BeWARD
SAFETY & SECURITY

COMMAND GUIDE

8-Port 10/100/1000T 802/3at PoE +

2-Port 100/1000X SFP Wall-mount Managed Switch (-40~75°C)

- **STWP-0802HP**
- **STWP-01602HP**

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Trademarks

Copyright © BEWARD Technology Corp. 2026.
Contents are subject to revision without prior notice.
BEWARD is a registered trademark of BEWARD Technology Corp. All other trademarks belong to their respective owners.

Disclaimer

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

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

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

FCC Warning

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

CE Mark Warning

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

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy savings, please remove the power cable to disconnect the device from the power circuit. Without removing the power cable, the device will still consume power from the power source. In view of Saving the Energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power cable from the device if this device is not intended to be active.

WEEE Warning

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

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

Contents

Chapter 1 COMMAND LINE INTERFACE 13

1.1 Accessing the CLI 13

1.2 Command Line Modes 13

1.3 Command Help 14

1.4 Command Line Editing 15

1.5 Requirements 15

Chapter 2 TELNET CLI MANAGEMENT 17

2.1 Telnet Login 17

Chapter 3 Commands for CLI Configuration 18

3.1 802.1x 18

3.1.1 dot1x 18

3.1.2 dot1x authentication 19

3.1.3 dot1x reauthentication 20

3.1.4 dot1x timeout reauth-period 21

3.1.5 dot1x timeout quiet-period 22

3.1.6 dot1x timeout supp-timeout 23

3.1.7 dot1x max-req 24

3.1.8 dot1x guest-vlan 25

3.1.9 dot1x guest-vlan 26

3.1.10 show dot1x 29

3.1.11 show dot1x authenticated-hosts 29

3.1.12 show dot1x interface 30

3.1.13 show dot1x guest-vlan 30

3.2 AAA 31

3.2.1 aaa authentication 31

3.2.2 login authentication 33

3.2.3 ip http login authentication 35

3.2.4 enable authentication 37

3.2.5 show aaa authentication 38

3.2.6 show line lists 39

3.2.7 tacacs default-config 40

3.2.8 tacacs host 41

3.2.9 show tacacs default-config 42

3.2.10 show tacacs 42

3.2.11 radius default-config 43

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

3.2.12 radius host 44
3.2.13 show radius default-config 45
3.2.14 show radius 45
3.3 ACL 47
3.3.1 mac acl 47
3.3.2 permit (MAC) 47
3.3.3 deny (MAC) 48
3.3.4 ip acl 50
3.3.5 permit (IP) 50
3.3.6 deny (IP) 52
3.3.7 ipv6 acl 55
3.3.8 permit (IPv6) 55
3.3.9 deny (IPv6) 57
3.3.10 bind acl 59
3.3.11 show acl utilization 60
3.4 Administration 62
3.4.1 enable 62
3.4.2 exit 63
3.4.3 configure 63
3.4.4 interface 64
3.4.5 line 65
3.4.6 end 65
3.4.7 reboot 66
3.4.8 system name 67
3.4.9 system contact 67
3.4.10 system location 68
3.4.11 username 69
3.4.12 enable password 70
3.4.13 ip address 71
3.4.14 ip default-gateway 72
3.4.15 ip dns 73
3.4.16 ip dhcp 73
3.4.17 ipv6 autoconfig 74
3.4.18 ipv6 address 75
3.4.19 ipv6 default-gateway 76
3.4.20 ipv6 dhcp 77
3.4.21 ip service 77
3.4.22 ip session-timeout 78
3.4.23 exec-timeout 79

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

3.4.24 password-thresh 80
3.4.25 silent-time 82
3.4.26 history 83
3.4.27 clear service 85
3.4.28 ssl 85
3.4.29 ping 86
3.4.30 traceroute 86
3.4.31 clear arp 87
3.4.32 show version 88
3.4.33 show info 88
3.4.34 show history 89
3.4.35 show username 90
3.4.36 show ip 91
3.4.37 show ip dhcp 91
3.4.38 show ipv6 92
3.4.39 show ipv6 dhcp 92
3.4.40 show line 93
3.5 Cable Diagnostics 94
3.5.1 show cable-diag interface 94
3.6 DHCP Snooping 95
3.6.1 Ip dhcp snooping 95
3.6.2 ip dhcp snooping vlan 95
3.6.3 ip dhcp snooping trust 96
3.6.4 ip dhcp snooping verify 97
3.6.5 ip dhcp snooping limit rate 98
3.6.6 clear ip dhcp snooping statistics 98
3.6.7 show ip dhcp snooping 99
3.6.8 show ip dhcp snooping interface 100
3.6.9 show ip dhcp snooping binding 100
3.6.10 ip dhcp snooping option 101
3.6.11 ip dhcp snooping option action 102
3.6.12 ip dhcp snooping option circuit-id 102
3.6.13 ip dhcp snooping option remote-id 103
3.6.14 show ip dhcp snooping option 104
3.6.15 ip dhcp snooping database 105
3.6.16 ip dhcp snooping database write-deley 106
3.6.17 ip dhcp snooping database timeout 107
3.6.18 clear ip dhcp snooping database statistics 108
3.6.19 renew ip dhcp snooping database 109

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

3.6.20 show ip dhcp snooping database 110
3.7 DoS 110
3.7.1 dos 110
3.7.2 port dos 113
3.7.3 ip gratuitous-arps 114
3.7.4 show dos 115
3.8 Dynamic ARP Inspection 116
3.8.1 ip arp inspection 116
3.8.2 ip arp inspection vlan 116
3.8.3 ip arp inspection trust 117
3.8.4 ip arp inspection validate 118
3.8.5 ip arp inspection rate-limit 119
3.8.6 clear ip arp inspection statistics 120
3.8.7 show ip arp inspection 121
3.8.8 show ip arp inspection interface 121
3.9 GVRP 123
3.9.1 gvrp 123
3.9.2 gvrp (port) 123
3.9.3 gvrp port registration mode 124
3.9.4 gvrp port creation vlan forbidden 125
3.9.5 clear gvrp statistics 125
3.9.6 show gvrp statistics 126
3.9.7 show gvrp 127
3.9.8 show gvrp port configuration 128
3.10 IGMP Snooping 129
3.10.1 Ip igmp snooping 129
3.10.2 ip igmp snooping report-suppression 129
3.10.3 ip igmp snooping version 130
3.10.4 ip igmp snooping unknown-multicast action 131
3.10.5 ip igmp snooping forward-method 132
3.10.6 ip igmp snooping querier 133
3.10.7 ip igmp snooping vlan 134
3.10.8 ip igmp snooping vlan parameters 135
3.10.9 ip igmp snooping static port 137
3.10.10 ip igmp snooping vlan static router port 138
3.10.11 ip igmp snooping static group 139
3.10.12 ip igmp profile 141
3.10.13 ip igmp filter 142
3.10.14 ip igmp max-group 143

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

3.10.15 clear ip igmp snooping groups 144
3.10.16 clear ip igmp snooping statistics 145
3.10.17 show ip igmp snooping counters 145
3.10.18 show ip igmp snooping groups 146
3.10.19 show ip igmp snooping router 146
3.10.20 show ip igmp snooping querier 147
3.10.21 show ip igmp snooping 148
3.10.22 show ip igmp snooping vlan 149
3.10.23 show ip igmp snooping forward-all 150
3.10.24 show ip igmp profile 150
3.10.25 show ip igmp port filter 151
3.10.26 show ip igmp port max-group 152
3.10.27 show ip igmp port max-group action 152
3.11 IP Source Guard 154
3.11.1 ip source verify 154
3.11.2 ip source binding 154
3.11.3 show ip source interface 155
3.11.4 show ip source binding 156
3.12 Link Aggregation 156
3.12.1 lag load-balance 156
3.12.2 lacp system-priority 157
3.12.3 lacp port-priority 158
3.12.4 lacp timeout 159
3.12.5 lag 159
3.12.6 show lag 160
3.13 LLDP 162
3.13.1 lldp 162
3.13.2 lldp tx-interval 162
3.13.3 lldp reinit-delay 163
3.13.4 lldp holdtime-multiplier 164
3.13.5 lldp tx-delay 165
3.13.6 lldp tlv-select 166
3.13.7 lldp tlv-select pvid 167
3.13.8 lldp tlv-select vlan-name 168
3.13.9 lldp lldpdu 170
3.13.10 lldp tx/rx 171
3.13.11 lldp med 172
3.13.12 lldp med tlv-select 173
3.13.13 lldp med fast-start-report-count 174

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

3.13.14 lldp med network-policy 174
3.13.15 lldp med network-policy add | remove 176
3.13.16 lldp med network-policy auto 177
3.13.17 lldp med location 178
3.13.18 show lldp 179
3.13.19 show lldp local-device 180
3.13.20 show lldp neighbor 182
3.13.21 show lldp med 184
3.13.22 show lldp statistics 186
3.13.23 show lldp tlv-overloading 188
3.14 Logging 190
3.14.1 logging 190
3.14.2 logging flash | buffered 191
3.14.3 logging host 192
3.14.4 show logging 194
3.14.5 show logging flash | buffered 195
3.14.6 clear logging flash | buffered 196
3.15 MAC Address Table 197
3.15.1 clear mac address-table 197
3.15.2 mac address-table aging-time 197
3.15.3 mac address-table static 198
3.15.4 mac address-table static drop 199
3.15.5 show mac address-table 200
3.15.6 show mac address-table counters 201
3.15.7 show mac address-table aging-time 201
3.16 Mirror 202
3.16.1 mirror session 202
3.16.2 show mirror 203
3.17 MLD Snooping 205
3.17.1 ipv6 mld snooping 205
3.17.2 ipv6 mld snooping report-suppression 206
3.17.3 ipv6 mld snooping version 206
3.17.4 ipv6 mld snooping vlan 207
3.17.5 ipv6 mld snooping vlan parameters 209
3.17.6 ipv6 mld snooping vlan static-port 210
3.17.7 ipv6 mld snooping vlan static-router-port 211
3.17.8 ipv6 mld snooping vlan static-group 212
3.17.9 ipv6 mld profile 213
3.17.10 ipv6 mld filter 215

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

3.17.11 ipv6 mld max-groups 216
3.17.12 clear ipv6 mld snooping groups 217
3.17.13 clear ipv6 mld snooping statistics 217
3.17.14 show ipv6 mld snooping groups counters 218
3.17.15 show ipv6 mld snooping groups 219
3.17.16 show ipv6 mld snooping router 219
3.17.17 show ipv6 mld snooping 220
3.17.18 show ipv6 mld snooping vlan 221
3.17.19 show ipv6 mld snooping forward-all 222
3.17.20 show ipv6 mld profile 222
3.17.21 show ipv6 mld filter 223
3.17.22 show ipv6 mld max-group 224
3.17.23 show ipv6 mld max-group action 224
3.18 Port Security 226
3.18.1 port-security 226
3.18.2 port-security address-limit 226
3.18.3 show port-security 227
3.19 Port Error Disable 229
3.19.1 errdisable recovery cause 229
3.19.2 errdisable recovery interval 230
3.19.3 show errdisable recovery 231
3.20 Port 233
3.20.1 description 233
3.20.2 speed 234
3.20.3 duplex 235
3.20.4 flow-control 235
3.20.5 shutdown 237
3.20.6 jumbo-frame 237
3.20.7 protected 238
3.20.8 eee 239
3.20.9 clear interface 240
3.20.10 show interface 241
3.21 QoS 243
3.21.1 qos 243
3.21.2 qos trust 244
3.21.3 qos map 245
3.21.4 qos queue 248
3.21.5 qos cos 249
3.21.6 qos trust 250

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

3.21.7 qos remark 251
3.21.8 show qos 252
3.21.9 show qos map 252
3.21.10 show qos interface 254
3.22 Rate Limit 255
3.22.1 rate limit 255
3.22.2 rate limit (interface) 255
3.23 RMON 257
3.23.1 Rmon event 257
3.23.2 Rmon alarm 258
3.23.3 rmon history 260
3.23.4 clear rmon interfaces statistics 261
3.23.5 show rmon event 262
3.23.6 show rmon event log 263
3.23.7 show rmon alarm 264
3.23.8 show rmon history 264
3.23.9 show rmon history statistics 265
3.24 SNMP 267
3.24.1 snmp 267
3.24.2 snmp trap 267
3.24.3 snmp view 268
3.24.4 snmp access group 269
3.24.5 snmp community 270
3.24.6 snmp user 271
3.24.7 snmp engineID 272
3.24.8 snmp host 273
3.24.9 show snmp 274
3.24.10 show snmp trap 275
3.24.11 show snmp view 275
3.24.12 show snmp group 275
3.24.13 show snmp community 276
3.24.14 show snmp host 276
3.24.15 show snmp user 277
3.24.16 show snmp engineid 277
3.25 Storm Control 278
3.25.1 Storm-control unit 278
3.25.2 storm-control ifg 279
3.25.3 storm-control 279
3.25.4 storm-control action 281

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

3.25.5 show storm-control 282
3.26 Spanning Tree 283
3.26.1 spanning-tree 283
3.26.2 spanning-tree bpdu 284
3.26.3 spanning-tree mode 284
3.26.4 spanning-tree priority 285
3.26.5 spanning-tree hello-time 286
3.26.6 spanning-tree max-hops 287
3.26.7 spanning-tree forward-delay 288
3.26.8 spanning-tree maximum-age 288
3.26.9 spanning-tree tx-hold-count 289
3.26.10 spanning-tree pathcost method 290
3.26.11 spanning-tree port-priority 290
3.26.12 spanning-tree cost 291
3.26.13 spanning-tree edge 291
3.26.14 spanning-tree bpdu-filter 292
3.26.15 spanning-tree bpdu-guard 293
3.26.16 spanning-tree link-type 293
3.26.17 spanning-tree mst configuration 294
3.26.18 spanning-tree mst priority 295
3.26.19 spanning-tree mst cost 296
3.26.20 spanning-tree mst port-priority 296
3.27 System File 298
3.27.1 boot system 298
3.27.2 save 299
3.27.3 copy 299
3.27.4 delete 301
3.27.5 restore-default 302
3.27.6 show config 302
3.27.7 show flash 303
3.28 Time 304
3.28.1 clock set 304
3.28.2 clock timezone 304
3.28.3 clock source 305
3.28.4 clock summer-time 306
3.28.5 show clock 308
3.28.6 sntp 308
3.28.7 show sntp 309
3.29 VLAN 311

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

3.29.1 vlan 311
3.29.2 vlan name 311
3.29.3 switchport mode 312
3.29.4 switchport hybrid pvid 312
3.29.5 switchport hybrid ingress-filtering 313
3.29.6 switchport hybrid acceptable-frame-type 314
3.29.7 switchport hybrid allowed vlan add 314
3.29.8 switchport hybrid allowed vlan remove 315
3.29.9 switchport access vlan 316
3.29.10 switchport tunnel vlan 316
3.29.11 switchport trunk native vlan 317
3.29.12 switchport trunk allowed vlan 317
3.29.13 switchport default-vlan tagged 318
3.29.14 switchport forbidden default-vlan 318
3.29.15 switchport forbidden vlan 319
3.29.16 management-vlan 320
3.29.17 show management-vlan 320
3.29.18 protocol-vlan group 321
3.29.19 protocol vlan binding 322
3.29.20 show protocol vlan group 322
3.29.21 show protocol vlan interfaces 323
3.30 Voice VLAN 325
3.30.1 voice vlan 325
3.30.2 voice vlan id 325
3.30.3 voice vlan oui-table 326
3.30.4 voice vlan cos 326
3.30.5 voice vlan aging-time 327
3.30.6 voice vlan cos mode 328
3.30.7 voice vlan enable 328
3.30.8 show voice vlan 329

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

Chapter 1 COMMAND LINE INTERFACE

1.1 Accessing the CLI

When accessing the management interface for the switch via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

1.2 Command Line Modes

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes is described below. Each of the command modes supports specific software commands.

