupId]

Displays a list of rules configured in the current ACL. If groupId is entered, the list of rules for the current group is shown; otherwise, all the list of rules are displayed。

no access-list <groupId>

Deletes the specified rule list. All rules of group groupId。

17.4 ACL based on time interval

The time section is used to describe a particular time range. Users may have the needs: some ACL rules need to be effective within a certain period of time, and they do not use packet filtering in other time periods, which is usually referred to as filtering in the time period. At this time, the user can first configure one or more time, then time name refers to the time period in the corresponding rule, this rule is effective only in the time period specified, so as to realize the ACL filter based on time。

If the time rule references is not configured, the system gives a message, and allow such rules to create success, but the rule will not take effect until the time reference user configuration, and the system time in the specified period of time within the scope of the ACL rules to take effect。

There are two situations for configuring the time section：

(1) Configure the relative time section: use one day at a time to a certain point in the form of a point；

(2) Configuration of absolute time: the use of a year, a month, a day, a part of a year, a month, a day, a part of the form。

Configuring ACL based on the time period：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Assign a relative time segment that contains time only to the time section	Global configuration mode
time-range WORD cycle-time days from <0-6> to <0-6>	Configure a relative period of time only for weeks	Global configuration mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	Configure a time interval between time and week	Global configuration mode
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	Assign an absolute time period to the date section	Global configuration mode
no time-range WORD cycle-time	Delete all the relative time periods of a certain time period	Global configuration mode
no time-range WORD utter-time	Delete all absolute time periods of a certain time period	Global configuration mode
no time-range WORD	Delete a period of time (including deleting all the relative time and absolute time periods)	Global configuration mode
no time-range	Delete all the time periods	Global configuration mode
show time-range WORD cycle-time	Displays all the relative time periods of a given period of time	Privileged mode
show time-range WORD utter-time	Displays all absolute time periods of a certain time period	Privileged mode
show time-range WORD	Display a certain period of time (including all absolute and absolute time periods)	Privileged mode
show time-range	Show all the time periods	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range WORD	The so and so ACL rule applies a certain period of time and plays a role when ACL is applied to the interface	Global configuration mode
no acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range (WORD|)	Cancel a certain ACL rule and apply a certain period of time or all time periods	Global configuration mode
show acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range	Displays all the time periods of the application of a certain ACL rule	Privileged mode
show all acl time-range	Displays the time periods for all ACL rules to be applied	Privileged mode

It's important to note that：

(1) The time interval is configured with a number of relative time periods, the relationship between the relative time interval, the system time in any relative period of time, the time period is activated；

(2) There are several absolute time periods for a certain time period, and the absolute time period is the relationship. The system time is in any absolute time period, and the time period is in the active state；

(3) If to a certain time while the configuration of the relative time and absolute time, relative time and absolute time and system time relationship, at the same time only in the relative time and absolute time, the time period is active；

(4) Define up to 256 time periods; a maximum period of time can be configured 256 relative time and absolute time; a ACL rule can be used up to 256 time periods; in the period of ACL association rules applied to the interface when the time comes into play。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

17.5 ACL filter configuration

The switch defaults all ports do not do ACL filtering。

Command list：

access-group <groupId>

Mode: two layer interface configuration mode

parameter：

groupId：The binding of ACL and port number

Function: configure ACL port filter。

Note: if the above command configuration fails or fails, there may be the following reason：

Too many rules in the ACL group or the hardware resources are exhausted or occupied by other applications。

Display ACL port filter configuration

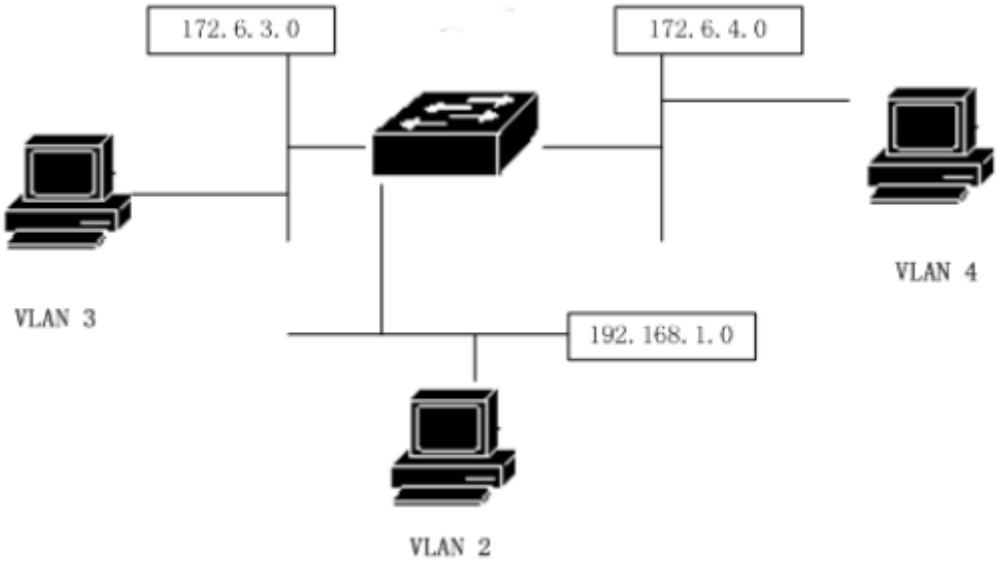
show acccess-group

Removes the current port and ACL port filter configuration

no acl- group <groupId>

17.6 ACL configuration example

A switch connects three subnets, designing ACL, blocking the source address as the 192.168.1.0 network address. The communication flow that allows other network addresses to pass. The 192.168.1.0 segment connects to the 1/1 port of switch。



The switches are configured as follows：

Switch#config t

SEC.RU | Короткий путь к информации
Скачано с sec.ru

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10
```

Note: according to the specific needs of the configuration of the time period, the time section associated with ACL rules, refer to the configuration as follows：