Mode-based Command Hierarchy

The **Command Line Interface (CLI)** groups all the commands in appropriate modes by the nature of the commands. Examples of the CLI command modes are described below. Each of the command modes supports specific switch's commands.

The CLI Command Modes table captures the command modes; the prompts are visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Previous Mode
User Mode	This is the first level of access. Perform basic tasks and list system information.	**COMMAND>**	Enter Logout command
Privileged Mode	From the User Mode, enter the enable command.	**Switch#**	To exit to the User Mode, enter exit or Logout.
Global Config Mode	From the Privileged Mode, enter the configuration command.	**Switch (Config)#**	To exit to the Privileged Mode, enter the exit command.
Interface Config Mode	From the Global Config mode, enter the interface <port#> command.	**Switch (config-if)#**	To exit to the Global Config mode, enter exit.

Table 4-1 CLI Command Modes

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

The CLI is divided into various modes. The commands in one mode are not available until the operator switches to that particular mode. The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, and displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

■ User Mode

When the operator logs into the CLI, the User Mode is the initial mode. The User Mode contains a limited set of commands. The command prompt shown at this level is:

Command Prompt: switch>

■ Privileged Mode

To have access to the full suite of commands, the operator must enter the Privileged Mode. The Privileged Mode requires password authentication. From Privileged Mode, the operator can issue any Exec command to enter the Global Configuration mode. The command prompt shown at this level is:

Command Prompt: switch#

■ Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the Interface Configuration mode. The command prompt at this level is:

Command Prompt: switch(Config)#

From the Global Config mode, the operator may enter the following configuration modes:

■ Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface. In this mode, a physical port is set up for a specific logical connection operation. The command prompt at this level is:

Command Prompt: Switch(config-if)#

1.3 Command Help

To enter ? at any command mode, and the CLI will return possible commands at that point, along with some description of the keywords:

Switch(config)# **copy tftp ?**

running-config Running configurations

startup-config Startup configurations

firmware Runtime firmware image

To use the <Tab> key to do keyword auto completion:

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

Switch(config)# **copy tftp r<Tab>**

Switch(config)# **copy tftp running-config**

You do not need to type in the entire commands; you only need to type in enough characters for the CLI to recognize the command as unique. The following example shows you how to enter the show running-config command:

Switch(config)# **sh ru**

Note: If you want to stop displaying the information, press key "**q**" to escape.

1.4 Command Line Editing

Before you press <Enter>, the current command line can be edited using special keys including arrows and <Ctrl> keys. The following table describes the special keys and their function supported by the CLI:

Keys	Function
<Ctrl>-B; ←	Moves the cursor back one character
<Ctrl>-D	Deletes the character at the cursor
<Ctrl>-E	Jumps to the end of the current command line
<Ctrl>-F; →	Moves the cursor forward one character
<Ctrl>-K	Deletes from the cursor to the end of the command line
<Ctrl>-N; ↓	Enters the next command line in the command history
<Ctrl>-P; ↑	Enters the previous command line in the command history
<Ctrl>-U	Deletes from the cursor to the beginning of the command line
<Ctrl>-W	Deletes the last word typed
<Esc> B	Moves the cursor backward one word
<Esc> D	Deletes from the cursor to the end of the word
<Esc> F	Moves the cursor forward one word
<Backspace>	Delete the character before the cursor
<Del>	Delete the character at the cursor

1.5 Requirements

- **Workstations** running Windows XP/2003/Vista/7/8/10/2008/10/11, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- **Serial Port** Connection (Terminal)
  - The above Workstations come with **COM Port** (DB9) or **USB-to-RS-232** converter.

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

- The above Workstations have been installed with **terminal emulator**, such as Hyper Terminal included in Windows XP/2003.

- **Ethernet Port** Connection
  - Network cables -- Use standard network (UTP) cables with RJ-45 connectors.
  - The above PC is installed with Web browser and JAVA runtime environment plug-in.

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

Chapter 2 TELNET CLI MANAGEMENT

2.1 Telnet Login

The Managed Switch supports telnet for remote management. The switch asks for user name and password for remote login when using telnet; please use **"admin"** for both username and password.

Default IP address: **192.168.0.100**
Username: **admin**
Password: **admin**

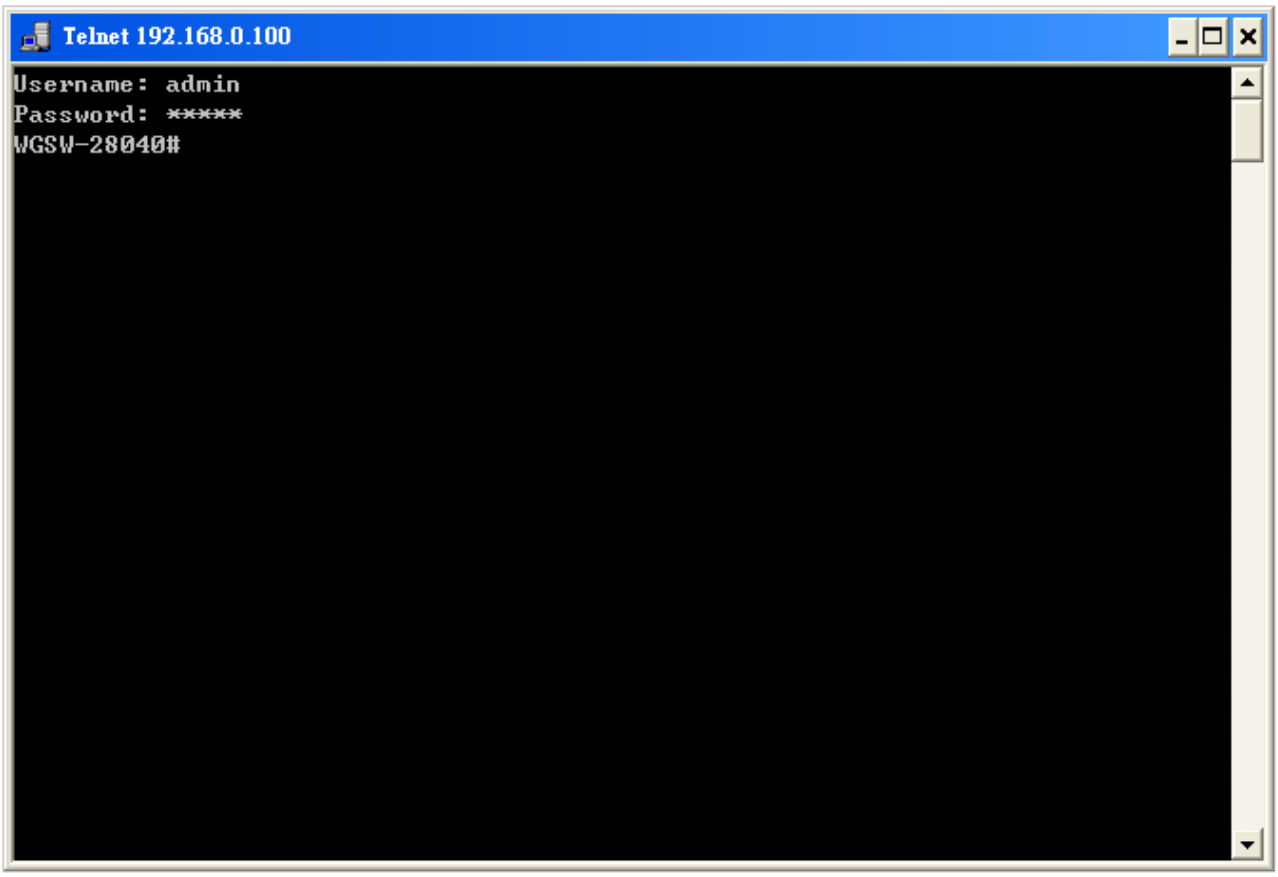

Figure 4-1 Managed Switch Telnet Login Screen

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

Chapter 3 Commands for CLI Configuration

3.1 802.1x

3.1.1 dot1x

Command:

```
dot1x

no dot1x
```

Default:

Default is disabled

Mode:

Global Configuration

Usage Guide:

The "**dot1x**" command enables the global setting of IEEE 802.1X port-based network access control. Only when it is enabled, can the port-based setting work.

Use the **no** form of this command to disable

Example:

The following example shows how to enable 802.1X access control on port 1.

```
Switch(config)# dot1x
switch(config)# interface gi1
switch(config-if)# dot1x auto
switch(config-if)# exit
switch(config)# show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+---------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.2 dot1x authentication

Command:

```
dot1x (auto|force-auth|force-unauth)

no dot1x
```

Parameter:

auto	Port control will depend on the outcome of authentication.
force-auth	Force this port to be unconditional authorized.
force-unauth	Force this port to be unconditional unauthorized.

Default:

Default is disabled

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x**" command to enable 802.1X function on port. Use the **no** form of this command to disable this function.

The enable of 802.1X global setting is a must

Example:

The following example shows how to enable 802.1X access control on port 1.

```
Switch(config)# dot1x
switch(config)# interface gi1
switch(config-if)# dot1x auto
switch(config-if)# exit
switch(config)# show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+---------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.3 dot1x reauthentication

Command:

```
dot1x reauth

no dot1x reauth
```

Default:

Default is disabled

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x reauth**" command to enable 802.1X periodical reauthentication function on port. Use the **no** form of this command to disable this function.

Example:

The following example shows how to enable 802.1X access control on port 1.

```
switch(config)# interface gi1
switch(config-if)# dot1x reauth
switch(config-if)# exit
switch(config)# show dot1x
802.1x protocol is: Enabled
802.1x protocol version: 2
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+--------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Seconds
Supplicant Timeout: 30 Seconds
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.4 dot1x timeout reauth-period

Command:

```
dot1x timeout reauth-period <30-65535>

no dot1x timeout reauth-period
```

Parameter:

<30-65535>	Specify the re-authentication period.

Default:

3600 seconds

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x timeout reauth-period**" command to configure the re-authentication period. Use the **no** form of this command to restore the period to default value.

Example:

The example shows how to configure re-authentication period to 300 sec. on port 1.

```
switch(config)# interface gi1
switch(config-if)# dot1x timeout reauth-period 300
switch(config-if)# exit
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+--------------------+-----------------
gi1 Authentication | Initialize | Enabled | 300
Quiet Period: 60 Seconds
Supplicant Timeout: 30 Seconds
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.5 dot1x timeout quiet-period

Command:

```
dot1x timeout quiet-period <0-65535>

no dot1x timeout quite-period
```

Parameter:

<0-65535>	Specify the quiet period.

Default:

36 seconds

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x timeout quiet-period**" command to configure the quiet period. Use the **no** form of this command to restore the period to default value.

Example:

The example shows how to configure quiet period to 300 sec. on port 1.

```
switch(config)# interface gi1
switch(config-if)# dot1x timeout quite-period 300
switch(config-if)# exit
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+--------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 300 Seconds
Supplicant Timeout: 30 Seconds
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.6 dot1x timeout supp-timeout

Command:

```
dot1x timeout supp-timeout <1-65535>

no dot1x timeout supp-timeout
```

Parameter:

<1-65535>	Specify the supplicant period.

Default:

30 seconds

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x timeout supp-timeout**" command to configure the supplicant period. Use the **no** form of this command to restore the period to default value.

Example:

The example shows how to configure supplicant period to 300 sec. on port 1.

```
switch(config)# interface gi1
switch(config-if)# dot1x timeout supp-timeout 300
switch(config-if)# exit
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+--------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Seconds
Supplicant Timeout: 300 Seconds
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.7 dot1x max-req

Command:

```
dot1x max-req <1-10>

no dot1x max-req
```

Parameter:

<1-10>	Specify the maximum request retries.

Default:

2 times

Mode:

Interface Configuration

Usage Guide:

Use the "**dot1x max-req"** command to configure the maximum request retries. Use the **no** form of this command to restore the period to default value.

Example:

The example shows how to configure maximum request retries to 4 times on port 1.

```
switch(config)# interface gi1
switch(config-if)# dot1x max-req 4
switch(config-if)# exit
switch(config)# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+---------------------+-----------------
gi1 Authentication | Initialize | Enabled | 3600
Quiet Period: 60 Seconds
Supplicant Timeout: 30 Seconds
Max req: 4
Session Time (HH:MM:SS): 0: 0: 0: 0
```


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

3.1.8 dot1x guest-vlan

Command:

```
dot1x guest-vlan <1-4094>

no dot1x guest-vlan
```

Parameter:

<1-4094>	Specify VLAN ID to enable 802.1X guest VLAN.