```
Switch(config)#time-range test cycle-time from 8 30 to 17 30 days from 1 to 5
Switch(config)#acl 1 time-range test
Switch(config)#interface ge1/20
Switch(config-ge1/2)#access-group 1
```

17.7 ACL configuration debugging

If the ACL configuration fails, there may be the following reasons：

1、Before configuring the access control list, make sure that all IP are connected, and then add access control lists. This access control list blocks the IP data stream whose source address is 192.168.1.0 segment through the switch. Note the subnet complement method. Use the show access-list command to list access control lists for viewing, and be sure to pay attention to the source address and destination address. Don't write back. Then view the access control list. And the default access control list finally has an implicit deny any statement, if you want to let the other through, you need to add a

SEC.RU | Короткий путь к информации
Скачано с sec.ru

permit any statement, otherwise it can not pass。

2、The system is configured with a static IP MAC binding。

3、The current interface enables the DHCP SNOOPING protocol。

4、System CFP resource exhaustion。

Eighteenth chapters
TCP/IP basic configuration

For a two layer switch with network management function, it is necessary to provide the basic network configuration for TCP/IP protocol and realize the communication function with other devices。

The main contents of this chapter are as follows：

- Configuring the VLAN interface
- Configuring ARP
- Configuring static routing
- TCP/IP basic configuration example

18.1 Configuring the VLAN interface

In the switch, each three layer interface is attached to a certain VLAN, so the three layer interface is also called VLAN interface. The creation and deletion of the VLAN interface is accomplished manually. switches can be divided into 4094 VLAN at most, but at most 32 subnets can be built. The creation of subnet interface can be created according to the needs of users; the subnet interface can be deleted manually by users, and can be deleted with the deletion of the VLAN in which the subnet is located。

Each VLAN interface has a name. The name of the VLAN interface is the string "VLAN", followed by the VLAN ID number, such as the name of the three layer interface of VLAN 1 is "vlan1", and the name of the three layer interface of VLAN 4094 is "vlan4094"。

Like ports, the VLAN interface also has management status and link state. At present, the switch does not provide the configuration of the management state of the VLAN interface. As long as the VLAN interface is established, the management state of the VLAN interface is always UP. Link state VLAN interface is corresponding to the interface of the VLAN contained in the port, as long as the link state of a port in VLAN is RUNNING, then the link state of the VLAN

SEC.RU | Короткий путь к информации
Скачано с sec.ru

interface is RUNNING, if VLAN in all ports are not RUNNING, then the link state of the VLAN interface is not RUNNING。

On the VLAN interface, you can configure the IP address and indicate the network prefix of the network segment connected to the interface (converted to network mask). Currently, switches only support one IP address on one VLAN interface. Before configuring the IP address, users need to create the VLAN first and add the related ports to the VLAN. By default, the switch has the interface of VLAN1, and the IP address 192.168.0.1/24 is set on this interface, and the user can also modify the IP address of the VLAN1 interface. The VLAN interface other than VLAN1 defaults not to set the IP address。

The commands for configuring the IP address of the VLAN interface are as follows：

command	describe	CLI mode
Ip interface vlan <2-4094>	Create a VLAN interface	Global configuration mode
No Ip interface vlan <2-4094>	Deleting a VLAN interface	Global configuration mode
ip address <ip-prefix>	Set the IP address on the VLAN interface. Parameters include the IP address of the interface and the network prefix of the connected segment. If the VLAN interface originally exists the IP address, first delete the original IP address, and then set the specified IP address. The format of the parameter is A.B.C.D/M。	Interface configuration mode
no ip address [ip-prefix]	Deleting the IP address of the VLAN interface. If the parameter is specified, the parameter must be the same as the parameter given at the time of the setting, otherwise the command is invalid. The format of the parameter is A.B.C.D/M。	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

See the command of the VLAN interface as follows：

command	describe	CLI mode
show interface [if-name]	View the information of the VLAN interface, including the IP address, MAC address, management state, link state, etc. of the interface. The parameter is the interface name of the VLAN interface. If no parameters are specified, all ports and VLAN interfaces are checked。	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the VLAN interface。	privileged mode

Example：

The subnet 193.1.1.0 is configured on the VLAN3 interface, the subnet prefix is 24 (that is, mask 255.255.255.0), the IP address of the interface is 193.1.1.1, and the information of the VLAN3 interface is looked at. The following commands：

switch(config)#interface vlan3

switch(config-vlan3)#ip address 193.1.1.1/24

switch(config-vlan3)#end

switch#show interface vlan3

18.2 Configuring ARP

ARP (Address Resolution Protocol) protocol is a mapping protocol for the IP address to the corresponding MAC address. When the source end of the Ethernet data frame to send in the same VLAN in the end, is to determine the destination according to the 48 bit Ethernet MAC address, destination packet according to the destination MAC address to determine whether to receive the packet。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Suppose that the two adjacent segment of the host A and B communicate through the switch, the host A to host B before sending data to the first and the host A directly connected to the switch interface to send the ARP request message, get the ARP response to send data packets to the interface. After receiving the data packet, the switch first broadcasts a ARP request message to the host B, then receives the ARP response message from the host B, and then sends the data packet to the host B。

There is a ARP cache on the switch, called the ARP table, which stores the mapping records of the IP address to the MAC address in the directly connected network. Each item in the ARP table has a lifetime. The default is 20 minutes. When the switch does not receive the ARP request or reply message of the IP address during the lifetime, the ARP table corresponding to the IP address will be deleted。

This section includes the following contents：

- Configuring static ARP
- Configuring ARP bindings
- Configuring ARP aging time
- View ARP information

18.2.1 Configuring static ARP

There are two different ARP table entries in ARP table, one is static ARP, and the other is dynamic ARP. Static ARP is the ARP table item configured by the user, the system will not automatically refresh and delete, need the user to manually complete. Dynamic ARP is the system automatically learning ARP according to the received ARP request or response package. The system automatically creates and deletes, updates and maintains in real time, without user intervention, but the user can manually delete the dynamic ARP items。

The switch does not configure a static ARP table item by default. It is important to note that when a VLAN interface is deleted or the subnet segment IP of the interface changes, the static and dynamic ARP table entries in the original subnet segment are deleted。

Configure the static ARP command as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
arp <ip-address> <mac-address> [if-name]	Configuring static ARP table entries. The first parameter is the IP address, and the IP address must be within a subnet segment. The second parameter is the MAC address, the MAC address must be unicast MAC address, and the MAC address format is HHHH.HHHH.HHHH, such as 0010.5cb1.7825. The third parameter is the two - level interface name, optionally, which indicates that the static ARP table entry is associated with a specific two - layer interface。	Global configuration mode
no arp {<ip-address> | <ip-prefix> | all | dynamic | static }	Delete ARP table entries. It includes deleting a ARP table item of IP, deleting a ARP table item of a network segment, deleting all ARP table items, deleting all dynamic ARP table items, deleting all static ARP items。	Global configuration mode
arp static {<ip-prefix> | all}	Modify all or all of the dynamic ARP items in a network segment to a static ARP table item。	Global configuration mode
arp aging <time>	Configuring ARP aging time only takes effect on dynamic learning ARP	Global configuration mode

18.2.2 View ARP information

The commands for viewing ARP information are listed below：

command	describe	CLI mode
show arp [<ip-prefix> | dynamic | static]	Look at the ARP table item information in the ARP table, including all the ARP table entries, the ARP table entries	Normal mode, privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	of a segment, the dynamic ARP table entries and the static ARP table entries。	
show running-config	Viewing the current configuration of the system, you can see the configuration of ARP。	privileged mode

18.3 Configuring static routing

A static route is defined by the user, and a routing that can send packets from the source address to the destination address through the specified path. By configuring a static route as the default route, the packets that cannot be routed are sent to the default gateway。

Static routing is manually configured by administrators. It is suitable for the network with simpler network structure. The administrator can configure the static route to make the switch work normally. Static routing does not take advantage of network bandwidth because it does not have routing updates。

Default routing is also a static route. In brief, the default route is the route that is used only when no matching routing item is found. That is, the default route is used only when there is no proper routing. In the routing table, the default route appears in the form of network 0.0.0.0/0 (mask 0.0.0.0). If the destination of the message is not in the routing table and there is no default route in the routing table, the message will be discarded and a ICMP message from the source will be returned to indicate the destination address or unreachable information of the network. Default routing is very useful in the network. In a typical network consists of hundreds of switches, running dynamic routing protocols may consume more bandwidth resources, using the default routing can save time and packet occupied by routing forwarding bandwidth resources, so you can meet a large number of users in a certain extent and communication needs。

A switch can configure multiple static routes to the same destination, but only one of the routes is activated for actual data forwarding. The switch does not configure static routing by default。

Configure the static routing command as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
ip route <ip-prefix> <nexthop-address>	Set static routing. The first parameter specifies the length of the network segment IP and the network prefix, and the second parameter specifies the next hop IP address。	Global configuration mode
ip route <ip-address> <mask-address> <nexthop-address>	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address。	Global configuration mode
no ip route <ip-prefix> [nexthop-address]	Delete static routing. The first parameter specifies the length of the network segment IP and the network prefix, and the second parameter specifies the next hop IP address. If there are no second parameters, delete all the routes that match the specified segment. If you have second parameters, delete the routing that matches the specified segment and the next hop。	Global configuration mode
no ip route <ip-address> <mask-address> [nexthop-address]	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address. If there are no third parameters, delete all the routes that match the specified segment. If you have third parameters, delete the routing that matches the specified segment and the next hop。	Global configuration mode

See the routing command as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
show ip route [<ip-address> | <ip-prefix>	View the active routing information, you can choose to see all the routing, a route, a network segment of the routing, static routing。	Normal mode, privileged mode
show ip route database	View all the routing information (including active and inactive routes), and you can choose to view all the routes。	Normal mode, privileged mode
show running-config	Viewing the current configuration of the system, you can see the configuration of the static route。	privileged mode

Example：

The destination network is 200.1.1.0, subnet mask is 255.255.255.0, and the next hop is 10.1.1.2. Configure command as：

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2

or Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Delete the destination IP address is 200.1.1.0, subnet mask is 255.255.255.0, the next hop is 10.1.1.2 static routing. Configure command as：

Switch(config)#no ip route 200.1.1.0/24

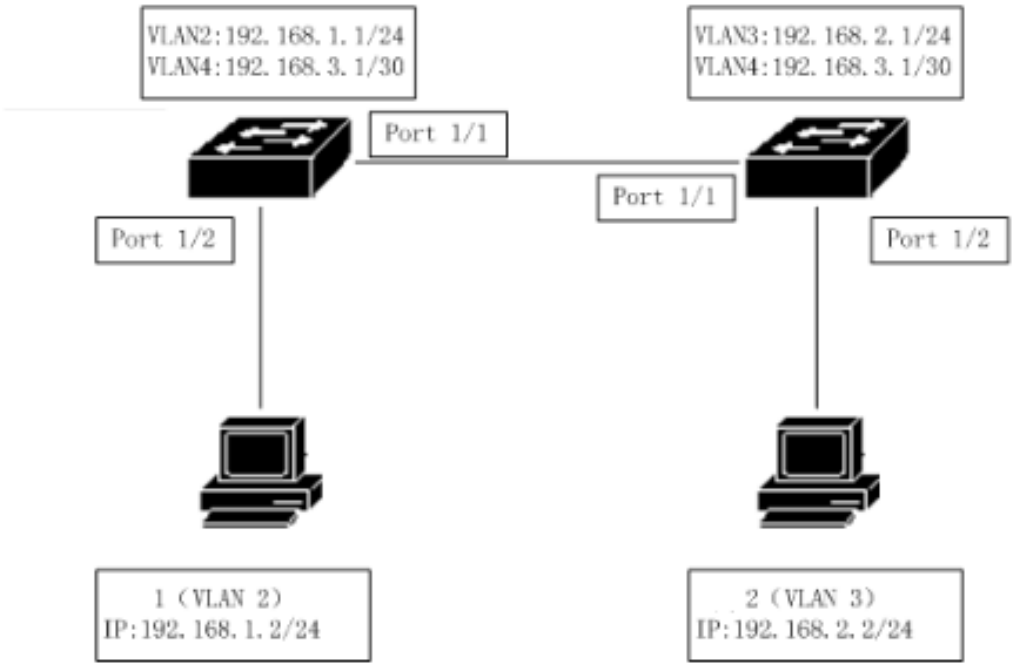
or Switch(config)#no ip route 2001.1.0/24 10.1.1.2

or Switch(config)#no ip route 200.1.1.0 255.255.255.0

or Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.4 TCP/IP basic configuration example



In the diagram, the switch 1 is a two layer switch, and the switch 2 is a three layer switch。

18.4.1 Three layer interface

On the switch 1, configure the corresponding three layer interface of VLAN2, and assign a IP address 192.168.1.1/24。

Configuration is as follows：

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switch access vlan 2

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip add 192.168.1.1/24

Verification: the user 1 is able to access the three layer interface IP address of the VLAN2 corresponding to the Ping switch 1。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

18.4.2 Static routing

The user 2 must access the switch 1 and must access the switch 1 through the routing function of the switch 2。

Switch 1 is configured as follows：

Switch#config t

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

Switch 2 is configured as follows：

Switch#config t

Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Verification: User 2 can ping general switch 1。

18.4.3 ARP

Configure 1 of the user's static ARP, allowing only 1 of users to access from VLAN2. Suppose the user's MAC address is 1 00:00:00:00:00:01。

Switch 1 is configured as follows：

Switch#config t

Switch(config)#arp 192.168.1.2 0000.0000.0001

Verification: the user 1 is able to access the three layer interface IP address of the VLAN2 corresponding to the Ping switch 1。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Nineteenth chapters
SNMP configuration

switches provide SNMP remote management of switches. This chapter describes how to configure SNMP, including the following：

The main contents of this chapter are as follows：

- SNMP introduce
- SNMP configuration
- SNMP configuration example

19.1 SNMP introduce

SNMP is a simple network management protocol, is the most widely used network management protocol, it has five major functions: fault management, billing management, configuration management, performance management, security management. It provides information format for communication between network management application software and network management agent (agent)。

SNMP network management protocol has four main elements: management workstation, management agent, management information base, network management protocol. The management agent is the server of the management workstation accessing the switch. The information of the management workstation accessing the network management agent is organized in the form of MIB, and the management information base is formed。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

SNMP has three big operations: GET operation, SET operation, TRAP operation. The GET operation enables the management workstation to obtain the value of the object in the proxy. The SET operation enables the management workstation to set the value of the object in the proxy. The TRAP operation enables the agent to notify the event of the management workstation。

The TRAP message is sent to the management workstation automatically when the event occurs. These messages include cold start, hot start, port link up, link down, shared name authentication failure, STP state switching, etc.。

At present, SNMP has three versions: SNMPV1, SNMPV2, SNMPV3, and the latter version is the upgraded version in the previous, the function has been enhanced, and the security has been improved. The switch supports all three SNMP versions and can parse three versions of the SNMP protocol package. When you send TRAP messages, you can use any version of SNMPV1, SNMPV2, and SNMPV3。

switches support RFC, BRIDGE, and private MIB objects, and can fully manage switches through SNMP. Some MIB:RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2575, RFC 2573, RFC 2574, are listed below ，

RFC 2674 and other common MIB.

Figure is an example of SNMP protocol interaction between management workstation and management agent. Management workstation can access switch management agent SNMP message sent by Get Request, GetNext Request, GetBulk Request and Set Request, gets or sets the exchange value of the MIB object, Get Response switch management agency send SNMP message to the management station. When there are some events on the switch, the management agent of the switch sends the SNMP TRAP message to the management workstation。

SNMP protocol interaction between management workstation and management agent

19.2 SNMP configuration

The SNMP configuration includes the community configuration of the switch, the configuration of the TRAP workstation, the information of the SNMP system, and the configuration of group engine, ID, user and snmpV3. The switch has a read-only shared default, and the share name is public. The switch can configure up to 8 shares。The switch does not configure TRAP workstations by default. The switch has a default local engine ID, and the switch can modify the local engine ID. The switch has a default user name:initialnone, which belongs to a non identified unencrypted user name. The switch can configure multiple different levels of user names. The switch has a default group name:initial, and switches can configure different group name according to different user names。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The commands of SNMP are as follows：

command	describe	CLI mode
snmp community <community-name> {ro | rw}	Configure the name of the shared object that accesses the network management, which is an interactive command. When configuring, the user can input the created name of the shared body and read / write permission according to the prompt。	Global configuration mode
no snmp community <community-name>	Deletes the specified SNMP share name。	Global configuration mode
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	Add or modify the sending target of SNMP trap. This is an interactive command. Notify name is unique, and if you modify the existing name, you can modify the trap to send the target item. Host is the destination address to send trap; version is sent in snmpV1, snmpV2c or snmpV3 mode. This command defaults to the target port of 162。	Global configuration mode
no snmp trap <notify-name>	Delete the specified SNMP trap。	Global configuration mode
snmp system information <contact | location | name> <information-string>	Configure system information, configurable system information include: contact, location and name。	Global configuration mode
no snmp system information <contact | location | name >	Delete a system configuration information。	Global configuration mode
snmp engine-id local <engine-id-octet-string>	Configure engine ID for version 3 of SNMP. The ID is a 24 bit sixteen decimal number; when the input is less than 24 bits, it is automatically padded with 0。	Global configuration mode
snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]	The SNMP user command is to set a user name corresponding to the local engine ID of the snmpv3. And the group name corresponding to the user name. If the user name supports authentication, the authentication protocol (MD5 or Sha) and the	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	corresponding identification password need to be set。	
no snmp user <user-name> <group-name> v3	Delete a user name corresponding to the local engine ID of SNMPv3。	Global configuration mode
snmp group <group-name> v3 {auth | noauth} [notify <notify view name> | write <write view name> | read <read view name>]	The SNMP group command is a set of group names that the security level is (auth or noauth), and the notification, writable, or readable view specified by the security model (V3)。	Global configuration mode
no snmp group <group-name> v3 {auth | noauth}	Delete a group name, the security level is (auth or noauth), the security model (V3) specified view。	Global configuration mode
show snmp community	Show all the current public name and the corresponding read and write permissions information。	Normal mode, privileged mode
show snmp trap	Display all the trap names and the corresponding trap sent target IP address and version information。	Normal mode, privileged mode
show snmp system information	Display system information set by SNMP	Normal mode, privileged mode
show snmp engine-id	Display SNMPV3 local engine-id。	Normal mode, privileged mode
show snmp user [specify name of user]	Displays a user name information corresponding to the local engine ID of snmpv3. Include the group name corresponding to the user name and the authentication and encryption information supported by the user name。	Normal mode, privileged mode
show snmp group	Displays all group names, security levels (auth or noauth), notification specified by the security model (V3), writable or readable view information。	Normal mode, privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

19.3 SNMP configuration example

Configure the name of a shared name called private. The read and write permissions are read and write。

Configure a SNMP trap called test and send the destination IP to 192.168.0.10; use the SNMP version of 1。

The specific content of the configuration system is contact：E-mail:networks@lenovo.com。

The specific content of the configuration system is location：ShennanRoad,Shenzhen,China。

Set a user name initialmd5 that supports MD5 authentication, the group name is initia, and the authentication password is 047b473f93211a17813ce5fff290066b。

Set the group name initial, the security level is (auth), the notification specified by the security model (V3), writable or readable view names are Internet, Internet, Internet。

The configuration of the switch is as follows：

Switch#config t

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail:networks@lenovo.com

Switch(config)#snmp system information location ShennanRoad,Shenzhen,China

Switch(config)# snmp user initialmd5 initial v3 auth md5 17813ce5fff290066b

Switch(config)# snmp group initial v3 auth read internet write internet notify internet

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Twentieth chapters

RMON configuration

The main contents of this chapter are as follows：

- RMON introduce
- RMON configuration
- RMON configuration example

20.1 RMON introduce

RMON (Remote Monitoring) is a standard monitoring specification. It is mainly used to monitor data flow in a network segment and even in the whole network. It is one of the widely used network management standards. The RMON specification is extended by SNMP MIB, so it is also a MIB, which is the most important enhancement of the MIB II standard. RMON makes SNMP more effective and proactive in monitoring remote devices。

RMON monitoring system consists of two parts: detector (proxy or monitor) and management station. RMON agents store network information in RMON MIB, which are directly implanted into network devices (such as routers, switches, etc.). Management station uses SNMP to obtain RMON data information。

This device supports the 4 most commonly used groups in RMON：

(1) Statistical group (Statistics): provide statistical data for each interface, where most of the objects are counters, recording the information collected by the monitor from the interface。

(2) Historical group (History): data stored at a fixed time interval to a specified interface。

(3) Alarm group (alarm): sampling the specified data of all interfaces at a fixed time interval, comparing with the set threshold, and triggering the corresponding event when the condition is satisfied。

(4) Event group (event): setting events, you can choose to log records or send Trap。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

20.2 RMON configuration

The RMON command consists of 4 groups of configurations to view configuration and view data：

command	describe	CLI mode
rmon statistics <1-100> (owner WORD|)	A group configuration that specifies the specified number of ports for this port. This is an interactive command. The configuration is that the user can enter the number and owner according to the prompt, and the owner is optional. The serial number is the configuration number of the statistical group, and the value ranges from 1 to 100。	Port configuration mode
no rmon statistics <1-100>	Statistical group configuration to cancel specified number。	Port configuration mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	The historical group parameter that specifies the ordinal number for this port, which is an interactive command. The configuration user can enter the serial number, the number of requesting buckets, the time interval and the owner according to the prompt. The serial number is the number of the historical group configuration, the value range is from 1 to 100; the number of bucket requests is the maximum number of the saved data, the value range is 1 to 100; the sampling interval is in seconds, and the value range is from 1 to 3600。	Port configuration mode
no rmon history <1-100>	The history group configuration to cancel the specified number。	Port configuration mode
rmon alarm <1-60> WORD	Configuring an alarm group	Global

SEC.RU | Короткий путь к информации
Скачано с sec.ru

<1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	parameter with a specified ordinal number, which is an interactive command. Configuration user can input serial number, monitor object, time interval, contrast mode, upper limit value, upper limit event sequence number, lower limit value, lower limit time sequence number and owner. The serial number is the number of alarm configuration, the 1 to 60 range; the monitoring object is a MIB node OID, the sampling time interval in seconds, the 1 to 3600 range of contrast; you can select absolute or delta, said the absolute value (the value of each sample respectively) and relative value (increment relative to the last sampling sampling); range limit threshold is 1 to 2147483647; the event must advance configuration, 1 to 60 is the range of numbers。	configuration mode
no rmon alarm <1-60>	Alarm group configuration to cancel specified number。	Global configuration mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	Configuring the event group parameter of the specified ordinal number, which is an interactive command. The configuration user can enter the serial number, event type, shared name, description and owner according to the prompt. The serial number is event group configuration number, 1 to 60 range; event types can choose log (log), log-trap (log and a Trap) and none (no action) and trap (a Trap), when the choice of log-trap or trap, you must also specify the name of	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	the equipment (in the common body the body name configuration is ignored)。	
no rmon event <1-60>	Event group configuration to cancel the specified number。	Global configuration mode
show rmon (statistics|history-control|alarm|event) config	View the RMON configuration information, which is an interactive command. Configuration users can input and view objects according to the prompts。	Global configuration mode
show rmon statistics-data interface IFNAME|	View the RMON statistics group data, configure the user to input the interface name。	Global configuration mode
show rmon history-data interface IFNAME|	View the RMON history group data, configure the user to enter the interface name。	Global configuration mode

20.3 RMON configuration example

Enable port group configuration for ge1/1, the ordinal number is 10, and the owner is tereco。

Enable the port ge1/8 history group data acquisition, the serial number is 2, the maximum preservation of 80 data, sampling interval is 1 minutes, no owner。

Configure events with a serial number of 1, log log, no owner。

Configure an event with a number of 3, send Trap, share the name of public, no owner。

An alarm group with a serial number of 5 is used to monitor the number of bytes received per port. The Trap alarm is issued when the number of bytes per half is greater than 1000, and the log is less than 10. No owner。

The switch is configured as follows：

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#rmon statistics 10 owner tereco
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/8
Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60
Switch(config-ge1/8)#exit
```


SEC.RU | Короткий путь к информации
Скачано с sec.ru

Switch(config)#rmon event 1 log

Switch(config)#rmon event 3 trap public

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1

Twenty-first chapters

Cluster configuration

The switch provides a cluster management function that enables a single device to manage a set of network devices。This chapter describes how to configure cluster management, including the following：

- Introduction of cluster management
- Brief introduction of cluster configuration
- Configuration management equipment
- Configuration member device
- Configuring access cluster members
- Cluster management display and maintenance
- Example of cluster management typical configuration

21.1 Introduction of cluster management

21.1.1 Cluster definition

A cluster is a set of network devices that can be managed as a single device。

The purpose of cluster management: to solve the centralized management of a large number of scattered network devices。

Cluster advantages: save public network IP address; simplify configuration management task. Network managers only need to configure the public network IP address on a switch in the cluster,

SEC.RU | Короткий путь к информации
Скачано с sec.ru

so that the management and maintenance of other switches in the cluster can be realized。

Switches that configure public network IP addresses and perform management functions are command switches, and other managed switches are member switches, command switches and member switches that form a cluster"。

The cluster configures and manages the switches within the cluster by using the following three protocols。

- NDP（Neighbor Discovery Protocol）
- NTDP（Neighbor Topology Discovery Protocol）
- Cluster （Cluster Management Protocol）

The working process of the cluster and the cluster topology collection including the establishment and maintenance, and maintenance of the cluster topology collection process is relatively independent, topology collection process begins to start up in the cluster before the establishment of the working principle is as follows：

- All devices acquire the information of neighbor devices through NDP, including the software version, host name, MAC address and port name of neighbor devices。
- The management device collects the device information and the connection information of each device through the NTDP, and determines the cluster candidate devices from the collected topology information。
- The management device completes the operation of adding candidate devices to cluster and member devices leaving the cluster according to the candidate device information collected by NTDP。

The cluster message is two layer Ethernet message, the specific format and interactive process refer to the national standard "YDT 1692-2007 Ethernet switch cluster management technical requirements"

21.1.2 Cluster role

According to the position and function of the devices in the cluster, different roles are formed. The user can specify roles by configuration, and all the roles are as follows：

1）Command Switch：

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch in the cluster with the public network IP address。

- Command switches create clusters；
- Command switches discover and determine candidate switches by collecting information from NDP (Neighbor Discovery Protocol) and NTDP (Neighbor Topology Discovery Protocol)；

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Command switches control cluster maintenance by adding candidate switches to clusters or deleting member switches from clusters;
- After the cluster is established, the command switch provides a management channel for the cluster。

2）member switch

Managed switches in a cluster。

A member switch is a candidate switch before joining the cluster。

Member switch does not have public network IP;

The management of the member switch is completed by the command exchange agent。

3）Candidate switch

A switch that has the ability to join clusters, but has not yet joined any cluster。

The switch must first be a candidate switch, and then it can become a member switch。

4）Independent exchange

Switch without cluster function。

Various roles can be converted according to certain rules:

- When a user creates a cluster on a candidate device, the current candidate device is designated as a cluster management device. Each cluster must specify one (and only one) management device. After the management device is assigned, the management device discovers and identifies the candidate devices by collecting relevant information. The user can join the candidate device into the cluster through the appropriate configuration。
- When a candidate device joins a cluster, it becomes a member device。
- When a member device in the cluster is deleted, it will revert to a candidate device。
- Management devices can only be restored to candidate devices only when the cluster is removed。

21.1.3 NDP profile

NDP is used to obtain the information of directly connected neighbor equipment, including connection port, device name, software version and other information. The working principle is as follows:

- Run the NDP device periodically transmits the NDP message to the neighbors, including NDP information in the NDP message (name of equipment, including the current version of the software, equipment port and other information) and NDP information on the receiving device aging time. It also receives and does not forward the NDP message sent by neighbor devices。
- The NDP running device stores and maintains the NDP neighbor information table, and

SEC.RU | Короткий путь к информации
Скачано с sec.ru

creates a table item for each neighbor device in the NDP neighbor information table. If the new found a neighbor that is the first time it sends the received NDP message, NDP will be in the neighbor information table to add a table; if different from neighbors received NDP information and old information, update the NDP table in the corresponding data item, if the same, only updated if the aging time. Over ageing time has not received the neighbors send NDP information will automatically delete the corresponding neighbor table entry。

21.1.4 NTDP profile

NTDP is used to collect the information of each device and the connection information between devices in a certain network range. NTDP provides device information for management devices that can join the cluster and collects topological information of the devices within the specified hop count。

NDP provides adjacency list information for NTDP, NTDP sends and forwards NTDP topology collection request according to adjacency information, collects NDP information of each device in a certain network range and its connection information with all neighbors. After collecting the information, the management equipment or network management can use the information according to the need to complete the required functions. When a member device NDP neighbor discovery has changed, the handshake message will notify neighbor management equipment change, management of equipment can start NTDP for the specified topology collection, so that the NTDP can reflect the change of network topology。

The management device can periodically collect topology in the network, and the user can initiate a topology collection by manually configuring commands. Management equipment collects topological information process as follows：

- The management device sends the NTDP topology to collect the request packets from the ports that enable the NTDP function。
- Receive the request message immediately send response message to the topology of equipment management equipment, and has the function of NTDP in the port of a copy of the request message and sends it to the adjacent equipment; the response message contains the topological equipment basic information and all adjacent equipment information NDP。
- The neighbor device receives the request message and executes the same operation until the topology collects the request packets to all devices within the specified hop range。

When the topology collection request message diffusion within the network, a large number of network equipment also received the request and send topology topology collection response message, in order to avoid network congestion and task management device is busy, you can take the following measures to control the topology collection request message diffusion speed：

- After receiving the topology collection request, the device does not immediately forward

SEC.RU | Короткий путь к информации
Скачано с sec.ru

the topology collection request packet, but delays waiting for a certain time, and then begins to forward the topology collection request packet at the port enabling the NTDP function。

- On the same device, except for the first port, each port enabled the NTDP function to send the topology collection request message at the previous port, and then it will delay a certain period of time before forwarding the topology collection request packet。

21.1.5 Cluster management maintenance

1) Candidate devices join clusters

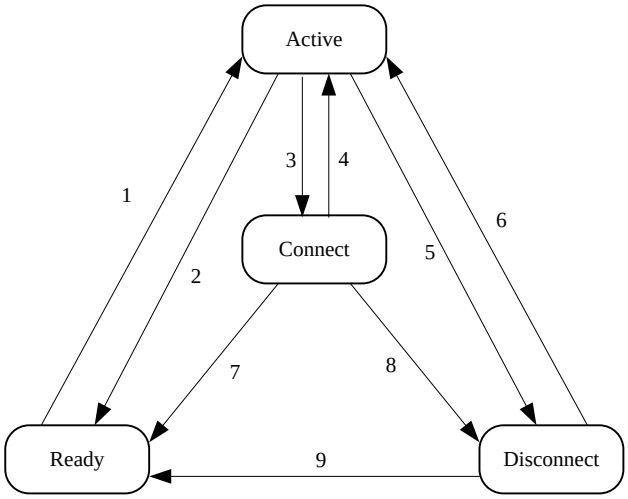
The user should first specify the management of equipment in the establishment of the cluster, management of equipment through the NDP and NTDP protocol to discover and identify the candidate equipment, the candidate equipment automatically join the cluster, can also manually configure the candidate device to join the cluster。

After the candidate device is successfully added into the cluster, the cluster member sequence number and cluster management of the management device allocated to it are obtained

Private IP addresses used, etc.。

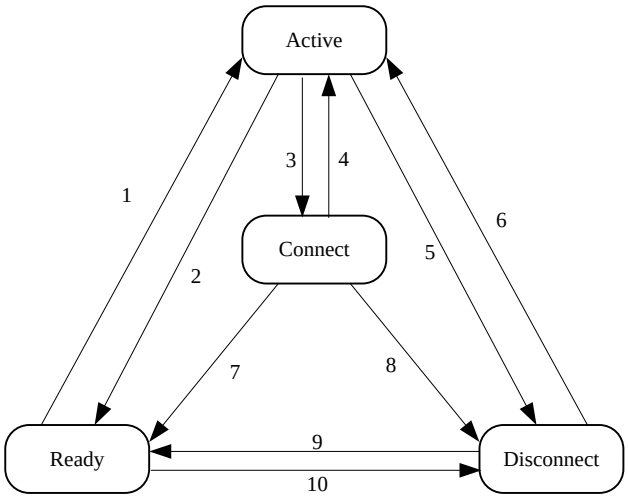
2) Trunking communication

In the cluster, the management device and the member device communicate with each other through handshake message to maintain the connection state between them, and manage the connection state of the equipment and member equipment as shown in the following picture。



State transition diagram of command switch

SEC.RU | Короткий путь к информации
Скачано с sec.ru



Member switch state transition graph

The command switch collects the basic information of the device, identifies a device as a candidate switch, and begins with the Ready state。

The deletion of member operations in any state migrates the state of the member switch back to the Ready state and identifies it as a candidate switch。

- The cluster is established successfully, the candidate to become a member of the equipment into the equipment cluster, management of equipment status information is saved to the local members of equipment, and the member state is identified as Active, a member of equipment will also be saved to the local state information itself, and its status is identified as Active。
- Management device and member device send handshake message regularly. After receiving the handshake message of the member equipment, the management equipment does not respond, keeps the member equipment as Active state, and the member equipment does not respond, and keeps the state of itself as Active。
- If the management of equipment to send handshake message member device at three times handshake message transmission time interval is not received within the handshake message sending members of equipment, will be saved in the local members of the state of the device by Active migration to Connect; similarly, if a member of equipment to management did not receive a handshake message sending management equipment three times handshake message transmission time interval by transmitting handshake message, its status will migrate from Active to Connect。
- If the management of equipment received in the Connect state member of the device to send in effective reservation time handshake message or message management, the member state of the device transfer back to Active, otherwise the migration is Disconnect, in which management equipment that the member is disconnected; in the Connect state member of the equipment if the retention time received the sending equipment management handshake message or message

SEC.RU | Короткий путь к информации
Скачано с sec.ru

management, its state will migrate to Active, otherwise it will migrate to Disconnect。

- When the restoration of communications equipment and management of equipment members interrupted when the device is in the Disconnect state members will rejoin the cluster join after the success of members in the management of equipment equipment and the local state will return to Active。

If topology changes are found, member devices also pass the change information to the management device through handshake messages。

21.1.6 Managing VLAN

Managing VLAN limits the scope of cluster management. By configuring VLAN, the following functions can be implemented：

- The management message of cluster (including NDP, NTDP message and handshake message) will be limited in the management of VLAN, isolated from other messages, which increases the security。
- Managing devices and member devices to implement internal communications by managing VLAN。

Cluster management requirements management equipment and members / candidate device port, including cascade port (when the candidate device is connected by another candidate equipment and management of equipment, equipment connected to each candidate between ports are called cascade port) allows management through VLAN, so：

- If the port does not allow VLAN to pass through, the device connected to the port cannot join the cluster, so the cluster should be connected with the management device before the cluster, including the cascade port, allowing the management of the VLAN to pass。
- Only when the management of equipment and equipment connected to the member / candidate port and port default VLAN ID cascade is the management of VLAN, the message will allow the configuration management of VLAN with no label through, otherwise the message management must be labeled by VLAN。

For VLAN, see Chapter sixth configuring VLAN"。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

21.2 Brief introduction of cluster configuration

Before the user configures the cluster, it is necessary to define the roles and functions of each device in the cluster, and configure the related functions to do the planning work for the communication with the internal equipment of the cluster。

Configuration task		Detailed configuration
Configuration management equipment	NDP function of enable system and port	15.3.1
	Configuring NDP parameters	15.3.2
	NTDP function of enable system and port	15.3.3
	Configuring NTDP parameters	15.3.4
	Configure manual collection of NTDP information	15.3.5
	Enable cluster function	15.3.6
	Build clusters	15.3.7
	Configuring internal member interactions in clusters	15.3.8
	Configuring cluster member management	15.3.9
Configuration member device	NDP function of enable system and port	15.4.1
	NTDP function of enable system and port	15.4.2
	Configure manual collection of NTDP information	15.4.3
	Enable cluster function	15.4.4
Configuring cluster members to access each other		15.5

note：

After the cluster is established, the cluster will not dissolve when the NDP or NTDP function is closed on the management device and member device, but it will affect the normal operation of the cluster that has been established。

21.3 Configuration management equipment

21.3.1 Enable system and port NDP capabilities

command	describe	CLI mode
ndp global enable	Enabling global NDP functionality. Global shutdown by default。	Configuration mode
ndp enable	The NDP function of enable ports. All ports are closed by default NDP	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

note：

- *The NDP function of both the global port and the port must be enabled, and the NDP can run normally。*
- *NDP function does not support aggregated ports。*
- *In order to avoid the topology information of the devices that are not required to join the cluster during topology collection and add it to the cluster, it is recommended that the NDP function be closed on the ports that do not need to join the cluster device。*

21.3.2 Configuring NDP parameters

command	describe	CLI mode
ndp aging-timer <aging-time>	Configure the aging time of the NDP message sent by the device on the receiving device. Default 180 seconds。	Configuration mode
ndp hello-timer <hello-time>	Configuring the time interval for NDP packets to be sent. Default 60 seconds。	Configuration mode

note

The aging time of NDP message on the receiving device can not be less than the NDP transmission time interval, otherwise it will cause the instability of the NDP port neighbor information table。

21.3.3 Enable system and interface NTDP capabilities

command	describe	CLI mode
ntdp global enable	Enabling global NTDP functionality. Global shutdown by default。	Configuration mode
ntdp enable	The NTDP function of enable ports. All ports are closed by default NDP	Interface configuration mode

note：

- *The NTDP function of both the global port and the port must be enabled, and the NTDP can run normally。*
- *NTDP function does not support aggregated ports。*

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- *In order to avoid the topology information of the devices that are not required to join the cluster during topology collection and add it to the cluster, it is recommended that the NTDP function be closed on the ports that do not need to join the cluster device。*

21.3.4 Configuring NTDP parameters

command	describe	CLI mode
ntdp hop <hop-value>	The range of configuration topology collection. By default, the maximum number of hops from the topology collection device is 3 in the topology collected。	Configuration mode
ntdp timer <interval-time>	Time interval for configuring timing topology collection. Default 1 minutes。	Configuration mode
ntdp timer hop-delay <time>	Configuring the collected device before the first port forwards the topology to collect the waiting time before the request message. Default 200 milliseconds。	Configuration mode
ntdp timer port-delay <time>	Configure port delay time for current device forwarding topology to collect requests. Default 20 milliseconds。	Configuration mode

21.3.5 Configure manual collection of NTDP information

After the cluster is established, the management equipment collects the topology information periodically. In addition, users can manually collect NTDP information manually (regardless of whether the cluster is established), and initiate a collection process of NTDP information, so as to effectively manage and monitor the equipment more effectively。

command	describe	CLI mode
ntdp explore	Topology information is collected manually。	Common mode, privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

21.3.6 Enable cluster function

command	describe	CLI mode
cluster enable	Enable cluster function. The default cluster function is closed。	Configuration mode

21.3.7 Build clusters

Managing VLAN limits the scope of cluster management. By configuring VLAN, the following functions can be implemented：

- The management message of cluster (including NDP, NTDP message and handshake message) will be limited in the management of VLAN, isolated from other messages, which increases the security。
- Managing devices and member devices to implement internal communications by managing VLAN。

command	describe	CLI mode
cluster management-vlan <vlan-id>	Designated management VLAN. The default management VLAN is VLAN1。	Configuration mode

note：
If the current device is in the cluster, it is not allowed to modify the management VLAN。
The situation is not in the cluster：

1） Check whether the VLAN exists, no direct failure exists, and move on to the next step
2） Re check all the interfaces, if the interface where VLAN and management VLAN is not the same VLAN, then open the global switch of NDP and ntdp are closed, and do the corresponding closed empty operation, and then re opened。
3） Find the three layer interface that you want to configure VLAN. If you don't find it, create a new three level interface to the VLAN. If the new build fails, you can manage VLAN configuration successfully, you can NDP and ntdp, but you can't join the cluster。
4） The MAC of the three layer interface is set to dev_id. If the VLAN is set up successfully and the new three layer interface fails, then the vlan1 of MAC is used as dev_id

If the configuration management of VLAN, but the user directly in the VLAN database to remove the VLAN, it will automatically manage the VLAN set to vlan1, NDP, ntdp and global switch will open and clusters are closed and the corresponding empty closed operation。

In the establishment of the cluster, the user must first set the members of equipment used in the cluster private IP address range, when the candidate device is added, the distribution of private IP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

address can be used in a cluster within the scope of the dynamic management of equipment, and given to the candidate for the communications equipment within the cluster, in order to achieve the management of equipment equipment management members and maintenance。

note :

command	describe	CLI mode
cluster ip-pool <IP/MASK>	Configure the private IP address range used by the member devices in the cluster on the device that you want to set up to manage the device。	Configuration mode

- The IP address and cluster address pool of the VLAN interface for managing device and member devices cannot be configured on the same network segment, otherwise the cluster will not work properly。
- Only when the device is not in the cluster can it be configured。
- Use management VLAN to find whether there is a corresponding three layer port, if there is no three layer, the direct return failure. (this device cannot be a cluster command exchange). If there are three levels of interface, the base address of the IP-POOL is configured to the three port, and if the configuration fails, IP-POOL is configured to fail。

By default, the device is not managed by the device, and the cluster is established：

command	describe	CLI mode
cluster build <name>	Manually build clusters, configure the current device to manage the device, and assign a cluster name。	Configuration mode
cluster auto-build <name>	Auto build cluster。 The automatic cluster function automatically adds all the candidate devices found within the specified hop count to the created cluster。	Configuration mode
cluster delete <name>	Delete cluster。	Configuration mode
cluster stop auto-add member	Automatically set up cluster configuration, stop automatically adding member switches. This operation can only stop	Configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	adding new devices, and the devices that have been added to the cluster will remain in the cluster。	

note：

- The user can only specify the management VLAN before the cluster is established. After the device has joined the cluster, the user can not modify the management VLAN. If you need to change the management VLAN after the cluster is established, you need to delete the cluster on the management device, reassign the management VLAN, and finally re build the cluster。
- For security reasons, it is recommended that management VLAN should not be configured to manage the connection ports between devices and member devices, and the default VLAN ID of cascading ports。
- Only when connected to the equipment and management of equipment and all members of the port cascade port default VLAN ID is the management of VLAN, the message can not allow management of the VLAN tag through, otherwise must be connected to configuration management equipment, equipment and all members of the port port cascade allowed VLAN management message with label through, please refer to "VLAN specific configuration"。
- The configuration of the private IP address range of the member devices in the cluster can only be configured when the cluster has not been established, and can only be configured on the management device. If the cluster has been established, the system does not allow to modify the IP address range。

21.3.8 Configure the cluster's internal members to interact

In the cluster, management equipment and equipment for real-time communication by members to maintain the handshake message, the connection state between them, we can effectively keep the time allocation handshake message sent in the management of equipment on time interval and equipment, the configuration will also effect on the cluster members of all equipment。

command	describe	CLI mode
cluster timer <interval-time>	Configuring the time interval for handshake packets to be sent. Default 10 seconds。	Configuration mode
cluster holdtime <hold-time>	Effective retention time of configuration device. Default 60 seconds	Configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

21.3.9 Configuring cluster member management

The user can manually specify the candidate devices to join in the cluster, or manually delete the specified member devices in the cluster. The join / delete operations of cluster members must be carried out on the management device, otherwise the error prompt message will be returned。

command	describe	CLI mode
cluster add member mac-address <mac-address>	Adding candidate devices to clusters。	Configuration mode
cluster delete member mac-address <mac-address>	Deleting member devices from a cluster。	Configuration mode

21.4 Configuration member device

21.4.1 Enable system and port NDP capabilities

See the 18.3.1 enabled system and port's NDP function

21.4.2 Enable system and port NTDP capabilities

See the 18.3.3 enabled system and port's NTDP function

21.4.3 Configure manual collection of NTDP information

See 18.3.5 configuration for manually collecting NTDP information

21.4.4 Enable cluster function

See 18.3.6 enable cluster functionality

21.5 Configuring access cluster members

After the NDP, NTDP and cluster functions are properly configured, the members of the cluster can be configured, managed and monitored by the management device. You can configure the member device configuration on the management device to switch to the specified member device operating interface。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
cluster switch-to member <member-number>	Switch from management device operation interface to member device operation interface。	Normal mode, privileged mode

The connection between cluster management equipment and member equipment is connected by Telnet, so it is necessary to pay attention to switch：

- *Before switching, the end device needs to execute the "telnet server enable" command to enable the telnet function, otherwise it will result in the handover failure。*
- *From the management device to the member device, if the member number n does not exist, an error message will be displayed. If the device Telnet user logged on is full, the handover failure will result。*

21.6 Cluster management display and maintenance

command	describe	CLI mode
show ndp[interface <ifname>]	Display NDP configuration information	Normal mode, privileged mode
reset ndp statistics [interface <ifname>]	Clear NDP statistics	Configuration view
show ntdp	Display system NTDP information	Normal mode, privileged mode
show ntdp device-list	Display device information collected by NTDP	Normal mode, privileged mode
show ntdp single-device mac-address <mac-address>	Displays the NTDP details of the specified device	Normal mode, privileged mode
show cluster	The status and statistical information of the cluster to which the device belongs	Normal mode, privileged mode
show cluster topology	Display cluster topology information	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Display candidate device information	Normal mode, privileged mode
show cluster members [<member-number>]	Display cluster member information。	Normal mode, privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

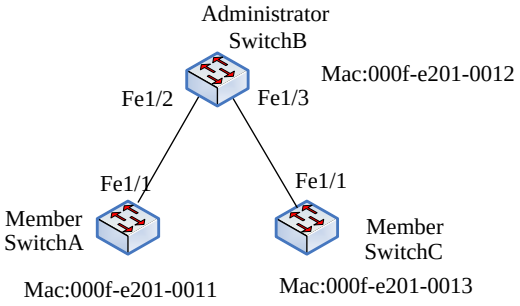
21.7 Example of cluster management typical configuration