Default:

Default is disabled

Mode:

Global Configuration

Usage Guide:

Use the **dot1x guest-vlan** command to globally enable guest VLAN function. Use the **no** form of this command to disable guest VLAN function.

For a port to become a member of guest VLAN after authentication fail, you should also enable guest VLAN on that port.

Example:

The example shows how to configure VLAN 2 as guest VLAN and enable guest VLAN on port 1.

```
switch(config)# dot1x guest-vlan 2
switch(config)# interface gi1
switch(config-if)# dot1x auto
switch(config-if)# dot1x guest-vlan
switch(config-if)# exit
switch(config)# show dot1x guest-vlan
Guest VLAN ID: 2
Port | Guest VLAN | In Guest VLAN
-------+------------+---------------
gi1 | Enabled | No
gi2 | Disabled | ---
gi3 | Disabled | ---
gi4 | Disabled | ---
gi5 | Disabled | ---
gi6 | Disabled | ---
gi7 | Disabled | ---
gi8 | Disabled | ---
```


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

```
gi9 | Disabled | ---
gi10 | Disabled | ---
gi11 | Disabled | ---
gi12 | Disabled | ---
gi13 | Disabled | ---
gi14 | Disabled | ---
gi15 | Disabled | ---
gi16 | Disabled | ---
gi17 | Disabled | ---
gi18 | Disabled | ---
gi19 | Disabled | ---
gi20 | Disabled | ---
gi21 | Disabled | ---
gi22 | Disabled | ---
gi23 | Disabled | ---
gi24 | Disabled | ---
gi25 | Disabled | ---
gi26 | Disabled | ---
gi27 | Disabled | ---
gi28 | Disabled | ---
```

3.1.9 dot1x guest-vlan

Command:

```
dot1x guest-vlan <1-4094>

no dot1x guest-vlan
```

Parameter:

<1-4094>	Specify VLAN ID to enable 802.1X guest VLAN.

Default:

Default is disabled

Mode:

Interface Configuration

Usage Guide:

Use the **dot1x guest-vlan** command to enable guest VLAN function on a port. Use the **no** form of this command to

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

disable guest VLAN function.

For a port to become a member of guest VLAN after authentication fail, you should also globally enable guest VLAN.

Example:

The example shows how to configure VLAN 2 as guest VLAN and enable guest VLAN on port 1.

```
switch(config)# dot1x guest-vlan 2 enable
switch(config)# interface gi1
switch(config-if)# dot1x auto
switch(config-if)# dot1x guest-vlan
switch(config-if)# exit
switch(config)# show dot1x guest-vlan
Guest VLAN ID: 2
Port | Guest VLAN | In Guest VLAN
-------+------------+---------------
gi1 | Enabled | No
gi2 | Disabled | ---
gi3 | Disabled | ---
gi4 | Disabled | ---
gi5 | Disabled | ---
gi6 | Disabled | ---
gi7 | Disabled | ---
gi8 | Disabled | ---
gi9 | Disabled | ---
gi10 | Disabled | ---
gi11 | Disabled | ---
gi12 | Disabled | ---
gi13 | Disabled | ---
gi14 | Disabled | ---
gi15 | Disabled | ---
gi16 | Disabled | ---
gi17 | Disabled | ---
gi18 | Disabled | ---
gi19 | Disabled | ---
gi20 | Disabled | ---
gi21 | Disabled | ---
gi22 | Disabled | ---
gi23 | Disabled | ---
gi24 | Disabled | ---
gi25 | Disabled | ---
```


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

```
gi26 | Disabled | ---
gi27 | Disabled | ---
gi28 | Disabled | ---
```


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

3.1.10 show dot1x

Command:

```
show dot1x
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show dot1x**" command to show dot1x enabling status.

Example:

This example shows how to show the dot1x enabling status.

```
Switch# show dot1x
802.1x protocol is: Disabled
802.1x protocol version: 2
```

3.1.11 show dot1x authenticated-hosts

Command:

```
show dot1x auth-hosts
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show dot1x auth-hosts**" command to show all dot1x authorized hosts.

Example:

This example shows how to show the dot1x authorized hosts.

```
Switch# show dot1x auth-hosts
User Name | Port | Session Time | Authentication Method | MAC Address
------------+-------+----------------+-----------------------+-------------
8389_1 | GE3 | 0: 0: 0:20 | Remote | 00:30:4F:D5:5C:19
```


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

3.1.12 show dot1x interface

Command:

```
show dot1x interface IF_PORTS
```

Parameter:

IF_PORTS	Select port to show dot1x configurations.

Mode:

Privileged EXEC

Usage Guide:

Use "**show dot1x interfaces**" command to show dot1x information of the specified port.

Example:

This example shows how to show dot1x configurations on interface gi1.

```
Switch# show dot1x interfaces gi1
Port | Mode | Current State | Reauth Control | Reauth Period
--------+--------------------+----------------------+-----------------+--------------
gi1 | 802.1X Disabled | - | Enabled | 3600
Quiet Period: 60 Second
Supplicant timeout: 30 Second
Max req: 2
Session Time (HH:MM:SS): 0: 0: 0: 0
```

3.1.13 show dot1x guest-vlan

Command:

```
show dot1x guest-vlan
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show dot1x guest-vlan**" command to show dot1x guest-vlan status.

Example:

This example shows how to show the dot1x guest-vlan status.

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

```
Switch# show dot1x guest-vlan
Guest VLAN ID: 2
Port | Guest VLAN | In Guest VLAN
-------+------------+---------------
gi1 | Enabled | No
gi2 | Disabled | ---
gi3 | Disabled | ---
gi4 | Disabled | ---
gi5 | Disabled | ---
gi6 | Disabled | ---
gi7 | Disabled | ---
gi8 | Disabled | ---
gi9 | Disabled | ---
gi10 | Disabled | ---
gi11 | Disabled | ---
gi12 | Disabled | ---
gi13 | Disabled | ---
gi14 | Disabled | ---
gi15 | Disabled | ---
gi16 | Disabled | ---
gi17 | Disabled | ---
gi18 | Disabled | ---
gi19 | Disabled | ---
gi20 | Disabled | ---
gi21 | Disabled | ---
gi22 | Disabled | ---
gi23 | Disabled | ---
gi24 | Disabled | ---
gi25 | Disabled | ---
gi26 | Disabled | ---
gi27 | Disabled | ---
gi28 | Disabled | ---
```

3.2 AAA

3.2.1 aaa authentication

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

Command:

```
aaa authentication (login | enable) (default | LISTNAME) METHODLIST
[METHODLIST] [METHODLIST] [METHODLIST]

no aaa authentication (login | enable) LISTNAME
```

Parameter:

login	Add/Edit login authentication list
enable	Add/Edit enable authentication list
default	Edit default authentication list
LISTNAME	Specify the list name for authentication type
METHODLIST	Specify the authenticate method, including none, local, enable, tacacs+, radius.

Default:

Default authentication list name for type login is “default” and default method is “local”.

Default authentication list name for type enable is “default” and default method is “enable”

Mode:

Global Configuration

Usage Guide:

Login authentication is used when user try to login into the switch. Such as CLI login dialog and WEBUI login web page.

Enable authentication is used only on CLI for user trying to switch from User EXEC mode to Privileged EXEC mode.

Both of them support following authenticate methods.

Local: Use local user account database to authenticate. (This method is not supported for enable authentication)

Enable: Use local enable password database to authenticate.

Tacacs+: Use remote Tacas+ server to authenticate.

Radius: Use remote Radius server to authenticate.

None: Do nothing and just make user to be authenticated.

Each list allows you to combine these methods with different orders. For example, we want to authenticate login user with remote Tacacs+ server, but server may be crashed. Therefore, we need a backup plan, such as another Radius server. So we can configure the list with Tacacs+ server as first authentication method and Radius server as second one.

Use no form to delete the existing list. However, “default” list is not allowed to remove.

Example:

This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
```


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

This example shows how to show existing login authentication lists

```
Switch# show aaa authentication login lists
Login List Name | Authentication Method List
-----------------+-------------------------------
default | local
test1 | tacacs+ radius local
```

This example shows how to add an enable authentication list to authenticate with order tacacs+, radius, enable.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
```

This example shows how to show existing enable authentication lists

```
Switch# show aaa authentication login lists
Enable List Name | Authentication Method List
-----------------+-------------------------------
default | enable
test2 | tacacs+ radius enable
```

3.2.2 login authentication

Command:

login authentication *LISTNAME*

no login authentication

Parameter:

LISTNAME Specify the login authentication list name to use.

Default:

Default login authentication list for each line is “default”.

Mode:

Line Configuration

Usage Guide:

Different access methods are allowed to bind different login authentication lists. Use “**login authentication**”

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

command to bind the list to specific line (telnet, ssh).

Use no form to bind the “default” list back.

Example:

This example shows how to create a new login authentication list and bind to telnet line.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# line telnet
Switch(config-line)# login authentication test1
```

This example shows how to show line binding lists.

```
Switch# show line lists
Line Type | AAA Type | List Name
-------------+-----------------+-----------------
telnet | login | test1
| enable | default
| exec | default
| commands | default
| accounting-exec | default
ssh | login | default
| enable | default
| exec | default
| commands | default
| accounting-exec | default
http | login | default
https | login | default
```


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

3.2.3 ip http login authentication

Command:

```
ip (http | https) login authentication LISTNAME

no ip (http | https) login authentication
```

Parameter:

http	Bind login authentication list to user access WEBUI with http protocol
https	Bind login authentication list to user access WEBUI with https protocol
LISTNAME	Specify the login authentication list name to use.

Default:

Default login authentication list for each line is “default”.

Mode:

Global Configuration

Usage Guide:

Different access methods are allowed to bind different login authentication lists. Use “**ip (http | https) login authentication**” command to bind the list to WEBUI access from http or https.

Use no form to bind the “default” list back.

Example:

This example shows how to create two new login authentication lists and bind to http and https.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# aaa authentication login test2 radius local
Switch(config)# ip http login authentication test1
Switch(config)# ip https login authentication test2
```

This example shows how to show line binding lists.

```
Switch# show line lists
Line Type | AAA Type | List Name
-------------+-----------------+-----------------
telnet | login | default
| enable | default
| exec | default
| commands | default
| acct-exec | default
| acct-cmd( 0) | default
```


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

```
| acct-cmd( 1) | default
| acct-cmd( 2) | default
| acct-cmd( 3) | default
| acct-cmd( 4) | default
| acct-cmd( 5) | default
| acct-cmd( 6) | default
| acct-cmd( 7) | default
| acct-cmd( 8) | default
| acct-cmd( 9) | default
| acct-cmd(10) | default
| acct-cmd(11) | default
| acct-cmd(12) | default
| acct-cmd(13) | default
| acct-cmd(14) | default
| acct-cmd(15) | default
ssh | login | default
| enable | default
| exec | default
| commands | default
| acct-exec | default
| acct-cmd( 0) | default
| acct-cmd( 1) | default
| acct-cmd( 2) | default
| acct-cmd( 3) | default
| acct-cmd( 4) | default
| acct-cmd( 5) | default
| acct-cmd( 6) | default
| acct-cmd( 7) | default
| acct-cmd( 8) | default
| acct-cmd( 9) | default
| acct-cmd(10) | default
| acct-cmd(11) | default
| acct-cmd(12) | default
| acct-cmd(13) | default
| acct-cmd(14) | default
| acct-cmd(15) | default
http | login | test1
https | login | test2
```


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

3.2.4 enable authentication

Command:

```
enable authentication LISTNAME

no enable authentication
```

Parameter:

LISTNAME	Specify the login authentication list name to use.

Default:

Default enable authentication list for each line is “default”.

Mode:

Line Configuration

Usage Guide:

Different access methods are allowed to bind different enable authentication lists. Use “**enable authentication**” command to bind the list to specific line (telnet, ssh).

Use no form to bind the “default” list back.

Example:

This example shows how to create a new enable authentication list and bind to telnet line.

```
Switch(config)# aaa authentication enable test1 tacacs+ radius enable
Switch(config)# line telnet
Switch(config-line)# enable authentication test1
```

This example shows how to show line binding lists.

```
Switch# show line lists
Line Type | AAA Type | List Name
-------------+-----------------+-----------------
telnet | login | default
| enable | test1
| exec | default
| commands | default
| accounting-exec | default
ssh | login | default
| enable | default
```


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

```
| exec | default
| commands | default
| accounting-exec | default
http | login | default
https | login | default
```

3.2.5 show aaa authentication

Command:

```
show aaa authentication (login | enable) lists
```

Parameter:

login	Show login authentication list
enable	Show enable authentication list

Mode:

Privileged EXEC

Usage Guide:

Use "**show aaa authentication**" command to show login authentication or enable authentication method lists.

Example:

This example shows how to show existing login authentication lists

```
Switch# show aaa authentication login lists
Login List Name | Authentication Method List
-----------------+------------------------------
default | local
test1 | tacacs+ radius local
```

This example shows how to show existing enable authentication lists

```
Switch# show aaa authentication login lists
Enable List Name | Authentication Method List
-----------------+------------------------------
default | enable
test2 | tacacs+ radius enable
```


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

3.2.6 show line lists

Command:

```
show line lists
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show line lists**" command to show all lines' binding list of all authentication, authorization, and accounting function.

Example:

This example shows how to show line binding lists.

```
Switch# show line lists
Line Type | AAA Type | List Name
-------------+-----------------+-----------------
telnet | login | default
| enable | default
| exec | default
| commands | default
| accounting-exec | default
ssh | login | default
| enable | default
| exec | default
| commands | default
| accounting-exec | default
http | login | default
https | login | default
```


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

3.2.7 tacacs default-config

Command:

```
tacacs default-config [key TACACSKEY] [timeout <1-30>]
```

Parameter:

key *TACACSKEY*	Specify default tacacs+ server key string
timeout *<1-30>*	Specify default tacacs+ server timeout value

Default:

Default tacacs+ key is “”.