1、Networking requirement：

The ABC consists of three switches, and the management VLAN is VLAN 10. Among them, Switch B is management equipment (Administrator); Switch A and Switch C are member devices (Member)。

The base address IP of the cluster address pool is 10.0.0.1, supporting 8 devices。

2、Network diagram：



3、Configuration steps：

Configuring member device SwitchA

Configuration management VLAN。

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch trunk vlan 10

Enabling global NDP functionality and NDP functionality on port ge1/1。

[SwitchA] ndp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enabling global NTDP functionality and NTDP functionality on port Ethernet1/0/1。

[SwitchA] ntdp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

Enable cluster function。

[SwitchA] cluster enable

Configuring member device SwitchC

Because the configuration of the member devices is the same, the configuration on Switch C is similar to that of Switch A, and the configuration process is slightly better。

Configuration management device SwitchB

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Configuration management VLAN。

[SwitchB] cluster management-vlan 10

[SwitchB] interface ge1/2

[SwitchB-ge1/2] switch trunk vlan 10

[SwitchB] interface ge1/3

[SwitchB-ge1/3] switch trunk vlan 10

Enabling global NDP and NTDP functions, and enabling ports ge1/2 and ge1/3 on the NDP, NTDP functions。

[SwitchB] ndp enable

[SwitchB] ntdp enable

[SwitchB] interface ge1/1

[SwitchB-ge1/2] ndp enable

[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3

[SwitchB-ge1/3] ndp enable

[SwitchB-ge1/3] ntdp enable

The aging time of the NDP message sent by the device is 200 seconds on the receiving device。

[SwitchB] ndp timer aging 200

The time interval for configuring the NDP message is 70 seconds。

[SwitchB] ndp timer hello 70

The maximum number of hops collected by the configuration topology is 2 hops。

[SwitchB] ntdp hop 2

Configuring the first port of the collected device to forward the topology, the delay time of collecting the request packets is 150ms。

[SwitchB] ntdp timer hop-delay 150

The delay time of collecting request packets of other ports forwarding topology is 15ms。

[SwitchB] ntdp timer port-delay 15

The configuration topology collects intervals of 3 minutes。

[SwitchB] ntdp timer 3

Enable cluster function。

[SwitchB] cluster enable

The private IP address of the configured member device ranges from 10.0.0.1 to 10.0.0.9。

[SwitchB] cluster ip-pool 10.0.0.1 8

Configure the current device to manage the device, and build a cluster called ABC,

SEC.RU | Короткий путь к информации
Скачано с sec.ru

members automatically join the cluster。

[SwitchB] cluster autobuild abc

When you add all the switches you want to add, you can turn off and automatically join the cluster function

[SwitchB]cluster stop auto-add member

Twenty-second chapters

System log configuration

The main contents of this chapter are as follows：

- System log introduction
- System log configuration
- configuration SYSLOG

22.1 System log introduction

The system log module is an important part of the switch, it is used to record the operation of the whole system, operation behavior and abnormal behavior of users, to help administrators understand and monitor system works. The system log module management system all comes from the log information of the running modules, collects, sorts, stores and displays the output of the log information。

There is also an important debugging function in the log system. System log with debugging can help administrators or other technical personnel to monitor the operation of the network, debug and diagnose the fault in the network. Administrators can easily select the content that needs debugging, and by observing the log information of debugging output to locate and solve the fault of equipment or network。

The main contents of this section are as follows：

- Format of log information
- Log storage
- Log display
- Debugging tools

SEC.RU | Короткий путь к информации
Скачано с sec.ru

22.1.1 Format of log information

The format of log information is as follows：

Timestamp priority: module name: log content

There is a space between the timestamp and the priority. There is a colon and a space between the priority and the module name. There is a colon and a space between the module name and the content of the log。

An example of the format of log information is as follows：

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; the log content is Port up notification received for port ge1/2。

1）time stamp

Timestamp format: year / month / day hours: Minutes: seconds。

The hours are 24 hours, from 0 to 23。

The timestamp records the time that the log information was generated, and the system time of the switch was used. System time has been set up in the switch factory, administrators can also modify the system after power failure, the system is still able to run。

2）priority

Priority records the importance of the log information. According to the importance of the log information, the log information is divided into four levels. The order of priority is from high to low: Critical, Warning, Informational and Debugging. The description of priority is as follows：

priority	describe
Critical	Serious mistake
Warning	Common mistakes, warnings, very important tips
Informational	Important hints, general tips, diagnostic information
Debugging	debug information

3）Module name

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The module name records the module generated by the log message, and the following table lists some of the main modules that generate log information：

Module name	describe
CLI	Command line interface module
MSTP	Multi instance spanning tree protocol module
VLAN	VLAN function module
ARP	ARP protocol module
IP	IP protocol module
ICMP	ICMP protocol module
UDP	UDP protocol module
TCP	TCP protocol module

4）Log content

Log content is a phrase or sentence, which represents the content of the log message. The administrator can know what happened in the system by reading the log content。

22.1.2 Log storage

There are three ways to store logs：

- The log is stored in memory。
- Log storage to NVM。
- Log storage to server。

There are four priority according to the log log table in memory, each table log information stored a priority, which is based on the priority of the log log is divided into four categories, there is a separate log table for each log. Each log table has 1K entries, which can store 1K log information. When the log table is full, the log information with the longest coverage is behind the log. This storage method has a problem, when the system restarts, the log information is gone, the administrator can not see the log information when the system crashes, can not locate the problem。

For important log information, such as log information of priority Critical and Warning, these log information can be stored in the NVM of the system. In this way, the log information in NVM can be retained after the system is restarted, so that the administrator can locate the problem when the system crashes. But there is a problem with this storage method because of the limited capacity

SEC.RU | Короткий путь к информации
Скачано с sec.ru

of NVM, and the log information entries stored in NVM are very limited。

There is a better way is to store your log messages to the server, using the SYSLOG protocol can achieve real-time, log information can be sent to the server, the server to save the log information and displayed on an interface. This storage mode is not only convenient for users to view log information, but also has huge capacity. It can store a large amount of log information on the server。

At present, the system only supports the storage of log information into memory, and does not support the storage of log information into NVM or server。

22.1.3 Log display

There are two ways to display logs: manual display and real-time display. Manual display is that the user displays the log information by inputting the command, and the real-time display is when the log information is generated, the log information is directly output to the terminal, and the user can see it in time。

For manual display, the user can view all the log information, or view a priority log information. The display order of the log information is the last log information, so that the user can first see the latest running state of the switch。

For real-time display, the user must open the terminal real-time display switch. If the switch is open, the log information is not only written into the log table, but also the log information is exported to the terminal. If the switch is closed, the log information will not be displayed on the terminal in real time. The system can only log information real-time output to the Console terminal, does not support the log information output to the Telnet terminal。

22.1.4 Debugging tools

Debugging is a useful diagnostic tool for network device, system and module of data packet transceiver module, state machine change tracking process allows administrators to understand and monitor systems and modules, or if the network equipment appeared abnormal situation, through the debugging tracking tool。

Debugging tools provide rich switches, and by controlling these switches, administrators can track what they're interested in. When the device or network is out of order, the administrator can open the debugging switch associated with this exception and find the problem by tracking the execution of the system and the module。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

When a debugging switch is turned on, the system generates log information that will be written to the corresponding log table. In general, the priority of log information generated by debugging is Informational. When the terminal real-time display switch is opened, the log information will be output to the terminal in real time. When the debugging switch is turned off, the system does not generate log information。

22.2 System log configuration

The system log configuration includes the following：

- Configuring terminal real time display switch
- View log information
- Configure debugging switch
- View debugging information

22.2.1 Configuring terminal real time display switch

By default, the terminal real-time display switch is closed, and the log information generated by the system is written into the log table, but it will not be displayed on the terminal in real time. There are also some log information in the system that are not limited by this switch. These log messages are always output to the Console terminal in real time。

The terminal display switch is corresponding to the priority and the system log, if a priority terminal real-time display switch is turned on, the log information of the priority will be displayed on the terminal in real time, if the terminal display switch does not turn a priority, the priority of the log information is not displayed in real time on the terminal。

The switch can only display the log information on the Console terminal in real time, and can not display the log information on the Telnet terminal in real time。

When the user uses the write command to the system configuration stored in the configuration file, real-time display terminal switch configuration will be stored into the system files, when the system restarts the configuration will be lost, need to re configure。

Configure the terminal real-time display switch command as follows：

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
log display [critical | warning | informational | debugging]	Open terminal real time display switch. If you do not input parameters, open all priority terminal real-time display switch, if you enter one of the parameters, open the specified priority terminal real-time display switch。	Privileged mode
no log display [critical | warning | informational | debugging]	Close the terminal real time display switch. If you do not input parameters, turn off all priority terminal real-time display switches, if you enter one of the parameters, close the specified priority terminal real-time display switch。	Privileged mode

22.2.2 View log information

The commands for viewing log information are listed below：

command	describe	CLI mode
show log display	Real time display switch configuration for displaying all priority terminals。	Normal mode, privileged mode
show log [critical | warning | informational | debugging]	Display log information in log table. If you don't input parameters, display all log table log information, if you enter one of the parameters, display the log information of the specified priority log table。	Normal mode, privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

22.2.3 Configure debugging switch

The system provides a rich debugging switch, involving multiple modules, which only lists the commands of each module, and the complete format of the commands. See the command manual。

When the user uses the write command to the system configuration stored in the configuration file, debugging switch configuration will be stored into the system files, when the system restarts the configuration will be lost, need to re configure。

The schematic command for configuring the debugging switch is as follows：

command	describe	CLI mode
debug ip …	Open system to send and receive IP packet related debugging switch。	privileged mode
no debug ip …	Close debugging switches for sending and receiving IP packets。	privileged mode
debug ip icmp …	Open system to send and receive ICMP packet related debugging switch。	privileged mode
no debug ip icmp …	Close debugging switches for sending and receiving ICMP packets。	privileged mode
debug ip arp …	Open system to send and receive ARP packet related debugging switch.	privileged mode
no debug ip arp …	Close debugging switches for sending and receiving ARP packets。	privileged mode
debug ip udp …	Open system to send and receive UDP packet related debugging switch。	privileged mode
no debug ip udp …	Close debugging switches for sending and receiving UDP packets。	privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

debug ip tcp …	Open system to send and receive TCP packet related debugging switch。	privileged mode
no debug ip tcp …	Close debugging switches for sending and receiving TCP packets。	privileged mode
debug mstp …	Open the debugging switch related to MSTP protocol diagnostics。	privileged mode
no debug mstp …	Close debugging switches related to MSTP protocol diagnostics。	privileged mode
debug igmp snooping …	Open IGMP SNOOPING function diagnostic related debugging switch。	privileged mode
no debug igmp snooping …	Close IGMP SNOOPING function diagnostic related debugging switches。	privileged mode
debug dhcp snooping …	Open DHCP SNOOPIN protocol for diagnosis of related debugging switches	privileged mode
no debug dhcp snooping …	Close the DHCP SNOOPIN protocol diagnostic debugging switch	privileged mode
no debug all	Turn off all debugging switches in the system。	privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

22.2.4 View debugging information

The commands for viewing the debugging information are as follows：

command	describe	CLI mode
show debugging [ip | mstp | igmp snooping | dhcp snooping]	See the debugging switch configuration. If you don't have input parameters, look at the debugging switch configuration of all modules. If you only input one of these parameters, you only look at the debugging switch configuration of a module. If the input parameter is IP, the debugging switch configuration of the IP, ICMP, ARP, UDP, and TCP modules will be checked。	Normal mode, privileged mode

22.3 configuration SYSLOG

SYSLOG includes the following：

- SYSLOG introduce
- SYSLOG configuration
- SYSLOG configuration example

22.3.1 SYSLOG introduce

SYSLOG is a standard protocol for the management of equipment log information, which has been greatly applied because of its simplicity of design. In the SYSLOG system, it is divided into three parts. One is to define each sub module to distinguish the log information produced by different modules; define different log information levels to observe the running status of the device。All kinds of log information of the equipment are collected according to this agreement. The second is the configuration file, how to deal with the custom log information collected, can be stored in local, can be sent to the network server specified, can be sent to the specified user login log information and so on; by the configuration file to decide how to save the equipment。The third is to send SYSLOG protocol message according to the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

message format defined by RFC. As you can see, in our switch system, the whole SYSLOG work convention is the system log module. The first part of the SYSLOG protocol is completed by each function sub module of the switch, and sends the log information of each level to the system log module. Maintaining four levels of log tables in the system log module。The second part of the SYSLOG protocol by the system log module to uniform distribution of log information, one is through the terminal display switch or real-time display in the serial port terminal two is stored manually; log table four levels in memory; three is to save the log information of high level on the NVM log records in order to avoid the loss of important power failure; the four is the log is sent to the remote server storage, collecting and sorting through the SYSLOG message. The SYSLOG sub module in the system log module only implements third parts, and transmits the system log to the server。

22.3.2 SYSLOG configuration

The SYSLOG configuration command contains：

- Open syslog protocol
- Closing the syslog protocol
- Set syslog send level
- Restore syslog send level to default value

command	describe	CLI mode
syslog open <server-ip> [udp-port]	Open the syslog protocol; server-ip parameters for the server IP address is required; udp-port parameters for the destination port number, protocol message optional, if not set to the default value of 514; if the server configuration and set to be consistent。	Global configuration mode
syslog close	Closing the syslog protocol	Global configuration mode
syslog level <critical | warning | informational | debugging>	Set the sending level of the log, such as set to debugging level, all the logs will be sent to the server。	Global configuration mode
no syslog level	Restore the send level to the default value debugging	Global configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

22.3.3 SYSLOG configuration example

（1） Configuration

Configure the syslog server IP address for the 192.168.2.201 server configuration software receives the syslog message UDP to port 200; the ge1/3 port is connected to the server; the server save only a maximum of two levels of logging。

The switch is configured as follows：

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#interface ge1/6
Switch(config-ge1/6)#switchport access vlan 3
Switch(config-ge1/6)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#exit
Switch(config)#syslog open 192.168.2.201 200
Switch(config)#syslog level warning

（2） Verification

Switch#show running-config
!
syslog open 192.168.2.201 200
syslog level warning
!
……
!
line vty

SEC.RU | Короткий путь к информации
Скачано с sec.ru

!

end

Switch#show syslog

Syslog is opened!

server ip address: 192.168.2.201

udp destination port: 200

severity level: warning

Twenty-third chapters

Port loop

The main contents of this chapter are as follows：

- profile
- Protocol principle
- Configuration introduction

23.1 Profile

When the loop appears a port switch condition, will cause the broadcast storm this port, and all radio package source MAC address to the learning loop port forwarding will cause the equipment can not be normal。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

23.2 Protocol principle

。。

23.2.1 Detection process

When a port is enabled when the ELD protocol, will be at this port to enable a regular timer timer expires, sending loop detection packets, if in a timer period received their loop detection packets, it is assumed that the existing port loop will execute the loop execution port blocking operation, and empty this port FDB。

If a port is a port member of multiple VLAN, then this port automatically sends loop detection packets to all VLAN. That is to say, this port automatically detects whether all VLAN loops belong to it。

23.2.2 Recovery mode

It says that when a port loop appears, the port will be blocked. The ELD protocol has two types of recovery patterns that users can configure: automatic recovery and manual recovery。

Automatic recovery is when a port is blocked after the circuit, ELD protocol enabled a recovery timer, the timer expires will perform a blocking loop reverse operation, and in the port loop detection timer is enabled again。

Manual recovery is the port is blocked, the protocol is no longer enabled timer to restore the port, the user to enter their own commands to perform the reverse operation of the blocking loop。

23.2.3 Protocol security

The ELD protocol in the network easily attacked, which means that the user can according to the ELD protocol packet format to port ELD protocol to send a packet to enable ELD protocol, the port is not possible in the loop is blocked due to the wrong decision。

The ELD protocol uses two strategies to prevent similar attacks and minimize errors。

First, the ELD protocol is a protocol without interaction, that is, it does not rely on other devices, then the packet itself can be simply encrypted. Our operation here is to send the ELD protocol package with a key, and the user can not disguise the protocol packet without the key。

Decision two, mainly to prevent the attacker to attack reflex through the capture packets, can receive the allocation of a certain period switch packet format to prevent attack, the user needs to configure。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

23.3 Configuration introduction

The ELD protocol is implemented based on ports, and there is no unified enable command。

23.3.1 Global configuration

command	describe	mode
loop-detection detection-time <1-65535>	Configure the loop detection time, this time must be less than 2 times the recovery time, the default is 5 seconds。	Global configuration mode
loop-detection resume-time <10-65535>	The automatic recovery time must be greater than 2 of the loop check time. If the automatic recovery is enabled, this configuration will take effect. The default recovery time is 600 seconds。	Global configuration mode
loop-detection protocol-safety	Enable protocol security check, default is closed。	Global configuration mode
loop-detection respond-packets	Configure the number of packets that must be received within a certain period of time. If the protocol security check is enabled, this configuration will take effect, with the default value of 10	Global configuration mode

Global configuration is the uniform attribute of configuration protocol。

23.3.2 Interface configuration

The interface configuration is configured for each port。

command	describe	mode
Loop-detection enable	Enable ELD protocol on a port。	Interface configuration mode
Loop-detection resume	Manual recovery, restart loop check。	Interface configuration mode
loop-detection resume-mode {automation | manual}	Configure recovery mode, select manual recovery or automatic recovery, default is automatic recovery。	Interface configuration mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	The command configures whether the port is shutdown when the loop is present。	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

23.3.3 Display configuration

Show loop-detection [ifname]

Display all the configuration of the protocol and the configuration of an interface。

Twenty-fourth chapters

SNTP configuration

The main contents of this chapter are as follows：

- SNTP introduce
- configuration SNTP
- SNTP information display

24.1 SNTP introduce

At present, the Internet has been widely used in the communication protocol to realize network time synchronization, namely NTP (Network Time Protocol Network Time Protocol), a protocol is a simplified version of the NTP protocol, namely SNTP (Simple Network Time Protocol simple network time protocol).

The NTP protocol can span a variety of platforms and operating system, with a very sophisticated algorithm, so the effect of delay and jitter is almost not affected by the network, can

SEC.RU | Короткий путь к информации
Скачано с sec.ru

provide 1-50ms accuracy while providing.NTP authentication mechanism, the security level is very high. But the complicated NTP algorithm, the system requires a higher.

SNTP (Simple Network Time Protocol) is a simplified version of NTP, in the implementation of the calculation time using a simple algorithm, the performance is high, and the accuracy can generally reach about 1 second, but also basically meet the needs of most occasions.

Because the message of SNTP and NTP message are completely identical, the SNTP Client implemented by this switch can be fully compatible with NTP Server

24.2 configuration SNTP

project	Default value
SNTP state	Disable closes SNTP services
NTP Server	There are three NTP Server defaults 211.115.194.21 203.109.252.5 192.43.244.18
The synchronization time interval of SNTP	1800 second
local time zone	+8, East eight district

24.2.1 Default SNTP settings

Open and close SNTP

Configuration is as follows:

Switch# configure terminal

Enter global configuration modeSwitch(config)# sntp enable

Open SNTP

Switch(config)# sntp disable

Close SNTP

24.2.2 Configuring SNTP Server address

Because of SNTP's packets and NTP is exactly the same, so SNTP Client can be fully compatible with NTP Server. network there are more NTP Server, you can select a network delay less as a switch on the NTP Server.

The specific NTP server address can be logged on http://www.time.edu.cn/ or http://www.ntp.org/ to obtain

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Such as 192.43.244.18 (time.nist.gov)

This switch has three default Server address, 211.115.194.21, 203.109.252.5 and 192.43.244.18 respectively, the first switch using the first Server address to the synchronization time, if synchronization is not to use second Server addresses, and so on. In general, users do not need to configure the Server address, and use the default Server address directly. If you need to configure the Server address in a special case, you need to delete the default Server address first and then add a new Server address。

Add a Server address configuration as follows：

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp server 210.72.145.44

Add SNTP server IP, if the switch already exists three Server addresses, it will increase the failure, you need to delete the address and then add

The configuration of deleting Server address is as follows：

Switch(config)# no sntp server

Delete all Server addresses

Switch(config)# no sntp server 210.72.145.44

Delete one of the Server addresses

The configuration of setting the Server address back to the default address is as follows：

Switch(config)# sntp server default

The Server address is reset to the default address, that is, address 211.115.194.21, 203.109.252.5 and 192.43.244.18

24.2.3 Configure the SNTP sync clock interval

SNTP Client requires timing and NTP Server synchronous clocks, so that clock timing is positive.

Configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Set the timing synchronization clock interval, the unit is seconds, the range is 60 seconds -65535 seconds. The default value is 1800 seconds, set here for 60 seconds

Switch(config)# no sntp interval

The timing synchronization clock interval is restored to the default 1800 seconds

24.2.4 Configuring the local time zone

After the SNTP protocol communication, the time is Greenwich mean time (GMT), in order to prepare for hunting local time, you need to set the region to adjust the standard time. The switch

SEC.RU | Короткий путь к информации
Скачано с sec.ru

defaults the local time zone to the East eight zone and the time zone in which China is located。

Configuration is as follows:

Switch# configure terminal

Switch(config)# sntp time-zone -8

Set the local time zone to the West eight area

Switch(config)# no sntp time-zone

The local time zone is restored to the East eight area

24.3 SNTP information display

Configuration is as follows:

Switch# show sntp

Switch# show running-config

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Twenty-fifth chapters

OAM configuration

The main contents of this chapter are as follows：

- OAM introduce
- configuration OAM
- Typical configuration examples of OAM

25.1 OAM introduce

Ethernet OAM (Operations, Administration and Maintenance) is a tool to monitor network problems. It works at the data link layer and uses OAMPDU Protocol Data Units (OAM) to report the state of the network, so that the network administrator can manage the network more effectively。

At present, Ethernet OAM mainly solves the common link problem of "last mile" in Ethernet access. By enabling the Ethernet OAM function on two point to point devices, the link state between two devices can be monitored。

This section mainly introduces the main functions of Ethernet OAM, including the main functions of Ethernet：

- Link performance monitoring: it can detect link failures；
- Fault detection and warning: notify the network administrator in time when the link fails；
- Loop test: detecting link failures by returning non OAMPDU loops。

25.1.1 Link performance monitoring

Link monitoring is used to detect and detect link layer failures in various environments。

Ethernet OAM uses the interaction of Event Notification OAMPDU to monitor the link. When the link failure occurs, after the local link monitors the fault, the Event Notification OAMPDU is sent to the Ethernet OAM entity to notify the general link event. Administrators can observe the log information dynamically to grasp the status of the network。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Event type	Chinese meaning	describe
Errored Symbol Event	Error signal event	In unit time, the number of false signals exceeds the threshold
Errored Frame Event	Error frame event	In unit time, the number of error frames exceeds the threshold
Errored Frame Period Event	Wrong frame periodic events	The number of error frames exceeds the threshold when the specified number of frames is received
Errored Frame Seconds Summary Event	Wrong frame seconds total event	Within the specified time, the number of frames per second exceeds the threshold

25.1.2 Remote fault detection

Ethernet fault detection is very difficult, especially when the network physical communication is not interrupted and the network performance drops slowly。

OAMPDU defines a flag (Flag domain) that allows Ethernet OAM entities to pass the fault information to the opposite end. The flag can represent the following emergency link events：

Table 5 emergency link events

Event type	Chinese meaning	describe	OAMPDU Sending frequency
Link Fault	Link fault	Loss of end-to-end link signal	Send once every second
Dying Gasp	Fatal fault	Unexpected local failures, such as power outages	Uninterrupted transmission
Critical Event	Emergency	Unclear emergency events, such as link single pass	Uninterrupted transmission

Ethernet OAM connection process is constantly sending Information OAMPDU, the end of the OAM entity can be the end of the emergency link event information through the Information OAMPDU to tell the remote OAM entity. In this way, the administrator can dynamically understand the state of the link, and deal with the corresponding errors in a timely manner。

25.1.3 Distal loopback

Yuan Duan loopback function refers to the active mode of the OAM entity to the end (Yuan Duan) send all other messages except OAMPDU, the end of the receipt of the message is directly returned to the end. It can be used to locate link failures and detect link quality: network administrators can judge the link performance (including packet loss rate, delay, jitter, etc.) by observing the return of non OAMPDU packets。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

25.2 configuration OAM

command	describe	CLI mode
oam errored-frame period <1-60>	Configuring Ethernet ports for periodic values of error frame event detection. The period of the default frame event is 1s。	Privileged mode
no oam errored-frame period	Reset Ethernet ports for periodic values of error frame event detection. The period of the default frame event is 1s。	Privileged mode
oam errored-frame threshold <0-4294967295>	Configuring thresholds for error frame event detection. The default error frame event threshold is 1。	Privileged mode
no oam errored-frame threshold	Reset threshold for error frame event detection. The default error frame event threshold is 1。	Privileged mode
oam errored-frame-period period <100-6000>	Configuring Ethernet ports to detect periodic values of false frame periodic event detection. The period of the default frame cycle event is 1000 milliseconds。	Privileged mode
no oam errored-frame-period period	Reset Ethernet ports for periodic values of false frame periodic event detection. The period of the default frame cycle event is 1000 milliseconds。	Privileged mode
oam errored-frame-period threshold <0-4294967295>	Configuring threshold values for periodic event detection in error frames. The default error frame event threshold is 1。	Privileged mode
no oam errored-frame-period threshold	Reset the threshold of periodic event detection for error frames. The default error frame event threshold is 1。	Privileged mode
oam errored-frame-seconds period <10-90>	Configuring Ethernet ports for periodic values of error frame seconds event detection. The period of the default frame event is 60s。	Privileged mode
no oam errored-frame-seconds period	Reset Ethernet port for periodic values of error frame seconds event detection. The period of the default frame event is 60s。	Privileged mode
oam errored-frame-seconds threshold <0-900>	Configuring thresholds for error frame seconds event detection. The default error frame seconds event threshold is 1。	Privileged mode
no oam errored-frame-seconds threshold	Reset error frame seconds threshold for event detection. The default error frame seconds event threshold is 1。	Privileged mode
oam mode (active| passive)	Configure Ethernet OAM mode, default Ethernet OAM link mode as active mode。	Interface configuration mode
oam enable	Open Ethernet OAM function, default Ethernet OAM function is closed。	Interface configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

oam loopback	Enable Ethernet OAM loopback function. Default Ethernet OAM loopback function shutdown。	Interface configuration mode
no oam loopback	Turn off Ethernet OAM loopback function. Default Ethernet OAM loopback function shutdown。	Interface configuration mode
show oam configuration	Displays the window and threshold of general link events。	Privileged mode
show oam local-state (IFNAME|)	View OAM local information	Privileged mode
show oam remote-state (IFNAME|)	View OAM peer to peer information	Privileged mode
show oam link-event (IFNAME|)	View OAM link event information	Privileged mode
show oam-loopback IFNAME	Display loopback information of a port。	Privileged mode

25.3 Typical configuration examples of OAM

1 Networking requirement
By configuring the Ethernet OAM protocol on Device A and Device B, the data link layer is managed; (Device A port: fe1/1, Device B port: fe1/1)

(1) Configuration Device A：
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1

On port Ethernet1/0/1, configure its Ethernet OAM connection mode as passive mode, and enable Ethernet OAM function。
Switch(config-fe1/1)#oam mode passive
Switch(config-fe1/1)#oam enable

(2) Configuration Device B:
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
The Ethernet OAM working mode of configuring port Ethernet1/0/1 is default mode active, and can make Ethernet OAM function。

Switch(config-fe1/1)#oam enable

(3) Checking configuration effect on (Device A):
Switch>enable
Switch#show oam fe1/1

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Twenty-sixth

CFM configuration

switch provides CFM function, which is mainly used to detect link connectivity in the two layer network, confirm the fault and determine the location of the fault, mainly including the following contents：

- CFM profile
- Brief introduction of CFM configuration task
- CFM base configuration
- Configure various functions of CFM
- CFM display and maintenance
- Typical configuration examples

26.1 CFM profile

CFM is the abbreviation of Connectivity Fault Management (connected error management). The CFM of this switch mainly refers to connected error detection, which follows the CFM protocol defined by IEEE 802.1ag. It is a two layer link based on end to end OAM VLAN (Operations Administration, and Maintenance, operation, management and maintenance) mechanism, mainly used in the two layer of the network detection link connectivity, confirm the fault and determine the fault position。

26.1.1 Basic concepts of CFM

1 Maintenance domain

The Maintenance Domain (MD) points out the network covered by the connectivity error detection, whose boundaries are defined by a series of maintenance endpoints configured on the port. The maintenance domain is marked by "domain name maintenance"。

In order to locate the fault point accurately, the concept of level (hierarchy) is introduced into the maintenance domain. Maintenance domain is divided into eight levels, represented by integer 0~7, the larger the number, the higher the level, the greater the scope of the maintenance domain. Different maintenance domains can be adjacent or nested, but can not cross, and nested can only be embedded by high-level maintenance domain to low-level maintenance domain, that is to say, low level maintenance domain must be included in the high-level maintenance domain. The CFM PDU of the low-level maintenance domain will be discarded after entering the high-level maintenance domain; the CFM PDU of the high-level maintenance domain can cross the low level

SEC.RU | Короткий путь к информации
Скачано с sec.ru

maintenance domain; the CFM PDU of the same level maintenance domain can not cross each other。

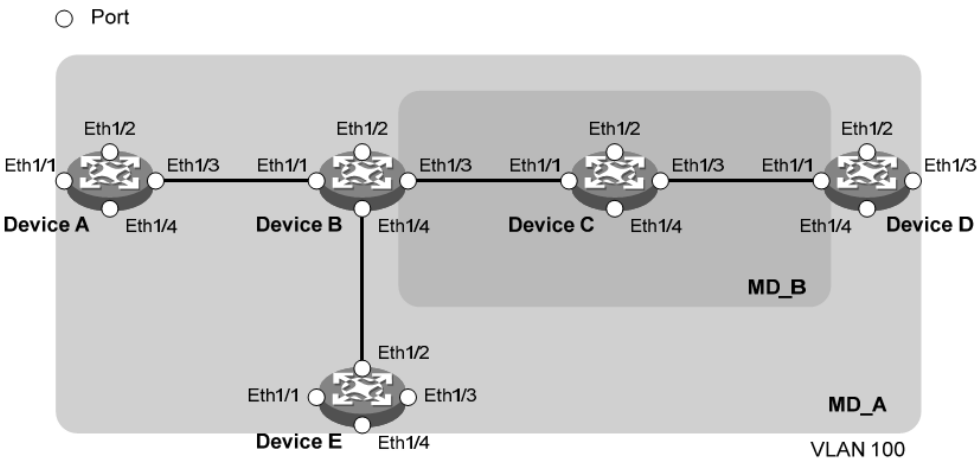


Figure 1-1

In practical application, to rational planning of maintenance domain: as shown in Figure 1-1, MD_B nested in the maintenance domain maintenance domain MD_A, to connectivity detection in MD_A, MD_A CFM PDU is required to cross the MD_B, it needs to be MD_A better than MD_B high level configuration. In this way, MD_A CFM PDU can pass through MD_B, so as to achieve the whole MD_A connectivity fault management, and the MD_B CFM PDU will not spread to MD_A。

Maintenance domain classification makes fault location more convenient and accurate, as shown in Figure 1-1, MD_B embedded in the maintenance domain maintenance domain MD_A, if it is found that the link is on the border of MD_A indicates that the domain of equipment malfunction, failure may occur in Device A ~ Device E five device. At this time, if not found in the MD_B link on the boundary of the fault range is reduced to Device B to Device D of the three sets of equipment; on the other hand, if the MD_B equipment is working properly, it can at least determine the Device C there is no fault。

2 Maintenance set

In the maintenance domain, Maintenance Association (MA) can be configured according to the requirements. Each maintenance set is a collection of maintenance points in the domain. The maintenance set is marked by "maintenance domain name + maintenance set name"。

The maintenance set serves a VLAN, and the message sent by the maintenance point of the maintenance has the tag of the VLAN. Meanwhile, the centralized maintenance point can receive the message sent by the other maintenance points in the maintenance set。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3 Maintenance point

The maintenance point (Maintenance Point, MP) in port configuration, belong to a set of maintenance, maintenance can be divided into endpoint (Maintenance Association End Point, MEP) and the maintenance of the middle point (Maintenance Association Intermediate Point, MIP) two。

1) Maintenance endpoint

The maintenance endpoint is identified by an integer called MEP ID, which determines the scope and boundary of the maintenance domain. The maintenance set and maintenance domain belonging to the maintenance endpoint determine the VLAN attribute and level of the message sent by the maintenance endpoint。

The level of the endpoint determines the level of the message that it can handle, and the level of the message that maintains the endpoint is the level of the endpoint of the maintenance. When the maintenance endpoint receives a message above their level, not processed, but according to its original path forwarding; and when the message received is less than or equal to their maintenance endpoint level will no longer maintain the forwarding endpoint for the corresponding processing, to ensure a low level maintenance domain message will not spread to the high level maintenance domain。

Maintenance endpoints have directionality, which can be divided into two types: extroverted MEP and inward MEP. The direction of the endpoint maintenance indicates the location of the maintenance domain relative to the port。

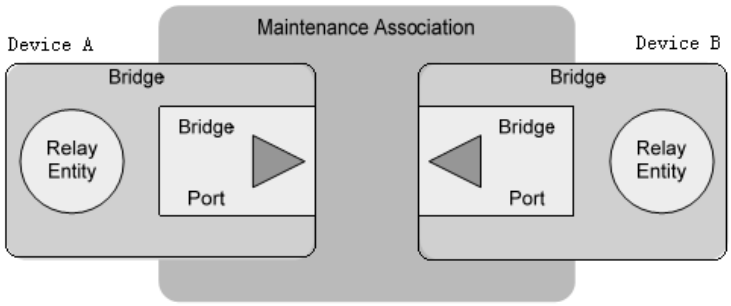


Fig. 1-2 schematic diagram of outgoing MEP

As shown in Figure 1-2, the outgoing maintenance endpoint sends the message outward through its port，

SEC.RU | Короткий путь к информации
Скачано с sec.ru

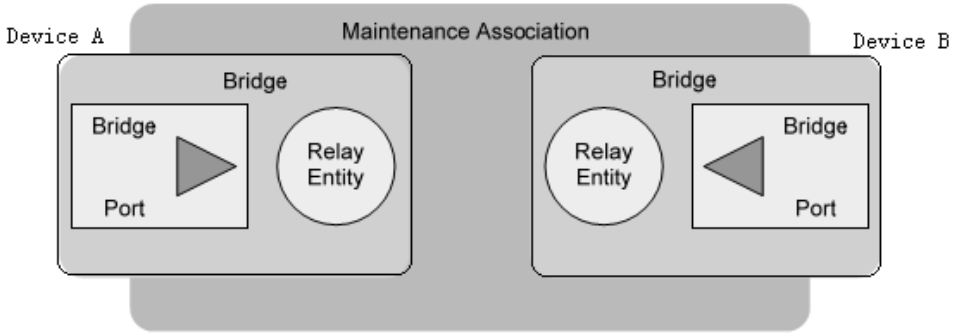


图 1-3

As shown in Fig. 1-3, the inward maintenance endpoint does not send messages outward through its ports, but sends messages outward from other ports on the device。