Default tacacs+ timeout is 5 seconds.

Mode:

Global Configuration

Usage Guide:

Use “**tacacs default-config**” command to modify default values of tacacs+ server. These default values will be used when user try to create a new tacacs+ server and not assigned these values.

Example:

This example shows how modify default tacacs+ configuration

```
Switch(config)# tacacs default-config timeout 20
Switch(config)# tacacs default-config key tackey
```

This example shows how to show default tacacs+ configurations.

```
Switch# show tacacs default-config
Timeout | Key
--------+---------
10 | tackey
```

This example shows how to create a new tacacs+ server with above default config and show results.

```
Switch(config)# tacacs host 192.168.1.111
Switch# show tacacs
Prio | Timeout | IP Address | Port | Key
------+---------+-----------------+--------+----------
1 | 10 | 192.168.1.111 | 49 | tackey
```


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

3.2.8 tacacs host

Command:

```
tacacs host HOSTNAME [port <0-65535>] [key TACPLUSKEY] [priority <0-65535>]
[timeout <1-30>]

no tacacs [host HOSTNAME]
```

Parameter:

host *HOSTNAME*	Specify tacacs+ server host name, both IP address and domain name are available.
port *<0-65535>*	Specify tacacs+ server udp port
key *TACPLUSKEY*	Specify tacacs+ server key string
priority *<0-65535>*	Specify tacacs+ server priority
timeout *<1-30>*	Specify tacacs+ server timeout value

Default:

Default tacacs+ key is “”.

Default tacacs+ timeout is 5 seconds.

Mode:

Global Configuration

Usage Guide:

Use “**tacacs host**” command to add or edit tacacs+ server for authentication, authorization or accounting.

Use no form to delete one or all tacacs+ servers from database.

Example:

This example shows how to create a new tacacs+ server

```
Switch(config)# tacacs host 192.168.1.111 port 12345 key tacacs+ priority 100
timeout 10
```

This example shows how to show existing tacacs+ server.

```
Switch# show tacacs
Prio | Timeout | IP Address | Port | Key
------+---------+------------------+--------+----------
100 | 10 | 192.168.1.111 | 12345 | tacacs+
```


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

3.2.9 show tacacs default-config

Command:

```
show tacacs default-config
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show tacacs default-config**" command to show tacacs+ default configurations.

Example:

This example shows how to show default tacacs+ configurations.

```
Switch# show tacacs default-config
Timeout | Key
--------+---------
10 | tackey
```

3.2.10 show tacacs

Command:

```
show tacacs
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show tacacs**" command to show existing tacacs+ servers.

Example:

This example shows how to show existing tacacs+ server.

```
Switch# show tacacs
Prio | Timeout | IP Address | Port | Key
------+---------+------------------+--------+----------
100 | 10 | 192.168.1.111 | 12345 | tacacs+
```


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

3.2.11 radius default-config

Command:

radius default-config [key *RADIUSKEY*] [retransmit *<1-10>*] [timeout *<1-30>*]

Parameter:

key *RADIUSKEY*	Specify default radius server key string
retransmit *<1-10>*	Specify default radius server retransmit value
timeout *<1-30>*	Specify default radius server timeout value

Default:

Default radius key is “”.

Default radius retransmit is 3 times.

Default radius timeout is 3 seconds.

Mode:

Global Configuration

Usage Guide:

Use “**radius default-config**” command to modify default values of radius server. These default values will be used when user try to create a new radius server and not assigned these values.

Example:

This example shows how modify default radius configuration

```
Switch(config)# radius default-config timeout 20
Switch(config)# radius default-config key radiuskey
Switch(config)# radius default-config retransmit 5
```

This example shows how to show default radius configurations.

```
Switch# show radius default-config
Retries| Timeout| Key
--------+--------+---------
5 | 20 | radiuskey
```

This example shows how to create a new radius server with above default config and show results.

```
Switch(config)# radius host 192.168.1.111
Switch# show radius
```


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

```
Prio | IP Address | Auth-Port| Retries| Timeout| Usage-Type| Key
------+-----------------+----------+--------+--------+-----------+---------
1 | 192.168.1.111 | 1812 | 5 | 20 | All | radiuskey
```

3.2.12 radius host

Command:

radius host *HOSTNAME* [auth-port *<0-65535>*] [key *RADIUSKEY*] [priority *<0-65535>*] [retransmit *<1-10>*] [timeout *<1-30>*] [type (login|802.1x|all)]

no radius [host *HOSTNAME*]

Parameter:

host *HOSTNAME*	Specify radius server host name, both IP address and domain name are available.
auth-port *<0-65535>*	Specify radius server udp port
key *RADIUSKEY*	Specify radius server key string
priority *<0-65535>*	Specify radius server priority
retransmit *<1-10>*	Specify radius server retransmit times
timeout *<1-30>*	Specify radius server timeout value
type	Usage type of this server
login	Use for login
802.1X	Use for 802.1x authentication
all	Use for both login and 802.1x authentication

Default:

Default radius key is “”.

Default radius timeout is 3 seconds.

Mode:

Global Configuration

Usage Guide:

Use “**radius host**” command to add or edit an existing radius server.

Use no form to delete one or all radius servers from database.

Example:

This example shows how to create a new radius server

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

```
Switch(config)# radius host 192.168.1.111 auth-port 12345 key radiuskey priority 100
retransmit 5 timeout 10 type all
```

This example shows how to show existing radius server.

```
Switch# show radius
Prio | IP Address | Auth-Port| Retries| Timeout| Usage-Type| Key
-----+----------------+----------+--------+--------+-----------+---------
100 | 192.168.1.111 | 12345 | 5 | 10 | All |radiuskey
```

3.2.13 show radius default-config

Command:

```
show radius default-config
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show radius default-config**" command to show radius default configurations.

Example:

This example shows how to show default radius configurations.

```
Switch# show radius default-config
Retries| Timeout| Key
-------+--------+---------
5 | 20 | radiuskey
```

3.2.14 show radius

Command:

```
show radius
```

Mode:

Privileged EXEC

Usage Guide:

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

Use “**show radius**” command to show existing radius servers.

Example:

This example shows how to show existing radius server.

```
Switch# show radius
Prio | IP Address | Auth-Port| Retries| Timeout| Usage-Type| Key
-----+----------------+----------+--------+--------+-----------+---------
100 | 192.168.1.111 | 12345 | 5 | 10 | All |radiuskey
```


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

3.3 ACL

3.3.1 mac acl

Command:

```
mac acl NAME

no mac acl NAME
```

Parameter:

NAME	Specify the name of MAC ACL

Mode:

Global Configuration

Usage Guide:

Use the **mac acl** command to create a MAC access list and to enter mac-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit "deny any" ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create a ip acl. You can verify settings by the following show acl command

```
Switch(config)# mac acl test
Switch(mac-al)# show acl
MAC access list test
```

3.3.2 permit (MAC)

Command:

```
[sequence <1-2147483647>] permit (A:B:C:D:E:F/A:B:C:D:E:F|any)
(A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7> <0-7>] [ethtype <1501-
65535>]
no sequence <1-2147483647>
```

Parameter:

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

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A:B:C:D:E:F/A:B:C:D:E:F|any)	Specify the source MAC address and mask of packet or any MAC address.
(A:B:C:D:E:F/A:B:C:D:E:F|any)	Specify the destination MAC address and mask of packet or any MAC address
[vlan <1-4094>]	(Optional) Specify the vlan ID of packet.
[cos <0-7> <0-7>]	(Optional) Specify the Class of Service value and mask of packet.
[ethtype <1501-65535>]	(Optional) Specify Ethernet protocol number of packet

Mode:

MAC ACL Configuration

Usage Guide:

Use the permit command to add permit conditions for a mac ACE that bypass those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add an ACE that permit packets with source MAC address 22:33:44:55:66:77 、VLAN 3 and Ethernet type 1999. You can verify settings by the following **show acl** command

```
Switch(config)# mac acl test
Switch(mac-al)# sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan
3 ethtype 1999
Switch(mac-al)# show acl
MAC access list test
sequence 999 permit 22:33:44:55:66:77/FF:FF:FF:FF:FF:FF any vlan 3 ethtype 1999
```

3.3.3 deny (MAC)

Command:

```
[sequence <1-2147483647>] deny (A:B:C:D:E:F/A:B:C:D:E:F|any)
(A:B:C:D:E:F/A:B:C:D:E:F|any) [vlan <1-4094>] [cos <0-7> <0-7>] [ethtype <1501-
65535>] [shutdown]

no sequence <1-2147483647>
```

Parameter:

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

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A:B:C:D:E:F/A:B:C:D:E:F|any)	Specify the source MAC address and mask of packet or any MAC address.
(A:B:C:D:E:F/A:B:C:D:E:F|any)	Specify the destination MAC address and mask of packet or any MAC address.
[vlan <1-4094>]	(Optional) Specify the vlan ID of packet.
[cos <0-7> <0-7>]	(Optional) Specify the Class of Service value and mask of packet.
[ethtype <1501-65535>]	(Optional) Specify Ethernet protocol number of packet
[shutdown]	(Optional) Shutdown interface while ACE hit

Mode:

MAC ACL Configuration

Usage Guide:

Use the deny command to add deny conditions for a mac ACE that drop those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use "**shutdown**" to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with destination MAC address aa:bb:cc:xx:xx:xx and VLAN 9. You can verify settings by the following **show acl** command

```
Switch(config)# mac acl test
Switch(mac-al)# sequence 30 permit any any
Switch(mac-al)# deny any aa:bb:cc:00:0:00/FF:FF:FF:00:00:00 vlan 9 shutdown
Switch(mac-al)# show acl
MAC access list test
sequence 30 permit any any
sequence 50 deny any AA:BB:CC:00:00:00/FF:FF:FF:00:00:00 vlan 9 shutdown
```


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

3.3.4 ip acl

Command:

```
ip acl NAME

no ip acl NAME
```

Parameter:

NAME	Specify the name of IPv4 ACL

Mode:

Global Configuration

Usage Guide:

Use the **ip acl** command to create an IPv4 access list and to enter ip-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit “deny any” ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create an IP ACL. You can verify settings by the following show acl command

```
Switch(config)#ip acl iptest
Switch(ip-al)# show acl
IP access list iptest
```

3.3.5 permit (IP)

Command:

```
[sequence <1-2147483647>] permit (<0-255>|ipinip|egp|igp|hmp|rdp|ipv6|
ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any)
(A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE]]
[sequence <1-2147483647>] permit icmp (A.B.C.D/A.B.C.D|any)
(A.B.C.D/A.B.C.D|any) (<0-255>|echo-reply|destination-unreachable|source-
quench|echo-request| router-advertisement|router-solicitation|time-
exceeded|timestamp| timestamp-reply|traceroute|any) (<0-255>|any)
[(dscp|precedence) VALUE]
```


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

```
[sequence <1-2147483647>] permit tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|
discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs-
ds|domain|www|
pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)
(A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-
data|ftp|telnet|smtp|time|hostname|whois| tacacs-
ds|domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)
match-all TCP_FLAG] [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit udp (A.B.C.D/A.B.C.D|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-
ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|
snmptrap|who|syslog|talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-
ds|domain|bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
snmp|snmptrap|who|syslog|PORT_RANGE|any)[(dscp|precedence) VALUE]

no sequence <1-2147483647>
```

Parameter:

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/A.B.C.D|any)	Specify the destination IPv4 address and mask of packet or any IPv4 address.
[dscp VALUE]	(Optional) Specify the DSCP of packet.
[precedence VLAUE]	(Optional) Specify the IP precedence of packet.
icmp-type	Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
icmp-code	Specify ICMP message code for filtering ICMP packet.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag

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

should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Mode:

IP ACL Configuration

Usage Guide:

Use the permit command to add permit conditions for an IP ACE that bypass those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add a set of ACEs. You can verify settings by the following **show acl** command.

This command shows how to permit a source IP address subnet.

```
Switch(ip-al)# permit ip 192.168.1.0/255.255.255.0
```

This command shows how to permit ICMP echo-request packet with any IP address.

```
Switch(ip-al)# permit icmp any any echo-request any
```

This command shows how to permit any IP address HTTP packets with DSCP 5.

```
Switch(ip-al)# permit tcp any any any www dscp 5
```

This command shows how to permit any source IP address SNMP packet connect to destination IP address 192.168.1.1.

```
Switch(ip-al)# permit udp any any 192.168.1.1/255.255.255.255 snmp
Switch(ip-al)# show acl
IP access list iptest
sequence 1 permit ip 192.168.1.0/255.255.255.0 any
sequence 21 permit icmp any any echo-request any
sequence 41 permit tcp any any any www dscp 5
sequence 61 permit udp any any 192.168.1.1/255.255.255.255 snmp
```

3.3.6 deny (IP)

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

Command:

```
[sequence <1-2147483647>] deny (<0-255>|ipinip|egp|igp|hmp|rdp|ipv6|
ipv6:rout|ipv6:frag|rsvp|ipv6:icmp|ospf|pim|l2tp|ip) (A.B.C.D/A.B.C.D|any)
(A.B.C.D/A.B.C.D|any) [(dscp|precedence) VALUE]] [shutdown]

[sequence <1-2147483647>] deny icmp (A.B.C.D/A.B.C.D|any) (A.B.C.D/A.B.C.D|any)
(<0-255>|echo-reply|destination-unreachable| source-quench|echo-request|router-
advertisement|router-solicitation| time-exceeded|timestamp| timestamp-
reply|traceroute|any) (<0-255>|any) [(dscp|precedence) VALUE] [shutdown]

[sequence <1-2147483647>] deny tcp (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|
discard|daytime|ftp-data|ftp|telnet|smtp|time|hostname|whois|tacacs-ds|
domain|www|pop2|pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any)
(A.B.C.D/A.B.C.D|any) (<0-65535>|echo|discard|daytime|ftp-data|ftp|telnet|
smtp|time|hostname|whois|tacacs-ds|domain|www|pop2|pop3|syslog|talk|
klogin|kshell|sunrpc|drip|PORT_RANGE|any)
[match-all TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

[sequence <1-2147483647>] deny udp (A.B.C.D/A.B.C.D|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|bootps|
bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|
talk|rip|PORT_RANGE|any) (A.B.C.D/A.B.C.D|any) (<0-65535>|echo|
discard|time|nameserver|tacacs-ds|domain|bootps|bootpc|tftp| sunrpc|ntp|netbios-
ns|snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]
[shutdown]

no sequence <1-2147483647>
```

Parameter:

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/A.B.C.D|any)	Specify the destination IPv4 address and mask of packet or any IPv4 address.
[dscp VALUE]	(Optional) Specify the DSCP of packet.
[precedence VLAUE]	(Optional) Specify the IP precedence of packet.
icmp-type	Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
icmp-code	Specify ICMP message code for filtering ICMP packet.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number

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

	of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
[shutdown]	(Optional) Shutdown interface while ACE hit

Mode:

IP ACL Configuration

Usage Guide:

Use the deny command to add deny conditions for an IP ACE that drop those packets hit the ACE. The “**sequence**” also represents hit priority when ACL bind to an interface. An ACE not specifies “**sequence**” index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use “**shutdown**” to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with source IP address 192.168.1.80. You can verify settings by the following **show acl** command

```
Switch(config)# ip acl iptest
Switch(ip-al)# deny ip 192.168.1.80/255.255.255.255 any
Switch(ip-al)# show acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```


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

3.3.7 ipv6 acl

Command:

```
ipv6 acl NAME

no ipv6 acl NAME
```

Parameter:

NAME	Specify the name of IPv6 ACL

Mode:

Global Configuration

Usage Guide:

Use the **ipv6 acl** command to create an IPv6 access list and to enter ipv6-acl configuration mode. The name of ACL must be unique that can not have same name with other ACL or QoS policy. Once an ACL is created, an implicit "deny any" ACE created at the end of the ACL. That is, if there are no matches, the packets are denied. Use the no form of this command to delete.

Example:

The example shows how to create an IPv6 ACL. You can verify settings by the following show acl command

```
Switch(config)#ipv6 acl ipv6test
Switch(ipv6-al)# show acl
IPv6 access list iptest
```

3.3.8 permit (IPv6)

Command:

```
[sequence <1-2147483647>] permit (<0-255>|ipv6) (X:X::X:X/<0-128>|any)
(X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit icmp (X:X::X:X/<0-128>|any) (X:X::X:X/<0-
128>|any) (<0-255>|destination-unreachable|packet-too-big| time-
exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-
report|mldv2-report|mld-done| router-solicitation|router-advertisement|nd-ns|nd-
na|any) (<0-255>|any)[(dscp|precedence) VALUE]
```


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

```
[sequence <1-2147483647>] permit tcp (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs-
ds|domain|www|pop2|pop3|syslog|
talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp| telnet|smtp|time|hostname|whois|tacacs-
ds|domain|www|pop2|
pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all
TCP_FLAG] [(dscp|precedence) VALUE]

[sequence <1-2147483647>] permit udp (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|
talk|rip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]

no sequence <1-2147483647>
```

Parameter:

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(X:X::X:X/<0-128>|any)	Specify the source IPv6 address and prefix of packet or any IPv6 address.
(X:X::X:X/<0-128>|any)	Specify the destination IPv6 address and prefix of packet or any IPv6 address.
[dscp VALUE]	(Optional) Specify the DSCP of packet.
[precedence VLAUE]	(Optional) Specify the IP precedence of packet.
icmp-type	Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
icmp-code	Specify ICMP message code for filtering ICMP packet.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst,

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

+syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

Mode:

IPv6 ACL Configuration

Usage Guide:

Use the permit command to add permit conditions for an IPv6 ACE that bypass those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE.

Example:

The example shows how to add a set of ACEs. You can verify settings by the following show acl command. This command shows how to permit a source IP address subnet.

```
Switch(ipv6-al)# permit permit ipv6 fe80:1122:3344:5566::1/64 any
Switch(ipv6-al)# show acl
IPv6 access list ipv6test
sequence 1 permit ipv6 fe80:1122:3344:5566::1/64 any
```

3.3.9 deny (IPv6)

Command:

```
[sequence <1-2147483647>] deny (<0-255>|ipv6) (X:X::X:X/<0-128>|any)
(X:X::X:X/<0-128>|any) [(dscp|precedence) VALUE] [shutdown]

[sequence <1-2147483647>] deny icmp (X:X::X:X/<0-128>|any) (X:X::X:X/<0-
128>|any) (<0-255>|destination-unreachable|packet-too-big| time-
exceeded|parameter-problem|echo-request|echo-reply| mld-query|mld-
report|mldv2-report|mld-done| router-solicitation|router-advertisement|nd-ns|nd-
na|any) (<0-255>|any)[(dscp|precedence) VALUE] [shutdown]

[sequence <1-2147483647>] deny tcp (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp|telnet|smtp| time|hostname|whois|tacacs-
ds|domain|www|pop2|pop3|syslog|
talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|daytime|ftp-data|ftp| telnet|smtp|time|hostname|whois|tacacs-
ds|domain|www|pop2|
```


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

```
pop3|syslog|talk|klogin|kshell|sunrpc|drip|PORT_RANGE|any) [match-all
TCP_FLAG] [(dscp|precedence) VALUE] [shutdown]

[sequence <1-2147483647>] deny udp (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|snmp|snmptrap|who|syslog|
talk|rip|PORT_RANGE|any) (X:X::X:X/<0-128>|any) (<0-
65535>|echo|discard|time|nameserver|tacacs-ds|domain|
bootps|bootpc|tftp|sunrpc|ntp|netbios-ns|
snmp|snmptrap|who|syslog|PORT_RANGE|any) [(dscp|precedence) VALUE]
[shutdown]

no sequence <1-2147483647>
```

Parameter:

<1-2147483647>	(Optional) Specify sequence index of ACE, the sequence index represent the priority of an ACE in ACL.
(A.B.C.D/A.B.C.D|any)	Specify the source IPv4 address and mask of packet or any IPv4 address.
(A.B.C.D/A.B.C.D|any)	Specify the destination IPv4 address and mask of packet or any IPv4 address.
[dscp VALUE]	(Optional) Specify the DSCP of packet.
[precedence VLAUE]	(Optional) Specify the IP precedence of packet.
icmp-type	Specify ICMP message type for filtering ICMP packet. Enter a type name of list or a number of ICMP message type.
icmp-code	Specify ICMP message code for filtering ICMP packet.
igmp-type	Specify IGMP type for filtering IGMP packet. Enter a type name of list or a number of IGMP type.
l4-source-port	Specify TCP/UDP source port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
l4-destination-port	Specify TCP/UDP destination port of for filtering TCP/UDP packet. Enter a port name of list or a number of TCP/UDP port.
match-all	Specify tcp flag for TCP packet. If a flag should be set it is prefixed by \"+\".If a flag should be unset it is prefixed by \"-\". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin.To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).
[shutdown]	(Optional) Shutdown interface while ACE hit

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

Mode:

IP ACL Configuration

Usage Guide:

Use the deny command to add deny conditions for an IPv6 ACE that drop those packets hit the ACE. The "**sequence**" also represents hit priority when ACL bind to an interface. An ACE not specifies "**sequence**" index would assign a sequence index which is the largest existed index plus 20. If packet content can match more than one ACE, the lowest sequence ACE is hit. An ACE can not be added if has the same conditions as existed ACE. Use "**shutdown**" to shutdown interface while ACE hit.

Example:

The example shows how to add an ACE that denies packets with destination IP address fe80::abcd. You can verify settings by the following **show acl** command

```
Switch334455(config)# ipv6 acl ipv6test
Switch334455(ip-al)# deny ipv6 any fe80::abcd/128
Switch334455(ip-al)# show acl
IPv6 access list ipv6test
sequence 1 deny ipv6 any fe80::abcd/128
```

3.3.10 bind acl

Command:

```
(mac|ip|ipv6) acl NAME

[no] (mac|ip|ipv6) acl NAME
```

Parameter:

(mac|ip|ipv6)	Specify a type of ACL to binding to interface
NAME	Specify the name of ACL

Mode:

Global Configuration

Context Configuration

Usage Guide:

Use the **show acl** command to show created ACLs. You can specify mac、ip or ipv6 to show specific type ACL or specify unique name string to show ACL with the name.

Example:

The example shows how to show all IP ACL.

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

```
Switch(config)# show ip acl
IP access list iptest
sequence 1 deny ip 192.168.1.80/255.255.255.255 any
```

3.3.11 show acl utilization

Command:

```
show all utilization
```

Mode:

Global Configuration

Usage Guide:

Use the **show acl utilization** command to show the usage of PIE of ASIC. When a ACL bind to interface, it needs ASIC PIE resource to help to filter packet. An ASIC has limited PIE resource. This command help user to know the PIE usage of AISC.

Example:

The example shows how to show PIE utilization

```
Switch(config)# show acl utilization
Group Index : 1
Group Assign to : Mac-based ACL and IPv4-based ACL
Group Maximun ACEs : 128
Group Remain ACEs : 125
Group Used ACEs : 3
ACEs Used by ACL : 3
ACEs Used by QoS : 0
------------------------------
Group Index : 2
Group Assign to : None
Group Maximun ACEs : 128
Group Remain ACEs : 128
Group Used ACEs : 0
ACEs Used by ACL : 0
ACEs Used by QoS : 0
------------------------------
```


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

```
Group Index : 3
Group Assign to : None
Group Maximun ACEs : 128
Group Remain ACEs : 128
Group Used ACEs : 0
ACEs Used by ACL : 0
ACEs Used by QoS : 0
-----------------------------
Group Index : 4
Group Assign to : None
Group Maximun ACEs : 128
Group Remain ACEs : 128
Group Used ACEs : 0
ACEs Used by ACL : 0
ACEs Used by QoS : 0
```


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

3.4 Administration

3.4.1 enable

Command:

```
enable [<1-15>]

disable [<1-14>]
```

Parameter:

<1-15>	Specify privileged level to enable
<1-14>	Specify privileged level to enable

Default:

Default privilege level is 15 if no privilege level is specified on enable command.

Default privilege level is 1 if no privilege level is specified on disable command.

Mode:

User EXEC

Usage Guide:

In User EXEC mode, user only allows to do a few actions. Most of commands are only available in privileged EXEC mode. Use "**enable**" command to enter the privileged mode to do more actions on switch.

In privileged EXEC mode, use "**exit**" command is able to go back to user EXEC mode with original user privilege level. If you need to go back to user EXEC mode with different privilege level, use "**disable**" command to specify the privilege level you need.

In privileged EXEC mode, the prompt will show "**Switch#**"

Example:

This example shows how to enter privileged EXEC mode and show current privilege level.

```
Switch> enable
Switch# show privilege
Current CLI Username:
Current CLI Privilege: 15
```

This example show how to enter user EXEC mode with privilege 3.

```
Switch# disable 3
Switch> show privilege
```


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

```
Current CLI Username:
Current CLI Privilege: 3
```

3.4.2 exit

Command:

```
exit
```

Mode:

User EXEC

Privileged EXEC

Global Configuration

Interface Configuration

Line Configuration

.....

Usage Guide:

In User EXEC mode, "**exit**" command will close current CLI session. In other modes, "**exit**" command will go to the parent mode. And every mode has the "exit" command.

Example:

This example shows how to enter privileged EXEC mode and use exit command to go back to user EXEC mode.

```
Switch> enable
Switch# exit
Switch>
```

3.4.3 configure

Command:

```
configure
```

Mode:

Privileged EXEC

Usage Guide:

Use "**configure**" command to enter global configuration mode. In global configuration mode, the prompt will show as

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

"**Switch(config)#**".

Example:

This example shows how to enter global configuration mode.

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

3.4.4 interface

Command:

```
interface IF_PORTS

interface range IF_PORTS
```

Parameter:

IF_PORTS	Specify the port to select. This parameter allows partial port name and ignore case. For Example: Gigabit4 ..... If port range is specified, the list format is also available. For Example: gi1-3 .....

Mode:

Global Configuration

Usage Guide:

Some configurations are port based. In order to configure these configurations, we need to enter Interface Configuration mode to configure them. Use "**interface**" command to enter the Interface Configuration mode and select the port to be configured.

In Interface Configuration mode, the prompt will show as "**Switch(config-if)#**"

Example:

This example shows how to enter Interface Configuration mode

```
Switch> enable
Switch# exit
Switch>
```


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

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)#
```

3.4.5 line

Command:

```
line (telnet | ssh )
```

Parameter:

telnet	Select telnet line to configure.
ssh	Select ssh line to configure.

Mode:

Global Configuration

Usage Guide:

Some configurations are line based. In order to configure these configurations, we need to enter Line Configuration mode to configure them. Use "**line**" command to enter the Line Configuration mode and select the line to be configured.

In Line Configuration mode, the prompt will show as "**Switch(config-line)#**"

Example:

This example shows how to enter Interface Configuration mode

```
Switch# configure
Switch(config)# line telnet
Switch(config-line)#
```

3.4.6 end

Command:

```
end
```

Mode:

Privileged EXEC

Global Configuration

Interface Configuration

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

Line Configuration

.....

Usage Guide:

Use “**end**” command to return to privileged EXEC mode directly. Every mode except User EXEC mode has the “end” command.

Example:

This example shows how to enter Interface Configuration mode and use end command to go back to privileged EXEC mode

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# end
Switch#
```

3.4.7 reboot

Command:

```
reboot
```

Mode:

Privileged EXEC

Usage Guide:

Use “**reboot**” command to make system hot restart.

Example:

This example shows how to restart the system

```
Switch# reboot
```


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

3.4.8 system name

Command:

system name *NAME*

Parameter:

NAME	Specify system name string.

Mode:

Global Configuration

Usage Guide:

Use "**system name**" command to modify system name information of the switch. The system name is also used to be CLI prompt.