2) Maintenance intermediate point

The maintenance intermediate point is located in the maintenance domain, and cannot send CFM protocol message actively, but it can process and respond to CFM protocol message. Maintaining the maintenance set and maintenance domain of the intermediate point determines the VLAN attribute and level of the received message of the maintenance intermediate point. Maintaining the intermediate point can be used with the maintenance endpoint to accomplish functions similar to Ping and tracert. Similar maintenance endpoints, while maintaining the middle point of message received above their level, not processed, but according to its original path forward; and when the message received is less than or equal to their own point maintenance intermediate level, will be processed。

As shown in Figure 1-4, is a hierarchical configuration of CFM, assuming that all six devices are only two ports, and the allocation of maintenance endpoints and maintenance intermediate points in some ports, such as the Device B port 1 configuration maintenance points are as follows: Level 5, level for the maintenance of intermediate point 3 within the maintenance endpoint, level 2 to level 0 maintenance endpoints and outgoing maintenance endpoint. There are four levels of maintenance domains in the graph. The maintenance area of the identification number is higher and the control range is wide; the maintenance area of the identification number is smaller and the control range is small。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

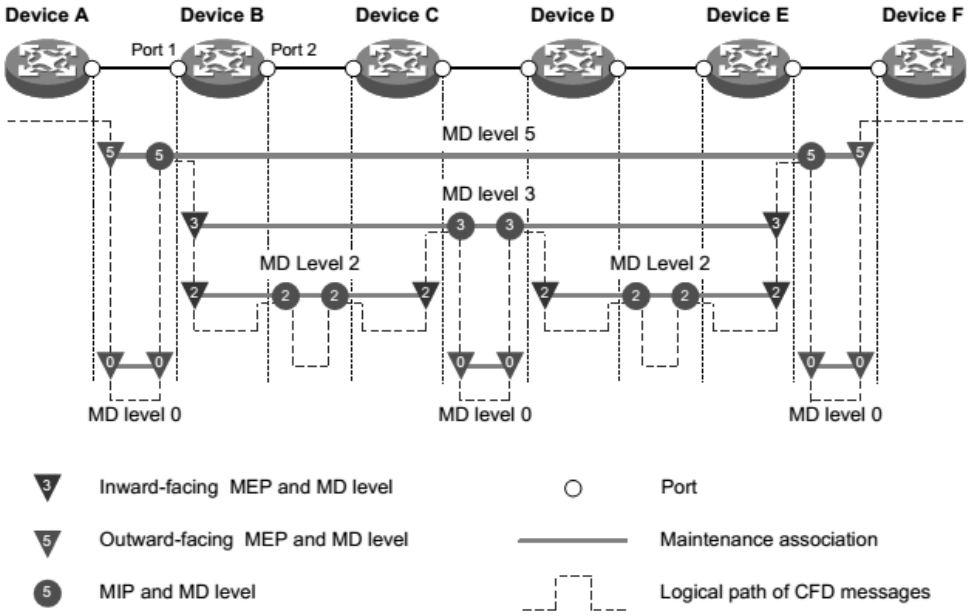


Figure 1-4 hierarchical configuration of maintenance points

4 Maintain endpoint list

The list is the same maintenance maintenance endpoint allows configuration within the set of local maintenance endpoints and the need to monitor the remote maintenance endpoint set, which defines a range of maintenance maintenance endpoint set: different devices on the same maintenance within the set of all maintenance endpoints should be included in this list, MEP and ID do not repeat. If the maintenance endpoint receives the CCM (Continuity Check Message, continuity check message) message from the remote device and the maintenance endpoint is not in the maintenance endpoint list of the same maintenance set, then the message is discarded。

5 Service instance

A service instance is represented by an integer that represents a maintenance set within a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the message processed by the maintenance point in the service instance。

26.1.2 Various functions of CFM

The effective application of connectivity error detection is based on reasonable network deployment and configuration. Its function is implemented between the configured maintenance points, including：

- Continuous testing function（Continuity Check，CC）
- Loopback function（Loopback，LB）
- Link tracking function（Linktrace，LT）

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. Continuous testing function

The continuity detection function is used to detect the connectivity between the maintenance endpoints. Connectivity failures may be caused by device failures or configuration errors. The realization of this function is that the CCM message is periodically sent from the maintenance endpoint, which is multicast message, and the other maintenance endpoints of the same maintenance set receive the message, and the remote state is obtained. If the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint during the 3.5 CCM packet transmission cycles, the link will be problematic and the log report will be output. When maintaining multiple maintenance endpoints in the domain to send CCM packets, the link detection between multipoint and multipoint is realized。

2. Loopback function

The loopback function, similar to the ping function of the IP layer, is used to verify the connection state between the local device and the remote device. The realization function is: the maintenance of endpoint (Loopback Message, LBM sends the message to the remote maintenance loop), and according to the end can receive feedback LBR (Loopback Reply, loopback reply message) to test the link state. Both LBM and LBR are unicast messages。

3. Link tracking function

Link tracking function is used to determine the source to the target endpoint maintenance path, this is sent by the source: LTM (Linktrace Message, linktrace message) to the target endpoint maintenance, maintenance and maintenance after the endpoint LTM intermediate point received the message, will send LTR (Linktrace Reply, link tracking response message) to the source side, the source is based on the received LTR to determine the path to the target endpoint maintenance. LTM is multicast message, and LTR is unicast message。

26.2 Brief introduction of CFM configuration task

Before configuring the CFM function, plan the network as follows：

- The maintenance domain of the whole network is graded to determine the boundary of each level maintenance domain。
- Determine the name of each maintenance domain, and the same maintenance domain has the same name on different devices。
- According to the VLAN that needs to be monitored, the maintenance set in each maintenance

SEC.RU | Короткий путь к информации
Скачано с sec.ru

domain is determined。

- Determine the name of each maintenance set, and the same maintenance set in the same maintenance domain has the same name on different devices。
- The maintenance endpoint should be planned on the boundary port of maintenance domain and maintenance set, and the maintenance intermediate point can be planned on non boundary equipment or port。
- A list of remote maintenance endpoints to determine maintenance endpoints。

After completing the network planning, please configure the following。

Configuration task		Explain	Detailed configuration
CFM base configuration	Enable CFM function		0
	Configuration service instance		0
	Configuration maintenance endpoint		**Ошибка! Источник ссылки не найден.**
	Configuration maintenance intermediate point		0
Configure various functions of CFM	Configuration continuity detection function		**Ошибка! Источник ссылки не найден.**
	Configuration loopback function		**Ошибка! Источник ссылки не найден.**
	Configuring link tracking function		**Ошибка! Источник ссылки не найден.**

note:

- The port blocked by the STP protocol can not receive, send and respond to the CFM protocol packet; but if the port is configured to be outgoing MEP, then even if the port has been blocked by the STP protocol, it will still receive and send CCM message。
- Only Ethernet ports support configuring CFM functions。

26.3 CFM base configuration

26.3.1 Enable CFM function

command	describe	CLI mode
cfm enable	Enable CFM function. Default shutdown。	Configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

26.3.2 Configuration service instance

Before configuring the maintenance endpoint and maintaining the intermediate point, the service instance must be configured first. A service instance is represented by an integer that represents a maintenance set within a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the message processed by the maintenance point in the service instance。

Create maintenance domains, maintenance sets and service instances in strict accordance with the following order。

command	describe	CLI mode
cfm md <md-name> level <level-value>	Create maintenance domain. There is no maintenance domain by default。	Configuration mode
cfm ma <ma-name> md <md-name> vlan <vlan-id>	Create maintenance set. The maintenance set has not been created by default	Configuration mode
cfm service-instance <instance-id> md <md-name> ma <ma-name>	Creating service instances. The default does not create a service instance	Configuration mode

26.3.3 Configuration maintenance endpoint

The maintenance endpoint is a functional entity in the service instance, and the CFM function is mainly embodied in the operation of the maintenance endpoint. It implements the functions of CC, LB and LT, and alerts the false CCM message and cross connection. Because the maintenance endpoint is configured on the service instance, the maintenance domain level and the VLAN attribute represented by the service instance naturally become the attributes of maintaining the endpoint. After creating the maintenance endpoint, you need to configure the remote maintenance endpoint list of the specified maintenance endpoint, and the remote maintenance endpoint list is a collection of remote maintenance endpoints that need to be monitored in the same maintenance set。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
cfm mep <mep-id> service-instance <instance-id> {inbound | outbound}	Create maintenance endpoints. There is no maintenance endpoint on the default port。	Interface mode
cfm remote-meplist <mep-list> service-instance <instance-id> mep <mep-id>	A list of remote maintenance endpoints configured with specified maintenance endpoints. There is no maintenance endpoint list for the default port。	Interface mode
cfm mep service-instance <instance-id> mep <mep-id> enable	Enable endpoint maintenance. The default maintenance endpoint is closed。	Interface mode

note:

- After the endpoint is enabled, the maintenance endpoint processes the received CCM packets。

26.3.4 Configuration maintenance intermediate point

A maintenance intermediate point is a functional entity in a service instance that responds to LBM and LTM messages。

The maintenance of the middle point is the system in accordance with the rules in each port created automatically, the creation rules are as follows: if the middle point of no maintenance port, then in accordance with the level from low to high order check each maintenance set domain, as shown in Figure 1-5 and in accordance with the process to decide whether to create a maintenance (intermediate point in the same VLAN)。

Figure 1-5 maintaining the creation process of the intermediate point

Please configure and maintain the creation rules of the intermediate points according to the network planning。

command	**describe**	**CLI mode**
cfm mip-rule {explicit | default} service-instance <instance-id>	Creation rules for intermediate points of configuration maintenance. By default, there are no maintenance rules for creating intermediate points,	Configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	and there is no creation maintenance intermediate point。	

note：

After configuring the creation rules for maintaining intermediate points, any of the following conditions can trigger the creation or deletion of the maintenance intermediate point：

- Enable CFM function。
- Creating or deleting maintenance endpoints on a port。
- The VLAN property of the port changes。
- The creation rules for maintaining intermediate points change。

26.4 Configure various functions of CFM

Before configuring the various functions of CFM, the basic configuration of CFM needs to be completed。

26.4.1 Configuration continuity detection function

By configuring the continuity detection function, the CCM messages can be sent between the maintenance endpoints to detect the connectivity status between the maintenance endpoints, so as to realize the management of link connectivity。

command	describe	CLI mode
cfm cc interval <interval-value> service-instance <instance-id>	The value of the time interval in the CCM message sent by the configuration maintenance endpoint. By default, the value of the time domain in the CCM message sent by the maintenance endpoint is 4。	Configuration mode
cfm cc service-instance <instance-id> mep <mep-id> enable	CCM message sending function that can maintain endpoint. By default, the CCM message sending function for maintaining endpoints is closed。	Interface mode

The relationship between the value of the time domain (Interval domain) in the CCM message sent by the endpoint maintenance and the CCM sending time interval and the remote MEP timeout time is shown in Table 1-1。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Table 1-1 the relationship between the time interval value and the CCM sending time interval and the MEP timeout time

note:

- The endpoint of the CCM message must be the same at the maintenance endpoint of the same maintenance domain and maintenance set on different devices。
- If the value of the time domain of sending the CCM message to the maintenance endpoint is 3, it is suggested that more maintenance endpoints should not be configured in the same maintenance domain and maintenance set, otherwise the performance of the whole machine will be affected。

26.4.2 Configuration loopback function

By configuring loopback function, the link state can be checked so as to verify the link connectivity。

command	describe	CLI mode
cfm loopback service-instance <instance-id> mep <mep-id> { target-mep <target-mep-id> | target-mac <mac-address> } [number <number>]	Enable loopback function to check link status。	Privileged mode

26.4.3 Configuring link tracking function

By configuring the link tracking function, the path between the specified maintenance endpoint and the destination maintenance endpoint can be found, thus the link failure can be realized

Location。 It includes the following two functions:

- Find the path from the specified maintenance endpoint to the destination maintenance endpoint: by sending the LTM message from the designated maintenance endpoint to the destination maintenance endpoint, and detecting the LTR message of the response to determine the path between the devices。
- Automatic transmission link tracking message: enable this function, while maintaining at the end of 3.5 CCM packet sending period has not received the message sent to the remote maintenance of CCM endpoint, which determine the same remote maintenance error connecting terminals, will send the LTM message LTM message (target for remote maintenance endpoints, TTL field of LTM message for a maximum of 255), through the LTR message response to locate fault detection。

command	describe	CLI mode
cfm linktrace service-instance <instance-id> mep <mep-id> {target-mep <target-mep-id> | target-mac <mac-address> } [ttl	Find the path from the specified maintenance endpoint to the	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

<ttl-value>] [hw-only]	destination maintenance endpoint。	
cfm linktrace auto-detection [size <size-value>]	Enable automatically send link tracking message function. By default, the automatic send link tracking message function is closed。	Configuration mode

26.5 CFM display and maintenance

After completing the above configuration, executing show command in any view can display the operation of CFM after configuration, and verify the effect of configuration by checking the display information。

command	describe	CLI mode
show cfm status	Displays the enabling state of CFM。	Privileged mode
show cfm md	Display configuration information of maintenance domain	Privileged mode
show cfm ma [[<ma-name>] md <md-name>]	Display configuration information of maintenance set	Privileged mode
show cfm service-instance [<instance-id>]	Display configuration information for service instances	Privileged mode
show cfm mp [interface <interface-name>]	Display maintenance point information	Privileged mode
show cfm mep <mep-id> service-instance <instance-id>	Displays the attributes and running information of the maintenance endpoint	Privileged mode
show cfm linktrace-reply [service-instance <instance-id> [mep <mep-id>]]	LTR message information obtained from the display maintenance endpoint	Privileged mode
show cfm remote-mep service-instance <instance-id> mep <mep-id>	Displays information about remote maintenance endpoints	Privileged mode
show cfm linktrace-reply auto-detection [size <size-value>]	Display the content of LTR message received automatically by sending LTM message	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

26.6 Typical configuration examples

Networking requirement:

Consists of five sets of equipment network is divided into MD_A and MD_B two maintenance domain, its level were 5 and 3, port Ethernet1/0/1 to each device of the Ethernet1/0/4 are VLAN 100, and the maintenance domain maintenance serves the VLAN。

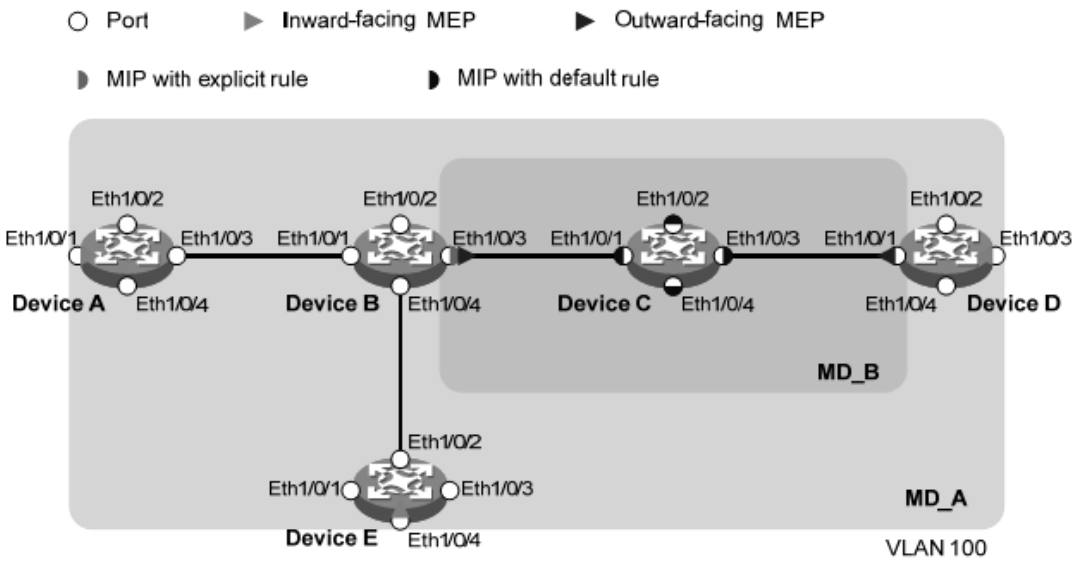
Ethernet1/0/4 Device A Ethernet1/0/1 Device, D Ethernet1/0/3 and Device E MD_A of the boundary ports, and in these ports are configured to maintain the endpoint; the boundary of the MD_B port for Device B Ethernet1/0/3 and Device D Ethernet1/0/1, and in the port configuration maintenance outgoing endpoint。

It is required to plan the MD_A maintenance intermediate point on Device B and configure it only on the port with low-level maintenance endpoints. According to this plan, the maintenance point of MD_A is configured on Device B due to the configuration of MD_B maintenance endpoint on the Device B Ethernet1/0/3, and the rule is created as Explicit rule。

It is required to plan the maintenance intermediate point of MD_B on Device C and configure it on all ports. According to this plan, the maintenance intermediate point of MD_B is configured on Device C, and its creation rule is Default rule。