Example:

This example shows how to modify contact information

```
Switch(config)# system name myname
myname(config)#
```

This example shows how to show system name information

```
Switch# show info
System Name : myname
System Location : Default Location
System Contact : Default Contact
MAC Address : 00:30:4F:EF:01:02
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

3.4.9 system contact

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

Command:

```
system contact CONTACT
```

Parameter:

CONTACT	Specify contact string.

Mode:

Global Configuration

Usage Guide:

Use "**system contact**" command to modify contact information of the switch.

Example:

This example shows how to modify contact information

```
Switch(config)# system contact callme
```

This example shows how to show system contact information

```
Switch(config)# system contact callme
Switch# show info
System Name : Switch
System Location : Default Location
System Contact : callme
MAC Address : 00:30:4F:EF:01:02
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

3.4.10 system location

Command:

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

```
system location LOCATION
```

Parameter:

LOCATION	Specify location string.

Mode:

Global Configuration

Usage Guide:

Use "**system location**" command to modify location information of the switch.

Example:

This example shows how to modify location information

```
Switch(config)# system location home
```

This example shows how to show system location information

```
Switch(config)# system location home
Switch# show info
System Name : SwitchEF0102
System Location : home
System Contact : Default Contact
MAC Address : 00:30:4f:EF:01:02
IP Address : 192.168.0.100
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 0 hours, 2 mins, 37 secs
```

3.4.11 username

Command:

```
username WORD<0-32> [privilege (admin | user | <0-15>)] (password | secret)
WORD<0-32>
```


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

```
no username WORD<0-32>
```

Parameter:

username ***WORD<0-32>***	Specify user name to add/delete/edit.
privilege admin	Specify privilege level to be admin (privilege 15)
privilege user	Specify privilege level to be user (privilege 1)
privilege ***<0-15>***	Specify custom privilege level
password ***WORD<0-32>***	Specify password string and make it not encrypted.

Default:

Default username “” has password “” with privilege 1.

Default username “admin” has password “admin” with privilege 15.

Mode:

Global Configuration

Usage Guide:

Use “**username**” command to add a new user account or edit an existing user account. And use “**no username**” to delete an existing user account. The user account is a local database for login authentication.

Example:

This example shows how to add a new user account.

```
Switch(config)# username test secret passwd
```

This example shows how to show existing user accounts.

```
Switch# show username
Priv | Type | User Name | Password
------+--------+--------------------+------------------------
01 | secret | | dnXencJRwflV6
15 | secret | admin | FzjrGO6vfbERY
15 | secret | test | 7p57T9yMkViSUS
```

3.4.12 enable password

Command:

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

```
enable [privilege <0-15>] (password | secret) WORD<0-32>

no enable [privilege <0-15>]
```

Parameter:

privilege *<0-15>*	Specify the privilege level to configure. If no privilege level is specified, default is 15.
password *WORD<0-32>*	Specify password string and make it not encrypted.
secret *WORD<0-32>*	Specify password string and make it encrypted.

Default:

Default enable password for all privilege levels are “”.

Mode:

Global Configuration

Usage Guide:

Use “**enable password**” command to edit password for each privilege level for enable authentication. And use “**no enable**” command to restore enable password to default empty value.

The only way to show this configuration is using “**show running-config**” command.

Example:

This example shows how to edit enable password for privilege level 15

```
Switch(config)# enable secret enblpasswd
```

3.4.13 ip address

Command:

```
ip address A.B.C.D [mask A.B.C.D]
```

Parameter:

address *A.B.C.D*	Specify IPv4 address for switch
mask *A.B.C.D*	Specify net mask address for switch

Default:

Default IP address is 192.168.0.100 and default net mask is 255.255.255.0.

Mode:

Global Configuration

Usage Guide:

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

Use "**ip address**" command to modify administration ipv4 address. This address is very important. When we try to use telnet, ssh, http, https, snmp… to connect to the switch, we need to use this ip address to access it.

Example:

This example shows how to modify the ipv4 address of the switch.

```
Switch(config)# ip address 192.168.1.200 mask 255.255.255.0
```

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip
IP Address: 192.168.1.200
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.254
```

3.4.14 ip default-gateway

Command:

```
ip default-gateway A.B.C.D

no ip default-gateway
```

Parameter:

A.B.C.D	Specify default gateway IPv4 address for switch

Default:

Default IP address of default gateway is 192.168.1.254.

Mode:

Global Configuration

Usage Guide:

Use "**ip default-gateway**" command to modify default gateway address. And use "**no ip default-gateway**" to restore default gateway address to factory default.

Example:

This example shows how to modify the ipv4 address of the switch.

```
Switch(config)# ip default-gateway 192.168.1.100
```

This example shows how to show current ipv4 default gateway of the switch.

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

```
Switch# show ip
IP Address: 192.168.1.1
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.100
```

3.4.15 ip dns

Command:

```
ip dns A.B.C.D [A.B.C.D]

no ip dns [A.B.C.D]
```

Parameter:

A.B.C.D	Specify the DNS server ip address.

Default:

Default IP address of DNS server is 168.95.1.1 and 168.95.192.1.

Mode:

Global Configuration

Usage Guide:

Use "**ip dns**" command to modify DNS server address. And use "**no ip dns**" to delete existing DNS server.

Example:

This example shows how to modify the DNS server of the switch.

```
Switch(config)# ip dns 111.111.111.111 222.222.222.222
```

This example shows how to show current DNS server of the switch.

```
Switch# show ip dns
DNS Server 1 : 111.111.111.111
DNS Server 2 : 222.222.222.222
```

3.4.16 ip dhcp

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

Command:

```
ip dhcp

no ip dhcp
```

Default:

Default DHCP client is disabled.

Mode:

Global Configuration

Usage Guide:

Use "**ip dhcp**" command to enabled dhcp client to get IP address from remote DHCP server.

Use "**no ip dhcp**" command to disabled dhcp client and use static ip address.

Example:

This example shows how to enable dhcp client.

```
Switch(config)# ip dhcp
```

This example shows how to show current dhcp client state of the switch.

```
Switch# show ip dhcp
DHCP Status : enabled
```

3.4.17 ipv6 autoconfig

Command:

```
ipv6 autoconfig

no ipv6 autoconfig
```

Default:

Default IPv6 auto config is enabled.

Mode:

Global Configuration

Usage Guide:

Use "**ipv6 autoconfig**" command to enabled IPv6 auto configuration feature.

Use "**no ipv6 autoconfig**" command to disabled IPv6 auto configuration feature.

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

Example:

This example shows how to disable IPv6 auto config.

```
Switch(config)# no ipv6 autoconfig
```

This example shows how to show current IPv6 auto config state.

```
Switch# show ipv6
IPv6 DHCP Configuration : Disabled
IPv6 DHCP DUID :
IPv6 Auto Configuration : Disabled
IPv6 Link Local Address : fe80::dcad:beff:feef:102/64
IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address : fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.4.18 ipv6 address

Command:

ipv6 address *X:X::X:X* prefix *<0-128>*

Parameter:

address *X:X::X:X*	Specify IPv6 address for switch
prefix *<0-128>*	Specify IPv6 prefix length for switch

Mode:

Global Configuration

Usage Guide:

Use "**ipv6 address**" command to specify static IPv6 address.

Example:

This example shows how to add static ipv6 address of the switch.

```
Switch(config)# ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128
```

This example shows how to show current ipv6 address of the switch.

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

```
Switch# show ipv6
IPv6 DHCP Configuration : Disabled
IPv6 DHCP DUID :
IPv6 Auto Configuration : Enabled
IPv6 Link Local Address : fe80::dcad:beff:feef:102/64
IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address : fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.4.19 ipv6 default-gateway

Command:

ipv6 default-gateway *X:X::X:X*

Parameter:

X:X::X:X	Specify default gateway IPv6 address for switch

Mode:

Global Configuration

Usage Guide:

Use "**ipv6 default-gateway**" command to modify default gateway IPv6 address.

Example:

This example shows how to modify the ipv6 default gateway address of the switch.

```
Switch(config)# ipv6 default-gateway fe80::dcad:beff:feef:103
Switch# show ipv6
IPv6 DHCP Configuration : Disabled
IPv6 DHCP DUID :
IPv6 Auto Configuration : Enabled
IPv6 Link Local Address : fe80::dcad:beff:feef:102/64
IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address : fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```


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

3.4.20 ipv6 dhcp

Command:

```
ipv6 dhcp

no ipv6 dhcp
```

Default:

Default DHCPv6 client is disabled.

Mode:

Global Configuration

Usage Guide:

Use "**ipv6 dhcp**" command to enabled dhcpv6 client to get IP address from remote DHCPv6 server.

Use "**no ipv6 dhcp**" command to disabled dhcpv6 client and use static ipv6 address or ipv6 auto config address.

Example:

This example shows how to enable dhcp client.

```
Switch(config)# ipv6 dhcp
```

This example shows how to show current dhcpv6 client state of the switch.

```
Switch# show ipv6 dhcp
DHCPv6 Status : enabled
```

3.4.21 ip service

Command:

```
ip (telnet | ssh | http | https)

no ip (telnet | ssh | http | https)
```

Parameter:

telnet	Enable/Disable telnet service
Ssh	Enable/Disable ssh service

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

http	Enable/Disable http service
https	Enable/Disable https service

Default:

Default telnet service is disabled.

Default ssh service is disabled.

Default http service is enabled.

Default https service is disabled.

Mode:

Global Configuration

Usage Guide:

Use "**ip service**" command to enable all kinds of ip services. Such as telnet, ssh, http and https.

Use no form to disable service.

Example:

This example shows how to enable telnet service and show current telnet service status.

```
Switch(config)# ip telnet
Telnetd daemon enabled.
Switch(config)# exit
Switch# show line telnet
Telnet ================================
Telnet Server : enabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 0 (seconds)
```

This example shows how to enable https service and show current https service status.

```
Switch(config)# ip https
Switch(config)# exit
Switch# show ip https
HTTPS daemon : enabled
Session Timeout : 10 (minutes)
```

3.4.22 ip session-timeout

Command:

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

```
ip (http | https) session-timeout <0-86400>
```

Parameter:

http	Specify session timeout for http service.
https	Specify session timeout for https service.
<0-86400>	Specify session timeout minutes. 0 means never timeout

Default:

Default session timeout for http and https is 10 minutes.

Mode:

Global Configuration

Usage Guide:

Use "**ip session-timeout**" command to specify the session timeout value for http or https service. When user login into WEBUI and do not do any action after session timeout will be logged out.

Example:

This example shows how to change http session timeout to 15min and https session timeout to 20min

```
Switch(config)# ip http session-timeout 15
Switch(config)# ip https session-timeout 20
```

This example shows how to enable https service and show current https service status.

```
Switch# show ip http
HTTPS daemon : enabled
Session Timeout : 15 (minutes)
Switch# show ip https
HTTPS daemon : disabled
Session Timeout : 20 (minutes)
```

3.4.23 exec-timeout

Command:

```
exec-timeout <0-65535>
```

Parameter:

<0-65535>	Specify session timeout minutes. 0 means never timeout

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

Default:

Default session timeout for all lines are 10 minutes.

Mode:

line Configuration

Usage Guide:

Use "**exec-timeout**" command to specify the session timeout value for CLI running on telnet or ssh service. When user login into CLI and do not do any action after session timeout will be logged out from the CLI session.

Example:

This example shows how to change telnet session timeout to 20min and ssh session timeout to 25min.

```
Switch(config)# line telnet
Switch(config-line)# exec-timeout 20
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# exec-timeout 25
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Telnet ================================
Telnet Server : disabled
Session Timeout : 20 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 0 (seconds)
SSH ===================================
SSH Server : disabled
Session Timeout : 25 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 0 (seconds)
```

3.4.24 password-thresh

Command:

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

```
password-thresh <0-120>
```

Parameter:

<0-120> Specify password fail retry number. 0 means no limit.

Default:

Default password fail retry number is 3.

Mode:

line Configuration

Usage Guide:

Use "**password-thresh**" command to specify the password fail retry number for CLI running on telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**".

Example:

This example shows how to change telnet fail retry number to 5 and ssh fail retry number to 6.

```
Switch(config)# line telnet
Switch(config-line)# password-thresh 5
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# password-thresh 6
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Telnet ==============================
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 5
Silent Time : 0 (seconds)
SSH ==================================
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 6
```


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

```
Silent Time : 0 (seconds)
```

3.4.25 silent-time

Command:

```
silent-time <0-65535>
```

Parameter:

<0-65535> Specify silent time with unit seconds. 0 means do not silent.

Default:

Default silent time is 0.

Mode:

line Configuration

Usage Guide:

Use "**silent time**" command to specify the silent time for CLI running on telnet or ssh service. When user input password to login and authenticate failed, the fail retry number will increase one. After fail retry number exceed configured one, the CLI will block login for the period of silent time which configured by the command "**silent-time**".

Example:

This example shows how to change telnet silent time to 15 and ssh silent time to 20.

```
Switch(config)# line telnet
Switch(config-line)# silent-time 15
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# silent-time 20
Switch(config-line)# exit
```

This example shows how show line information.

```
Switch# show line
Telnet ================================
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 3
```


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

```
Silent Time : 15 (seconds)
SSH ==================================
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 20 (seconds)
```

3.4.26 history

Command:

history ***<1-256>***

no history

Parameter:

<1-256> Specify maximum CLI history entry number.

Default:

Default maximum history entry number is 128.

Mode:

line Configuration

Usage Guide:

Use "**history**" command to specify the maximum commands history number for CLI running on telnet or ssh service. Every command input by user will record in history buffer. If all history commands exceed configured history number, older ones will be deleted from buffer.

Use "n**o history**" to disable the history feature. And use "**show history**" to show all history commands.

Example:

This example shows how to change telnet history number to 150 and ssh history number to 200.

```
Switch(config)# line telnet
Switch(config-line)# history 150
Switch(config-line)# exit
Switch(config)# line ssh
Switch(config-line)# history 200
Switch(config-line)# exit
```

This example shows how show line information.

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

```
Switch# show line
Telnet ==============================
Telnet Server : disabled
Session Timeout : 10 (minutes)
History Count : 150
Password Retry : 3
Silent Time : 0 (seconds)
SSH ==================================
SSH Server : disabled
Session Timeout : 10 (minutes)
History Count : 200
Password Retry : 3
Silent Time : 0 (seconds)
```

This example shows how show history commands.

```
Switch# show history
Maximun History Count: 100
--------------------------------------------------
1. enable
2. configure
3. line telnet
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. line telnet
12. exit
13. line telnet
14. history 100
15. exit
16. show history
17. exit
18. show history
```


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

3.4.27 clear service

Command:

```
clear (telnet | ssh)
```

Parameter:

telnet	Clear all telnet sessions.
ssh	Clear all ssh sessions.

Mode:

Privileged EXEC

Usage Guide:

Use "**clear service**" command to kill all existing sessions for the select service.

Example:

This example shows how to enable telnet service and show current telnet service status.

```
Switch# clear telnet
```

3.4.28 ssl

Command:

```
ssl
```

Mode:

Global Configuration

Usage Guide:

Use "ssl" command to generate security certificate files such as RSA, DSA.

Example:

This example shows how to generate certificate files.

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

This example shows how to show the certificate file lists.

```
Switch# show flash
```


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

```
File Name File Size Modified
------------------------ ---------------- -------------------------
startup-config 1191 2000-01-01 00:00:23
rsa1 974 2000-01-01 00:00:18
rsa2 1675 2000-01-01 00:00:18
dsa2 668 2000-01-01 00:00:18
ssl_cert 993 2000-01-01 00:00:18
image0 (active) 4372401 2012-09-24 01:57:29
image1 (backup) 0
```

3.4.29 ping

Command:

ping *HOSTNAME* [count <*1-999999999*>]

Mode:

Privileged EXEC

Usage Guide:

Use “ping” command to do network ping diagnostic.

Example:

This example shows how to ping remote host 192.168.1.111.

```
Switch# ping 192.168.1.111
PING 192.168.1.111 (192.168.1.111): 56 data bytes
64 bytes from 192.168.1.111: icmp_seq=0 ttl=128 time=10.0 ms
64 bytes from 192.168.1.111: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.1.111: icmp_seq=3 ttl=128 time=0.0 ms
--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/2.5/10.0 ms
```

3.4.30 traceroute

Command:

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

```
traceroute A.B.C.D [max_hop <2-255>]
```

Parameter:

A.B.C.D	Specify IPv4 to trace.
max_hop *<2-255>*	Specify maximum hop to trace.

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "**traceroute**" command to do network trace route diagnostic.

Example:

This example shows how to trace route host 192.168.1.111.

```
Switch# traceroute 192.168.1.111
traceroute to 192.168.1.111 (192.168.1.111), 30 hops max, 40 byte packets
1 192.168.1.111 (192.168.1.111) 0 ms 10 ms 0 ms
```

3.4.31 clear arp

Command:

```
clear arp [A.B.C.D]

show arp
```

Parameter:

A.B.C.D	Specify specific arp entry to clear.

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "**clear arp**" command to clear all or specific one arp entry.

Use "**show arp**" command to show all arp entries.

Example:

This example shows how to show arp entries.

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

```
Switch# show arp
Address HWtype HWaddress Flags Mask Iface
192.168.1.111 ether 00:30:4F:F1:4B:3C C eth0
```

This example shows how to clear all arp entries.

```
Switch(config)# clear arp
```

3.4.32 show version

Command:

```
show version
```

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "**show version**" command to show loader and firmware version and build date.

Example:

This example shows how to show system version.

```
Switch# show version
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
```

3.4.33 show info

Command:

```
show info
```

Mode:

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

User EXEC

Privileged EXEC

Usage Guide:

Use “show info” command to show system summary information.

Example:

This example shows how to show system version.

```
Switch# show info
System Name : Switch
System Location : Default Location
System Contact : Default Contact
MAC Address : 00:30:4F:EF:01:02
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
Loader Version : 1.3.0.26225
Loader Date : Thu May 17 15:19:42 CST 2012
Firmware Version : 2.5.0-beta.32811
Firmware Date : Mon Sep 24 19:33:42 CST 2012
System Object ID : 1.3.6.1.4.1.27282.3.2.10
System Up Time : 0 days, 1 hours, 49 mins, 29 secs
```

3.4.34 show history

Command:

```
show history
```

Mode:

User EXEC

Privileged EXEC

Global Configuration

Usage Guide:

Use “**show history**” to show commands we input before.

Example:

This example shows how show history commands.

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

```
Switch# show history
Maximun History Count: 100
-----------------------------------------------
1. enable
2. configure
3. line telnet
4. exit
5. show history
6. line
7. exit
8. show history
9. configure
10. line
11. line telnet
12. exit
13. line telnet
14. history 100
15. exit
16. show history
17. exit
18. show history
```

3.4.35 show username

Command:

```
show username
```

Mode:

Privileged EXEC

Usage Guide:

Use “**show username**” command show all user accounts in local database.

Example:

This example shows how to show existing user accounts.

```
Switch# show username
```


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

```
Priv | Type | User Name | Password
------+--------+--------------------+------------------------
01 | secret | | dnXencJRwflV6
15 | secret | admin | FzjrGO6vfbERY
15 | secret | test | 7p57T9yMkViSUS
```

3.4.36 show ip

Command:

```
show ip
```

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "**show ip**" command to show system IPv4 address, net mask and default gateway.

Example:

This example shows how to show current ipv4 address of the switch.

```
Switch# show ip
IP Address: 192.168.1.200
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.1.254
```

3.4.37 show ip dhcp

Command:

```
show ip dhcp
```

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "show ip dhcp" command to show IPv4 dhcp client enable state.

Example:

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

This example shows how to show current dhcp client state of the switch.

```
Switch# show ip dhcp
DHCP Status : enabled
```

3.4.38 show ipv6

Command:

```
show ipv6
```

Mode:

User EXEC

Privileged EXEC

Usage Guide:

Use "**show ipv6**" command to show system IPv6 address, net mask, default gateway and auto config state.

Example:

This example shows how to show current ipv6 address of the switch.

```
Switch# show ipv6
IPv6 DHCP Configuration : Disabled
IPv6 DHCP DUID :
IPv6 Auto Configuration : Enabled
IPv6 Link Local Address : fe80::dcad:beff:feef:102/64
IPv6 static Address : fe80::20e:2eff:fef1:4b3c/128
IPv6 static Gateway Address : ::
IPv6 in use Address : fe80::dcad:beff:feef:102/64
IPv6 in use Gateway Address : ::
```

3.4.39 show ipv6 dhcp

Command:

```
show ipv6 dhcp
```

Mode:

User EXEC

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

Privileged EXEC

Usage Guide:

Use "**show ipv6 dhcp**" command to show system IPv6 dhcp client enable state.

Example:

This example shows how to show current dhcpv6 client state of the switch.

```
Switch# show ipv6 dhcp
DHCPv6 Status : enabled
```

3.4.40 show line

Command:

```
show line [(telnet | ssh)]
```

Parameter:

telnet	Select telnet line to show.
ssh	Select ssh line to show.

Mode:

Privileged EXEC

Usage Guide:

Use "**show line**" command to show all line configurations including session timeout, history count, password retry number, silent time and the service enable/disable state.

Example:

This example shows how show all lines' information.

```
Switch# show line
Telnet ================================
Telnet Server : disabled
Session Timeout : 20 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 0 (seconds)
SSH ===================================
SSH Server : disabled
Session Timeout : 25 (minutes)
History Count : 128
Password Retry : 3
Silent Time : 0 (seconds)
```


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

3.5 Cable Diagnostics

3.5.1 show cable-diag interface

Command:

```
show cable-diag interfaces
```

Parameter:

login	Add/Edit login authentication list
enable	Add/Edit enable authentication list
default	Edit default authentication list
LISTNAME	Specify the list name for authentication type
METHODLIST	Specify the authenticate method, including none, local, enable, tacacs+, radius.

Mode:

Global Configuration

Usage Guide:

Display the estimated length of copper cable attached to the ports.

show cable-diag interface all

Display the estimated length of copper cables attached to all ports.

show cable-diag interface

Disable the estimated length of copper cable attached to port gi1.

Example:

```
Switch(config)# show cable-diag interfaces gi1
Port | Speed | Local pair | Pair length | Pair status
------+-------+------------+-------------+--------------
gi1 | auto | Pair A | 0.88 | Open
Pair B | 0.87 | Open
Pair C | 0.82 | Open
Pair D | 0.82 | Open
```


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

3.6 DHCP Snooping

3.6.1 Ip dhcp snooping

Command:

```
ip dhcp snooping

no ip dhcp snooping
```

Default:

DHCP snooping is disabled

Mode:

Global Configuration

Usage Guide:

Use the ip dhcp snooping command to enable DHCP Snooping function. Use the no form of this command to disable.

Example:

The example shows how to enable DHCP Snooping on VLAN 1. You can verify settings by the following show ip dhcp snooping command.

```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 1
switch(config)# show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1
circuit-id default format: vlan-port
remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

3.6.2 ip dhcp snooping vlan

Command:

```
ip dhcp snooping vlan VLAN-LIST
```

Parameter:

VLAN-LIST	Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection

Default:

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

Default is disabled on all VLANs

Mode:

Global Configuration

Usage Guide:

Use the **ip dhcp snooping vlan** command to enable VLANs on DHCP Snooping function. Use the **no** form of this command to disable VLANs on DHCP Snooping function.

Example:

The example shows how to enable VLAN 1-100 on DHCP Snooping, and then disable VLAN 30-40 on DHCP Snooping. You can verify settings by the following **show ip dhcp snooping** command.

```
switch(config)# vlan 1-100
switch(config)# exit
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 1-100
switch(config)# show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1-100
circuit-id default format: vlan-port
remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)
switch(config)# no ip dhcp snooping vlan 30-40
switch(config)# show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1-29,41-100
circuit-id default format: vlan-port
remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

3.6.3 ip dhcp snooping trust

Command:

```
ip dhcp snooping trust

no ip dhcp snooping trust
```

Default:

DHCP snooping trust is disabled

Mode:

Interface Configuration

Usage Guide:

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

Use the **ip dhcp snooping trust** command to set trusted interface. The switch does not check DHCP packets that are received on the trusted interface; it simply forwards it. Use the **no** form of this command to set untrusted interface.

Example:

The example shows how to set interface gi1 to trust. You can verify settings by the following **show ip dhcp snooping interface** command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping trust
switch(config-if)# do show ip dhcp snooping interface gi1
Interfaces|Trust State|Rate (pps)|hwaddr Check|Insert Option82|
----------+-----------+----------+------------+---------------+
gi1 | Trusted | None | disabled | disabled |
```

3.6.4 ip dhcp snooping verify

Command:

```
ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address
```

Default:

DHCP snooping verify mac-address is disabled

Mode:

Interface Configuration

Usage Guide:

Use the **ip dhcp snooping verify** command to verify MAC address function on interface.

The "**mac-address**" drop DHCP packets that chaddr and ethernet-source-mac is not match.

Example:

The example shows how to set interface gi1 to validate "**mac-address**". You can verify settings by the following **show ip dhcp snooping interface** command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping verify mac-address
switch(config-if)# do show ip dhcp snooping interface gi1
Interfaces|Trust State|Rate (pps)|hwaddr Check|Insert Option82|
```


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

```
----------+-----------+----------+------------+---------------+
gi1 | Untrusted | None | enabled | disabled |
```

3.6.5 ip dhcp snooping limit rate

Command:

```
ip dhcp snooping limit rate <1-300>

no ip dhcp snooping limit rate
```

Parameter:

<1-300>	Set 1 to 300 PPS of DHCP packet rate limitation

Default:

Default is un-limited of DHCP packet

Mode:

Interface Configuration

Usage Guide:

Use the **ip dhcp snooping limit rate** command to set rate limitation on interface. The switch drop DHCP packets after receives more than configured rate of packets per second. Use the **no** form of this command to return to default settings.

Example:

The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following **show ip dhcp snooping interface** command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping rate-limit 30
switch(config-if)# do show ip dhcp snooping interfaces gi1
Interfaces|Trust State|Rate (pps)|hwaddr Check|Insert Option82|
----------+-----------+----------+------------+---------------+
gi1 | Untrusted | 30 | disabled | disabled |
```

3.6.6 clear ip dhcp snooping statistics

Command:

```
clear ip dhcp snooping interfaces IF_PORTS statistics
```


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

Parameter:

IF_PORTS	specifies ports to clear statistics

Mode:

Global Configuration

Usage Guide:

Use the **clear ip dhcp snooping interfaces statistics** command to clear statistics that are recorded on interface.

Example:

The example shows how to clear statistics on interface gi1. You can verify settings by the following **show ip dhcp snooping interface statistics** command.

```
switch# clear ip dhcp snooping interfaces gi1 statistics
switch# show ip dhcp snooping interfaces gi1 statistics
Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port
With Option82 Dropped | Invalid Drop
-------+-----------+-----------------+----------------------+-------------------------+--------
gi1 | 0 | 0 | 0 | 0 | 0
```

3.6.7 show ip dhcp snooping

Command:

```
show ip dhcp snooping
```

Mode:

Global Configuration

Usage Guide:

Use the **show ip dhcp snooping** command to show settings of DHCP Snooping.

Example:

The example shows how to show settings of DHCP Snooping

```
switch(config)# show ip dhcp snooping
DHCP Snooping : enabled
Enable on following Vlans : 1
```


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

```
circuit-id default format: vlan-port
remote-id: : 00:11:22:33:44:55 (Switch Mac in Byte Order)
```

3.6.8 show ip dhcp snooping interface

Command:

```
show ip dhcp snooping interfaces IF_PORTS

no show ip dhcp snooping interfaces IF_PORTS
```

Parameter:

IF_PORTS specifies ports to show statistics

Mode:

Global Configuration

Usage Guide:

Use the **show ip dhcp snooping interfaces** command to show settings or statistics of interface.

Example:

The example shows how to show settings of interface gi1.

```
switch# show ip dhcp snooping interface gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+--------------+-------------+-------------------+-------------------+
gi1 | Untrusted | None | enabled | disabled |
```

The example shows how to show statistics of interface gi1.