By using the continuity detection function to detect all MD_A and MD_B in the maintenance of communication between endpoints, to link failures in the detection, the use of a loopback function for fault location; or to the entire network status after obtaining, using link path searching or fault location tracking function。

Network diagram:



Configuration steps:

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Configuring VLAN and ports

VLAN 100 is created on each device and configured ports Ethernet1/0/1 ~ Ethernet1/0/4 belong to VLAN 100。

2）Enable CFM function

Enable CFM function on Device A。

DeviceA> config t

[DeviceA] cfm enable

Device B～Device EThe configuration is similar to that of Device A, and the configuration process is slightly better。

3) Configuration service instance

4) # Create a maintenance domain MD_A with level 5 on Device A, create a maintenance set MA_A for VLAN 100 in MD_A, and create a service instance for MD_A and MA_A 1

[DeviceA] cfm md MD_A level 5

[DeviceA] cfm ma MA_A md MD_A vlan 100

[DeviceA] cfm service-instance 1 md MD_A ma MA_A

The configuration of Device E is similar to that of Device A, and the configuration process is slightly better。

In the Device B to create level 5 maintenance domain MD_A, created in MD_A VLAN 100 maintenance service to set MA_A, and for MD_A and MA_A to create a service instance 1; to create a level 3 maintenance domain MD_B, created in MD_B VLAN 100 maintenance service to set MA_B, and for MD_B and MA_B create a service instance 2。

[DeviceB] cfm md MD_A level 5

[DeviceB] cfm ma MA_A md MD_A vlan 100

[DeviceB] cfm service-instance 1 md MD_A ma MA_A

[DeviceB] cfm md MD_B level 3

[DeviceB] cfm ma MA_B md MD_B vlan 100

[DeviceB] cfm service-instance 2 md MD_B ma MA_B

The configuration of Device D is similar to that of Device B, and the configuration process is slightly better。

Create a maintenance domain MD_B with level 3 on Device C, create a maintenance set MA_B for VLAN 100 in MD_B, and create a service instance for MD_B and MA_B 2

[DeviceC] cfm md MD_B level 3

[DeviceC] cfm ma MA_B md MD_B vlan 100

[DeviceC] cfm service-instance 2 md MD_B ma MA_B

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4) Configuration maintenance endpoint

Create an internal maintenance endpoint 1001 in service instance 1 on the DeviceA port Ethernet1/0/1, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 1001, and then enable the endpoint 1001 to be maintained。

[DeviceA] interface ethernet 1/0/1

[DeviceA-Ethernet1/0/1] cfm mep 1001 service-instance 1 inbound

[DeviceA-Ethernet1/0/1] cfm remote-meplist 4002 5001 service-instance 1 mep 1001

[DeviceA-Ethernet1/0/1] cfm mep service-instance 1 mep 1001 enable

[DeviceA-Ethernet1/0/1] quit

On the DeviceB port Ethernet1/0/3, create the outgoing maintenance endpoint 2 in service instance 2001, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 2001, and then enable the maintenance endpoint 2001。

[DeviceB] interface ethernet 1/0/3

[DeviceB-Ethernet1/0/3] cfm mep 2001 service-instance 2 outbound

[DeviceB-Ethernet1/0/3] cfm remote-meplist 2001 4001 service-instance 2 mep 2001

[DeviceB-Ethernet1/0/3] cfm mep service-instance 2 mep 2001 enable

[DeviceB-Ethernet1/0/3] quit

#On the port Ethernet1/0/1 of Device D, create the outbound maintenance endpoint 2 in service instance 4001, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 4001, and then enable the maintenance endpoint 4001。

Create an internal maintenance endpoint 4002 in the service instance 1 on the port Ethernet1/0/3, and create a 4002 remote maintenance endpoint list at the same time。

[DeviceD] interface ethernet 1/0/1

[DeviceD-Ethernet1/0/1] cfm mep 4001 service-instance 2 outbound

[DeviceD-Ethernet1/0/1] cfm remote-meplist 2001 service-instance 2 mep 4001

[DeviceD-Ethernet1/0/1] cfm mep service-instance 2 mep 4001 enable

[DeviceD-Ethernet1/0/1] quit

[DeviceD] interface ethernet 1/0/3

[DeviceD-Ethernet1/0/3] cfm mep 4002 service-instance 1 inbound

[DeviceD-Ethernet1/0/3] cfm remote-meplist 1001 5001 service-instance 1 mep 4002

[DeviceD-Ethernet1/0/3] cfm mep service-instance 1 mep 4002 enable

[DeviceD-Ethernet1/0/3] quit

#On the port Ethernet1/0/4 of Device E, create and enable the internal maintenance endpoint 1 in the service instance 5001, and configure the remote maintenance endpoint list in the service instance 1。

[DeviceE] interface ethernet 1/0/4

[DeviceE-Ethernet1/0/4] cfm mep 5001 service-instance 1 inbound

SEC.RU | Короткий путь к информации
Скачано с sec.ru

[DeviceE-Ethernet1/0/4] cfm remote-meplist 1001 service-instance 1 mep 5001

[DeviceE-Ethernet1/0/4] cfm mep service-instance 1 mep 5001 enable

[DeviceE-Ethernet1/0/4] quit

5) Configuration maintenance intermediate point

Configuration rules for maintaining intermediate points are configured as Explicit rules in service instance 1 of Device B。

[DeviceB] cfm mip-rule explicit service-instance 1

Configuration rules for maintaining intermediate points are configured as Default rules in service instance 2 of Device C。

[DeviceC] cfm mip-rule default service-instance 2

6) Configuration continuity detection function

On the port Ethernet1/0/1 of Device A, the CCM message sending function of endpoint 1001 is maintained in the enabling service instance 1。

[DeviceA] interface ethernet 1/0/1

[DeviceA-Ethernet1/0/1] cfm cc service-instance 1 mep 1001 enable

[DeviceA-Ethernet1/0/1] quit

On the port Ethernet1/0/3 of Device B, the CCM message sending function of endpoint 2001 is maintained in the enabling service instance 2。

[DeviceB] interface ethernet 1/0/3

[DeviceB-Ethernet1/0/3] cfm cc service-instance 2 mep 2001 enable

[DeviceB-Ethernet1/0/3] quit

On the port Ethernet1/0/1 of Device D, the CCM message sending function of the endpoint 4001 is maintained in the enabling service instance 2, and the CCM message sending function of the maintenance endpoint 4002 in the enabling service instance 1 is enabled on the port Ethernet1/0/3。

[DeviceD] interface ethernet 1/0/1

[DeviceD-Ethernet1/0/1] cfm cc service-instance 2 mep 4001 enable

[DeviceD-Ethernet1/0/1] quit

[DeviceD] interface ethernet 1/0/3

[DeviceD-Ethernet1/0/3] cfm cc service-instance 1 mep 4002 enable

[DeviceD-Ethernet1/0/3] quit

On the port Ethernet1/0/4 of Device E, the CCM message sending function of endpoint 5001 is maintained in the enabling service instance 1。

[DeviceE] interface ethernet 1/0/4

[DeviceE-Ethernet1/0/4] cfm cc service-instance 1 mep 5001 enable

SEC.RU | Короткий путь к информации
Скачано с sec.ru

[DeviceE-Ethernet1/0/4] quit

7) Check configuration effect

When the link fault is detected by the continuity detection function, the loopback function can be used to locate the fault. for example：

Loop back function is enabled on Device A to check the link status of endpoints 1001 to 5001 maintained in service instance 1。[DeviceA] cfm loopback service-instance 1 mep 1001 target-mep 5001

Loopback to 0010-FC00-6512 with the sequence number start from 43404:

Reply from 0010-FC00-6512: sequence number = 43404

Reply from 0010-FC00-6512: sequence number=43405

Reply from 0010-FC00-6512: sequence number=43406

Reply from 0010-FC00-6512: sequence number=43407

Reply from 0010-FC00-6512: sequence number=43408

Send:5 Received:5 Lost:0

After obtaining the whole network state through the continuity detection function, the link tracking function can be used to find the path or locate the fault. for example：

Find the path to maintain endpoints 1001 to 5001 in the service instance 1 of Device A。

[DeviceA] cfm linktrace service-instance 1 mep 1001 target-mep 5001

Linktrace to MEP 5001 with the sequence number 1001-43462

MAC Address	TTL	Last MAC	Relay Action
0010-FC00-6512	63	0010-FC00-6511	Hit
0010-FC00-6511	62	0010-FC00-6510	FDB

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Twenty-seventh chapters

IPv6 basic configuration

switches support basic IPv6 functions, including IPv6 two layer forwarding, IPv6 ND function. This chapter describes how to configure IPv6, including the following：

- IPv6 profile
- IPv6 basic configuration task profile
- Configure IPv6 basic functionality
- Configuring IPv6 neighbor discovery protocol
- IPv6 static routing configuration
- IPv6 display and maintenance

27.1 IPv6 profile

IPv6 (Internet Protocol Version 6, the Internet Protocol version 6) is the second generation standard protocol of network layer protocol, also known as IPng (IP Next Generation, the next generation of the Internet), it is IETF (Internet Engineering Task Force, Internet engineering task force) a set of standardized design, is an upgraded version of IPv4. The most significant difference between IPv6 and IPv4 is that the length of the IP address increases from 32 bits to 128 bits。

27.1.1 The characteristics of IPv6 protocol

1 Simplified message header format

By reducing or moving some fields in the IPv4 header to the extended header, the length of the IPv6 basic message header is reduced. IPv6 uses a fixed length of basic packet header, thus simplifying the forwarding equipment for IPv6 packet processing, and improving the forwarding efficiency. Although the length of the IPv6 address is four times the length of the IPv4 address, the length of the IPv6 basic message header is only 40 bytes, which is two times the length of the IPv4 header (excluding the option field)。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

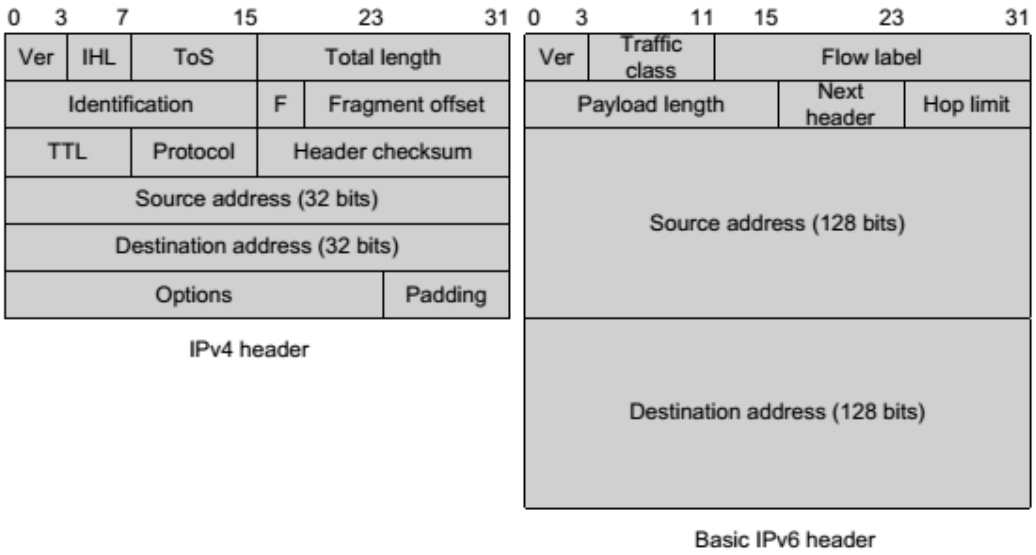


Figure 1-1 comparison of IPv4 header and IPv6 basic message header format

2 Plenty of address space

The source and destination address length of IPv6 is 128 bits (16 bytes). It can provide more than 3.4 * 1038 possible address spaces, fully meet the needs of multi-level address division, and address allocation of private networks within public networks and organizations。

3 Hierarchical address structure

The address space of IPv6 adopts hierarchical address structure, which is beneficial to fast routing lookup, and can effectively reduce the system resource occupied by IPv6 routing table by means of route aggregation。

4 Address auto configuration

In order to simplify host configuration, IPv6 supports stateful address configuration and stateless address configuration：

1) Stateful address configuration refers to obtaining IPv6 addresses and related information from a server (such as a DHCP server)；

2) Stateless address configuration means that the host automatically configures the IPv6 address and related information according to its link layer address and the prefix information issued by the router。

At the same time, the host can also form the link local address according to its own link layer address and default prefix (FE80:: /10) to realize the communication with other hosts on the chain。

5 Built in security

IPv6 uses IPSec as its standard extension head, providing end-to-end security features. This

SEC.RU | Короткий путь к информации
Скачано с sec.ru

feature also provides a standard for solving network security problems, and improves interoperability between different IPv6 applications。

6 Support QoS

The flow label (Flow Label) field of IPv6 header realizes the identification of traffic, and allows the device to identify packets in a traffic and provide special processing。

7 Enhanced neighbor discovery mechanism

IPv6 neighbor discovery protocol by a group of ICMPv6 (Internet Control Message Protocol for IPv6 IPv6, the Internet control message protocol) message, manages the neighbor nodes (i.e., nodes on the same link) information interaction. It replaces ARP (Address Resolution Protocol, address resolution protocol), ICMPv4 router discovery and ICMPv4 redirection message, and provides a series of other functions。

8 Flexible extended headers

IPv6 cancels the option field in the IPv4 header, and introduces a variety of extended headers, which improves the processing efficiency and greatly enhances the flexibility of the IPv6, and provides a good scalability for the IP protocol. The option field in the IPv4 header is at most 40 bytes, while the size of the IPv6 extension header is limited by the size of the IPv6 message。

27.1.2 IPv6 address introduction

1. IPv6 address representation

The IPv6 address is represented as a series of 16 bit sixteen binary numbers separated by colons (:). Each IPv6 address is divided into 8 groups, each of which is represented by 16 bits in 4 sixteen decimal numbers, and groups and groups are separated by colons, such as 2001:0000:130F:0000:0000:09C0:876A:130B。

In order to simplify the representation of IPv6 address, the "0" in IPv6 address can be handled in the following way：

1) The preamble "0" in each group can be omitted, that is, the above address can be written as 2001:0:130F:0:0:9C0:876A:130B。

2) If the address contains a group of two or more consecutive 0, it can be replaced by a double colon ":: "that is, the above address can be written as 2001:0:130F:: 9C0:876A:130B。

note：

Only one double colon can be used in an IPv6 address"::"， Otherwise, when the device transforms ":" to "0" to restore the 128 bit address，It is impossible to determine the number of "0" represented by "::"。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The IPv6 address consists of two parts: address prefix and interface identifier. The address prefix is equivalent to the network number field part in the IPv4 address, and the interface identifier corresponds to the host number part in the IPv4 address。

The address prefix is represented as: IPv6 address / prefix length. Among them, the IPv6 address is any form listed previously, and the prefix length is a decimal number, which represents the leftmost number of the IPv6 address is the address prefix。

2 Address classification of IPv6

There are three types of address in IPv6: unicast address, multicast address and anycast address。

1）Unicast address: used to uniquely identify an interface, similar to the unicast address of IPv4. The data message sent to the unicast address will be transmitted to the interface identified by this address。

2）Multicast address: used to identify a set of interfaces (usually this group of interfaces belonging to different nodes), similar to the multicast address of IPv4. The data packets sent to the multicast address are transmitted to all the interfaces identified by this address。

3）Anycast address: used to identify a set of interfaces (usually, this group of interfaces belong to different nodes). Send any message address multicast data is transmitted a set of interfaces to the address identified in the distance from the source node (recently measured according to the routing protocol using an interface)。

There is no broadcast address in IPv6, and the function of broadcast address is realized by multicast address。

The IPv6 address type is specified by several preceding addresses (called the format prefix), and the corresponding relationship between the main address type and the format prefix is shown in Table 1-1。

Table 1-1 the corresponding relationship between address type and format prefix

3 Unicast address types

There are many types of IPv6 unicast addresses, including global unicast addresses, link local addresses, and site local addresses。

1）Global unicast address is equivalent to IPv4 public address, which is provided to network service provider. This type of address allows aggregation of routing prefixes, thus limiting the number of global routing tables。

2) Link local address is used for neighbor discovery protocol and communication between local upper nodes in stateless automatic configuration. Data packets that use link local address as source or destination address are not forwarded to other links。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3) The local address of the site is similar to the private address in IPv4. The data packets that use the local address of the site as the source or destination address are not forwarded to other sites outside the site (equivalent to a private network)。

4) Loopback address: unicast address 0:0:0:0:0:0:0:1 (simplified as:: 1) is called loopback address, and cannot be assigned to any physical interface. Its function is the same as the loopback address in IPv4, that is, nodes send IPv6 messages to themselves。

5) Unknown address: Address::: called an unspecified address and cannot be assigned to any node. Before the node obtains the valid IPv6 address, it can fill the address in the source address field of the transmitted IPv6 message, but it can not be used as the destination address in the IPv6 message。

4 multicast

The multicast address shown in table 1-2 is reserved for a special purpose multicast address。

Table 1-2 list of reserved IPv6 multicast addresses

In addition, there is a class of multicast address: the requested node (Solicited-Node) address. This address is mainly used to obtain link layer address of neighbor nodes on the same chain and realize duplicate address detection. Each unicast or anycast IPv6 address has a corresponding address of the requested node. Its format is：

FF02:0:0:0:0:1:FFXX:XXXX

Among them, FF02:0:0:0:0:1:FF is 104 bit fixed format; XX:XXXX is the post 24 bit of unicast or anycast IPv6 address。

5 The interface identifier of IEEE EUI-64 format

The interface identifier in the IPv6 unicast address is used to identify a unique interface on the link. At present, the IPv6 unicast address basically requires the interface identifier to be 64 bits. The interface identifier of the IEEE EUI-64 format changes from the link layer address (MAC address) of the interface. The interface identifier in the IPv6 address is 64 bits, and the MAC address is 48 bits. Therefore, it is necessary to insert the sixteen decimal number FFFE (1111111111111110) at the middle position of the MAC address (starting from the twenty-fourth bit after the high position). To ensure that the interface identifier obtained from the MAC address is unique, the Universal/Local (U/L) bit (starting from the high bit) is set to 1 seventh". Finally, the number of groups is used as the interface identifier of the EUI-64 format。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

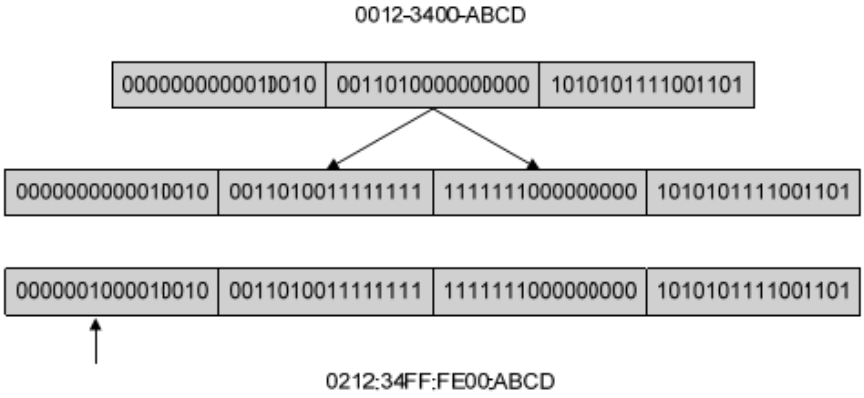


Figure 1-2 conversion process from MAC address to EUI-64 format interface identifier

27.1.3 IPv6 neighbor discovery protocol

IPv6 neighbor discovery protocol using ICMPv6 message five types, some functions to achieve the following: address resolution, verification of neighbors is reachable, duplicate address detection, router discovery / prefix discovery, address auto configuration and redirection.。

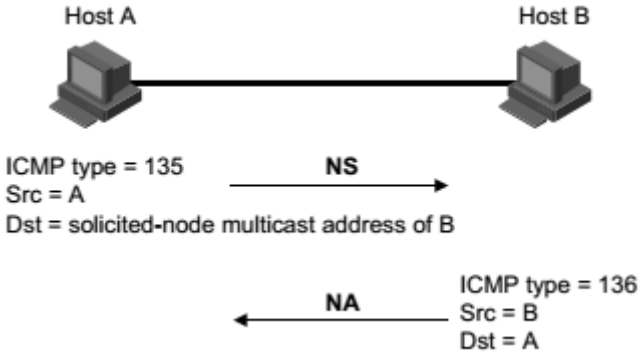
The type and role of ICMPv6 messages used by neighbor discovery protocols are shown in table 1-3。

Table 1-3 the type and role of ICMPv6 messages used in neighbor discovery protocols

The main functions of neighbor discovery protocol are as follows：

1 Address resolution

The link layer address of the neighbor node of the same chain is obtained (the same as the ARP function of IPv4), which is implemented by neighbor request message NS and neighbor notification message NA. As shown in Figure 1-3, node A is required to obtain the link layer address of node B。



Schematic diagram of address resolution in Figure 1-3

(1) Node A sends NS messages in multicast mode. The source address of the NS message is the interface IPv6 address of the node A, and the destination address is the multicast address of the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

requested node of the node B. The message content contains the link layer address of the node A。

(2) After the node B receives the NS message, it determines whether the destination address of the message is the multicast address of the requested node corresponding to its own IPv6 address. If it is, then the node B can learn the link layer address of the node A and return the NA message in unicast mode, which contains its own link layer address。

(3) The node A obtains the link layer address of the node B from the received NA message。

2 Verify whether neighbors are reachable

After obtaining the link layer address of neighbor node, neighbor request message NS and neighbor notification message NA can verify whether neighbor node is reachable or not。

(1) The node sends the NS message, where the destination address is the IPv6 address of the neighbor node。

(2) If the acknowledgement message of neighbor node is received, the neighbor is reachable; otherwise, the neighbor is unreachable。

3 Duplicate address detection

When a node acquires an IPv6 address, it is necessary to use the repeated address detection function to determine whether the address has been used by other nodes (similar to the free ARP function of IPv4). Duplicate address detection can be implemented by NS and NA, as shown in Figure 1-4。

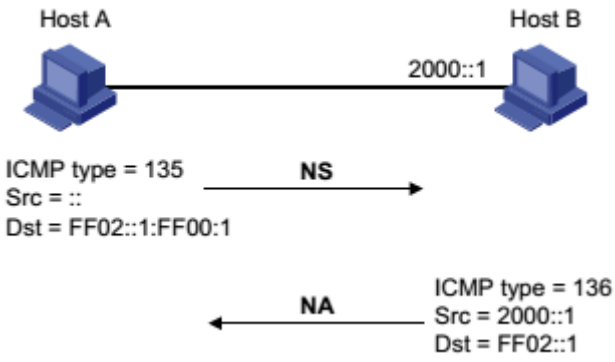


Fig. 1-4 duplicate address detection schematic diagram

(1) The node A sends the NS message, and the source address of the NS message is an unspecified address: the destination address is the multicast address of the requested node corresponding to the IPv6 address to be detected, and the message content contains the IPv6 address to be detected。

(2) If the node B has already used this IPv6 address, the NA message will be returned. It contains its own IPv6 address。

(3) The node A receives the NA message from the node B, and knows that the IPv6 address is already in use. Otherwise, the address is not used, and the node A can use the IPv6 address。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4 Router discovery / prefix discovery and address auto configuration

Router discovery / prefix discovery is that the node obtains the prefix of neighbor router and its network from the received RA message, and other configuration parameters。

Address stateless automatic configuration refers to the node to discover the acquired information according to the router discovery / prefix, and automatically configure the IPv6 address. The router discovery / prefix discovery is implemented through the router request message RS and the router notification message RA, and the specific process is as follows：

(1) When the node starts, it sends a request to the router through the RS message, requesting the prefix and other configuration information for the configuration of the node。

(2) The router returns the RA message, including prefix information options (the router also periodically releases RA messages)。

(3) The node automatically configures the IPv6 address and other information of the interface by using the address prefix and other configuration parameters in the RA message returned by the router。

- Prefix information options include not only the address prefix information, but also the prefix prefix lifetime (preferred lifetime) and valid (life cycle). When a node receives a periodically transmitted RA message, the prefix's preferred lifetime and valid lifetime are updated according to the message。
- In the effective life period, the automatically generated address can be used normally; after the expiration of the valid life period, the address automatically generated will be deleted。

5 Redirection

When the host is started, there may be only one default route to the default gateway in its routing table. When a certain condition is satisfied, the default gateway will send a redirect message to the source host ICMPv6, notify the host select Send follow-up message better next hop (IPv4 and ICMP redirect messages the same function)。

- The ICMPv6 redirection message is sent to the host when the following conditions are met：
- The interface of receiving and forwarding data packets is the same interface；
- The selected route itself has not been created or modified by the ICMPv6 redirection message；
- The selected route is not a default route；
- The forwarding IPv6 data packet does not contain a route extension header。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

27.1.4 IPv6 PMTU discovery

The links that are transmitted from the source to the destination may have different MTU links. In IPv6, when the length of message is greater than MTU of the link, the fragment of the message will be carried out at the source end, thus reducing the processing pressure of the intermediate forwarding device and rationally utilizing the network resources。

The purpose of the PMTU (Path MTU, path MTU) discovery mechanism is to find the smallest MTU on the path from the source end to the destination. The working process of PMTU is shown in Figure 1-5。

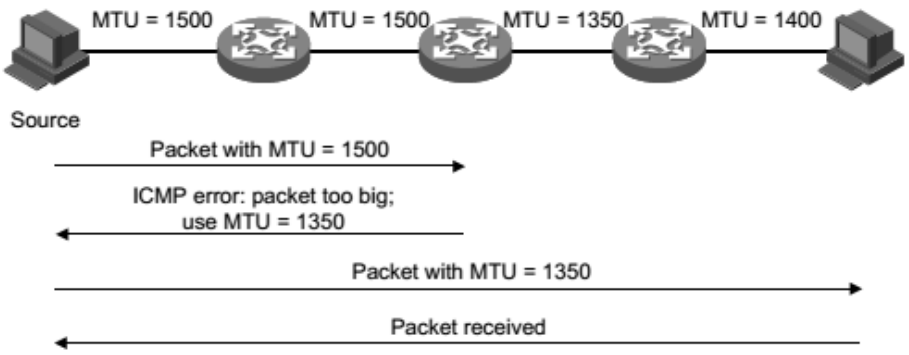


Figure 1-5 PMTU discovery work process

(1) The source host uses its own MTU to segment the message, and then sends the message to the destination host。

(2) The intermediate forwarding device receives the message forwarding, if packet forwarding interface support MTU value is less than the length of message packets are discarded, and the source to return a ICMPv6 error message, including forwarding fails MTU interface。

(3) When the source host receives the error message, it will fragment and send the message by using the MTU carried by the message。

(4) This is repeated until the destination host receives this message, thus determining the minimum MTU of the message from the source end to the destination path。

27.1.5 Protocol specification

The protocol specification related to the IPv6 foundation is available：

- RFC 1881：IPv6 Address Allocation Management
- RFC 1887：An Architecture for IPv6 Unicast Address Allocation
- RFC 1981：Path MTU Discovery for IP version 6
- RFC 2375：IPv6 Multicast Address Assignments
- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- RFC 2461：Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462：IPv6 Stateless Address Autoconfiguration
- RFC 2463：Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6
- (IPv6) Specification
- RFC 2464：Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526：Reserved IPv6 Subnet Anycast Addresses
- RFC 3307：Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513：Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596：DNS Extensions to Support IP Version 6

27.2 IPv6 basic configuration task profile

Configuring the basic functions of IPv6

Configuring IPv6 neighbor discovery protocol

Configuring PMTU discovery

Configuring ICMPv6 message sending

27.3 Configure IPv6 basic functionality

27.3.1Configuring IPv6 unicast address

IPv6 global unicast addresses are manually assigned。

IPv6 link local address is obtained in two ways：

- Automatic generation: when the VLAN port UP, the device automatically generates the link local address for the interface according to the link local address prefix (FE80:: /10) and the link layer address of the interface；
- Manually assigned: user manually configured IPv6 link local address。

command	describe	CLI mode
ipv6 address <ipv6-address>/<prefix-length>	Manually specify the IPv6 address. By default, the local address of the link is automatically generated according to the VLAN interface MAC address under the three layer interface。	Configuration mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru

27.4 Configuring IPv6 neighbor discovery protocol

27.4.1 Configuring the parameters of the RA message

The user can configure the interface whether to send RA messages and send RA messages according to the actual situation, and configure the related parameters in the RA message to notify the host. When the host receives the RA message, we can use these parameters to do the corresponding operation。The parameters and meanings of configurable RA messages are shown in table 1-4。

Table 1-4 parameters and descriptions in RA message

parameter	describe
Cur Hop Limit	When the host sends the IPv6 message, it will fill the Hop Limit field in the IPv6 header with the parameter value. At the same time, the parameter value is also used as the Hop Limit field value in the device reply message。
Prefix Information	When the host on the same link receives the prefix information of the device, it can perform stateless automatic configuration and other operations。
M flag	To determine whether the host uses stateful automatic configuration to obtain the IPv6 address。 If this flag is set to 1, the host will have state through automatic configuration (e.g. DHCP server) to obtain IPv6 address; otherwise, the stateless auto configuration to obtain IPv6 address, IPv6 address is generated according to their link layer address and router prefix information release。
O flag	To determine whether the host uses stateful automatic configuration to obtain additional information other than the IPv6 address。 If you set the other configuration flag is 1, the host will have state through automatic configuration (e.g. DHCP server) to obtain information in addition to other IPv6 address; otherwise, the stateless auto configuration for additional information。
Router Lifetime	The time used to set the router that releases the RA message as the default router for the host. According to the router survival time parameter value in the received RA message, the host can

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	determine whether or not the router that publishes the RA message will be the default router。
Retrans Timer	When the device sends NS messages, the NS message is re sent if the response is not received within the specified time interval。
Reachable Time	When the neighbor unreachability detection to verify that a neighbor, in time up to set, equipment up to that neighbor; exceed the time set, if you need to send messages to neighbors, neighbors will re confirm whether can reach。
Link MTU	The MTU option is used in the RA message to ensure that all nodes on the chain use the same MTU value, which is mainly used in the case that nodes may not know the link MTU. Other Neighbor Discovery messages must be silent and ignore this option。

Configure hop limit

Command：**ipv6 nd cur-hop-limit** *value*

View mode：VLAN interface mode

Default configuration: by default, the number of hops issued by the router is limited to 64 hops

Eliminating the inhibition of RA message publishing

Command：**ipv6 nd send-ra**

View mode：VLAN interface mode

Default configuration: suppresses publication of RA messages by default

Configuring the maximum time interval and minimum time interval for RA message publishing

Command：**ipv6 nd max-ra-interval** *value*

View mode：VLAN interface mode

Default configuration: by default, the maximum time interval for RA message release is 600 seconds

Command：**ipv6 nd min-ra-interval** *value*

View mode：VLAN interface mode

Default configuration: by default, the minimum time interval for issuing RA messages is 198 seconds

note：

- When a RA message is periodically published, the interval between the two adjacent times is

SEC.RU | Короткий путь к информации
Скачано с sec.ru

randomly selected between the maximum time interval and the minimum time interval as the time interval for periodically issuing RA messages。

- The minimum time interval should be less than 0.75 times the maximum time interval。

Configuring prefix information in RA messages

Command： **ipv6 nd prefix** X:X::X:X/M (*valid-lifetime preferred-lifetime* (**off-link** | **no-autoconfig**))

View mode：VLAN interface mode

Default configuration: by default, the prefix information in the RA message is not configured. The IPv6 address of the RA message will be used as the prefix information in the RA message。

Setting the managed address configuration flag bit

Command：**ipv6 nd managed-config-flag**

View mode：VLAN interface mode

Default configuration: by default, the managed address flag is 0, that is, the host automatically obtains the IPv6 address by stateless configuration。

Setting other configuration flag bits

Command：**ipv6 nd other-config-flag**

View mode：VLAN interface mode

Default configuration: by default, other configuration flags are 0, that is, the host automatically obtains other information by stateless configuration。

Configuring router lifetime in RA messages

Command：**ipv6 nd ra-lifetime** *value*

View mode：VLAN interface mode

Default configuration: by default, the lifetime of the router in the RA message is 1800 seconds。

Configuring a neighbor request message retransmission interval

Command：**ipv6 nd base retrans-timer** *value*

View mode：Configuration mode

Default configuration: by default, the time interval for sending NS messages by the interface is 1000 milliseconds。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Configuring retransmission interval of routers in RA messages

Command：**ipv6 nd retrans-timer** *value*

View mode：VLAN interface mode

Default configuration: by default, the value of the Retrans Timer field in the RA message issued by the interface is 0

Configuring the time to keep neighbors reachable

Command：**ipv6 nd base reachable-time** *value*

View mode：Configuration mode

Default configuration: by default, the interface maintains the reachable state of the neighbors for 30000 milliseconds。

Configuring the time to keep neighbors reachable

Command：**ipv6 nd reachable-time** *value*

View mode：VLAN interface mode

Default configuration: by default, the value of the Reachable Timer field in the RA message issued by the interface is 0。

Configuring link MTU size

Command：**ipv6 nd link-mtu** *value*

View mode：VLAN interface mode

Default configuration: by default, the value of the link MTU field in the RA message issued by the interface is 0。

When the source host sends the message from the interface, it will compare the MTU and Link MTU of the interface. If the message length is greater than two, the minimum value is used to segment the message。

27.4.2 The number of sending neighbor request messages when configuring duplicate address detection

Interface IPv6 address after the message is sent to the neighbor request duplicate address detection, if within a specified period of time (by IPv6 nd retrans-timer configuration command) did not receive a response, then continue to send the request information, when sending the number reached number set, has not yet received a response, the address available。

SEC.RU | Короткий путь к информации
Скачано с sec.ru

command	describe	CLI mode
ipv6 nd dad attempts <value>	By default, the number of neighbor requests sent by repeated address detection is 1, and when the value value is 0, it indicates the forbidden duplicate address detection。	Configuration mode

27.5 IPv6 static routing configuration

command	describe	CLI mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Configuring IPv6 static routing。	Configuration mode

27.6 IPv6 display and maintenance

After completing the above configuration, executing the show command in the privileged view can display the operation of the IPv6 after configuration, and verify the configuration effect by checking the display information。

command	describe	CLI mode
show ipv6 ndp nc	Display neighbor information。	Privileged mode
show ipv6 interface (<ifName>) brief	Display the IPv6 information that can configure the IPv6 address interface	Privileged mode
show ipv6 route (database)	Display IPv6 routing	Privileged mode

SEC.RU | Короткий путь к информации
Скачано с sec.ru