```
switch# show ip dhcp snooping interfaces gi1 statistics
Interfaces | Forwarded | Chaddr Check Dropped | Untrust Port Dropped | Untrust Port
With Option82 Dropped | Invalid Drop
-------+-----------+-----------------+----------------------+-------------------------+--------
gi1 | 0 | 0 | 0 | 0 | 0
```

3.6.9 show ip dhcp snooping binding

Command:

```
show ip dhcp snooping binding
```

Mode:

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

Usage Guide:

Use the **show ip dhcp snooping binding** command to show binding entries that learned by DHCP Snooping

Example:

The example shows how to show binding entries that learned by DHCP Snooping.

```
switch# show ip dhcp snooping binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address | IP | Type | Lease Time
--------+------+--------------------+-------------------------------------+--------------------+-----------
fa1 | 1 | 00:30:4F:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400
```

3.6.10 ip dhcp snooping option

Command:

```
ip dhcp snooping option

no ip dhcp snooping option
```

Default:

DHCP snooping option82 is disabled

Mode:

Interface Configuration

Usage Guide:

Use the **ip dhcp snooping option** command to enable that insert option82 content into packet. Use the **no** form of this command to disable.

Example:

The example shows how to enable option82 insertion. You can verify settings by the following **show ip dhcp snooping interface** command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping option
switch(config-if)# do show ip dhcp snooping interfaces gi1
Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
------------+--------------+-------------+-------------------+-------------------+
gi1 | Untrusted | None | disabled | enabled |
```


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

3.6.11 ip dhcp snooping option action

Command:

```
ip dhcp snooping option action (drop|keep|replace)

no ip dhcp snooping option action
```

Parameter:

drop	Drop packets with option82 that are received from un trusted port
keep	Keep original option82 content in packet
replace	Replace option82 content by switch setting

Default:

DHCP snooping option82 is drop

Mode:

Interface Configuration

Usage Guide:

Use the **ip dhcp snooping option action** command to set the action when receive packets that with option82 content. Use the **no** form of this command to default setting.

Example:

The example shows how to set action to replace option82 content. You can verify settings by the following **show running-config** command.

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping option action replace
```

3.6.12 ip dhcp snooping option circuit-id

Command:

```
ip dhcp snooping [vlan <1-4094>] option circuit-id STRING

no ip dhcp snooping [vlan <1-4094>] option circuit-id
```

Parameter:

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

vlan <1-4094>	VLAN ID to set user defined circuit-id string
STRING	Circuit-id string, 1 to 63 ASCII characters, no spaces.

Default:

Default circuit-id is port id + vlan id in byte format.

Mode:

Interface Configuration

Usage Guide:

Use the **ip dhcp snooping option circuit-id** command to set user-defined circuit-id string. Circuit-id is per port per VLAN setting. If a VLAN is not found user-defined circuit-id then use per port circuit-id string. Use the **no** form of this command to default setting.

Example:

The example shows how to set a user-defined circuit-id string on interface gi1 and VLAN 1. You can verify settings by the following **show running-config** command

```
switch(config)# interface gi1
switch(config-if)# ip dhcp snooping vlan 1 option circuit-id test
```

3.6.13 ip dhcp snooping option remote-id

Command:

```
ip dhcp snooping option remote-id STRING

no ip dhcp snooping option remote-id
```

Parameter:

STRING	Remote-id string, 1 to 63 ASCII characters, no spaces.

Default:

Default remote-id is the switch MAC address in byte order

Mode:

Global Configuration

Usage Guide:

Use the **ip dhcp snooping option remote-id** command to set user-defined remote-id string.

Remote-id is an global and unique string. Use the **no** form of this command to default setting.

Example:

The example shows how to set a user-defined remote-id string on switch. You can verify settings by the following **show ip dhcp snooping option remote-id**

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

```
switch(config)# ip dhcp snooping option remote-id test_remote
switch(config)# do show ip dhcp snooping option remote-id
Remote ID: test_remote
```

3.6.14 show ip dhcp snooping option

Command:

```
show ip dhcp snooping option remote-id
```

Mode:

Global Configuration

Usage Guide:

Use the **show ip dhcp snooping option remote-id** command to show remote-id string.

Example:

The example shows how to show remote-id string

```
switch(config)# do show ip dhcp snooping option remote-id
Remote ID: test_remote
```


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

3.6.15 ip dhcp snooping database

Command:

```
ip dhcp snooping database flash

ip dhcp snooping database tftp (A.B.C.D|HOSTNAME) NAME

no ip dhcp snooping database
```

Parameter:

(A.B.C.D| HOSTNAME)	Specify the IP address or hostname of remote TFTP server
NAME	Input name of backup file

Default:

DHCP snooping database is disabled

Mode:

Global Configuration

Usage Guide:

Use the **ip dhcp snooping database** command to enable DHCP Snooping database agent. The "**flash**" means that write backup file to switch local drive. The "**tftp**" means that write backup file to remote TFTP server. Use the **no** form of this command to disable.

Example:

The example shows how to enable DHCP Snooping database agent and write backup file to remote TFTP server with file name "backup_file". You can verify settings by the following **show ip dhcp snooping database** command.

```
switch(config)# ip dhcp snooping database tftp 192.168.1.50 backup_file
switch(config)# do show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
```


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

```
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

3.6.16 ip dhcp snooping database write-deley

Command:

```
ip dhcp snooping database write-delay <15-86400>

no ip dhcp snooping database write-delay
```

Parameter:

<15-86400>	Specifies the seconds of timeout. Specify the duration for which the transfer should be delayed after the binding database changes

Default:

DHCP snooping database write-delay is 300 seconds

Mode:

Global Configuration

Usage Guide:

Use the **ip dhcp snooping database write-delay** command to modify the write-delay timer. Use the **no** form of this command to default setting.

Example:

The example shows how to set write-delay timer to 60 seconds. You can verify settings by the following **show ip dhcp snooping database** command.

```
switch(config)# ip dhcp snooping database write-delay 60
switch(config)# do show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 60 seconds
Abort Timer : 300 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
```


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

```
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

3.6.17 ip dhcp snooping database timeout

Command:

```
ip dhcp snooping database timeout <0-86400>

no ip dhcp snooping database timeout
```

Parameter:

<0-86400> specifies the seconds of timeout。Specify (in seconds) how long to wait for the database transfer process to finish before stopping the process. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely

Default:

DHCP snooping database timeout is 300 seconds

Mode:

Global Configuration

Usage Guide:

Use the **ip dhcp snooping database timeout** command to modify the timeout timer. Use the **no** form of this command to default setting.

Example:

The example shows how to set timeout timer to 60 seconds. You can verify settings by the following **show ip dhcp snooping database** command.

```
switch(config)# ip dhcp snooping database timeout 60
switch(config)# do show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 60 seconds
Agent Running : Running
```


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

```
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

3.6.18 clear ip dhcp snooping database statistics

Command:

```
clear ip dhcp snooping database statistics
```

Mode:

Global Configuration

Usage Guide:

Use the **clear ip dhcp snooping database statistics** command to clear statistics of DHCP Snooping databae.

Example:

The example shows how to clear statistics of DHCP Snooping agent. You can verify settings by the following **show ip dhcp snooping database** command.

```
switch# clear ip dhcp snooping database statistics
switch# show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 60 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 0
```


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

```
Successful Transfers : 0 Failed Transfers : 0
Successful Reads : 0 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

3.6.19 renew ip dhcp snooping database

Command:

```
renew ip dhcp snooping database
```

Mode:

Global Configuration

Usage Guide:

Use the **renew ip dhcp snooping database** command to renew DHCP Snooping database from backup file.

Example:

The example shows how to renew DHCP Snooping database. You can verify settings by the following **show ip dhcp snooping database** and **show ip dhcp snooping binding** command.

```
switch# show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 60 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 1 Failed Transfers : 0
Successful Reads : 1 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
switch# show ip dhcp snooping binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address | IP | Type | Lease Time
--------+------+--------------------+--------------------------------------+--------------------+-----------
```


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

```
fa1 | 1 | 00:30:4F:C7:12:62 | 192.168.1.100(255.255.255.255)|DHCP Snooping | 86400
```

3.6.20 show ip dhcp snooping database

Command:

```
show ip dhcp snooping database
```

Mode:

Global Configuration

Usage Guide:

Use the **show ip dhcp snooping database** command to show settings of DHCP Snooping agent.

Example:

The example shows how to show settings of DHCP Snooping agent.

```
switch(config)# show ip dhcp snooping database
Type : tftp: 192.168.1.50
FileName : backup_file
Write delay Timer : 300 seconds
Abort Timer : 60 seconds
Agent Running : Running
Delay Timer Expiry : 300 seconds
Abort Timer Expiry : 299
Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.
Total Attempts : 1
Successful Transfers : 1 Failed Transfers : 0
Successful Reads : 1 Failed Reads : 0
Successful Writes : 0 Failed Writes : 0
```

3.7 DoS

3.7.1 dos

Command:

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

```
dos (daeqsa-deny | icmp-frag-pkts-deny | icmpv4-ping-max-check | icmpv6-ping-max-check | ipv6-min-frag-size-check | land-deny | nullscan-deny | pod-deny | smurf-deny | syn-sportl1024-deny | synfin-deny | synrst-deny | tcp-frag-off-min-check | tcpblat-deny | tcphdr-min-check | udpblat-deny | xma-deny)

no dos (daeqsa-deny | icmp-frag-pkts-deny | icmpv4-ping-max-check | icmpv6-ping-max-check | ipv6-min-frag-size-check | land-deny | nullscan-deny | pod-deny | smurf-deny | syn-sportl1024-deny | synfin-deny | synrst-deny | tcp-frag-off-min-check | tcpblat-deny | tcphdr-min-check | udpblat-deny | xma-deny)

dos icmp-ping-max-length <0-65535>

dos ipv6-min-frag-size-length <0-65535>

dos smurf-netmask <0-32>

dos tcphdr-min-length <0-31>
```

Parameter:

daeqsa-deny	Enable/Disable daeqsa-deny protection.
icmp-frag-pkts-deny	Enable/Disable icmp-frag-pkts-deny protection.
icmp-ping-max-length	Specify icmp-ping-max length.
icmpv4-ping-max-check	Enable/Disable icmpv4-ping-max-check protection.
icmpv6-ping-max-check	Enable/Disable icmpv6-ping-max-check protection.
ipv6-min-frag-size-check	Enable/Disable ipv6-min-frag-size-check protection.
ipv6-min-frag-size-length	Specify ipv6-min-fragsize length.
land-deny	Enable/Disable land-deny protection.
nullscan-deny	Enable/Disable nullscan-deny protection.
pod-deny	Enable/Disable pod-deny protection.
smurf-deny	Enable/Disable smurf-deny protection.
smurf-netmask	Specify smurf netmask.
syn-sportl1024-deny	Enable/Disable syn-sportl1024-deny protection.

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

synfin-deny	Enable/Disable synfin-deny protection.
synrst-deny	Enable/Disable synrst-deny protection.
tcp-frag-off-min-check	Enable/Disable tcp-frag-off-min-check protection.
tcpblat-deny	Enable/Disable tcpblat-deny protection.
tcphdr-min-check	Enable/Disable tcphdr-min-check protection.
tcphdr-min-length	Specify tcphdr-min length.
udpblat-deny	Enable/Disable udpblat-deny protection.
xma-deny	Enable/Disable xma-deny protection.

Default:

Default enable state of all DoS types are enabled.

Default smurf netmask length is 0.

Default tcphdr-min length is 20.

Default icmp-ping-max length is 512.

Default ipv6-min-frag-size length is 1240.

Mode:

Global Configuration

Usage Guide:

DoS is using to protect malicious attack from other devices. This command can configure DUT to enable/disable following types of attacks.

- **daeqsa-deny** : Destination MAC equals to source MAC
- **icmp-frag-pkts-deny** : Fragmented ICMP packets
- **icmp-ping-max-length** : DoS information
- **icmpv4-ping-max-check** : Check ICMPv4 ping maximum packets size
- **icmpv6-ping-max-check** : Check ICMPv6 ping maximum packets size
- **ipv6-min-frag-size-check** : Check minimum size of IPv6 fragments
- **ipv6-min-frag-size-length** : DoS information
- **land-deny** : Source IP equals to destination IP
- **nullscan-deny** : NULL Scan Attacks
- **pod-deny** : Ping of Death Attacks
- **smurf-deny** : Smurf Attacks
- **smurf-netmask** : DoS information
- **syn-sportl1024-deny** : SYN packets with sport less than 1024
- **synfin-deny** : SYN and FIN bits set in the packet
- **synrst-deny** : SYNC and RST bits set in the packet
- **tcp-frag-off-min-check** : TCP fragment packet with offset equals to one
- **tcpblat-deny** : Source TCP port equals to destination TCP port
- **tcphdr-min-check** : Check minimum TCP header

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

- **tcphdr-min-length** : DoS information
- **udpblat-deny** : Source UDP port equals to destination UDP port
- **xma-deny** : Xmascan: sequence number is zero and the FIN, URG and PSH bits are set

Example:

This example shows how to disable synfin-deny and smurf with netmask length 30.

```
Switch(config)# no dos synfin-deny
Switch(config)# dos smurf-netmask 30
```

This example shows how to show current dos state on interface gi1

```
Switch# show dos
Type | State (Length)
----------------------------+-----------------------
DMAC equal to SMAC | enabled
Land (DIP = SIP) | enabled
UDP Blat (DPORT = SPORT) | enabled
TCP Blat (DPORT = SPORT) | enabled
POD (Ping of Death) | enabled
IPv6 Min Fragment Size | enabled (1240 Bytes)
ICMP Fragment Packets | enabled
IPv4 Ping Max Packet Size | enabled (512 Bytes)
IPv6 Ping Max Packet Size | enabled (512 Bytes)
Smurf Attack | enabled (Netmask Length: 30)
TCP Min Header Length | enabled (20 Bytes)
TCP Syn (SPORT < 1024) | disabled
Null Scan Attack | enabled
X-Mas Scan Attack | enabled
TCP SYN-FIN Attack | enabled
TCP SYN-RST Attack | enabled
TCP Fragment (Offset = 1) | enabled
```

3.7.2 port dos

Command:

```
dos
```


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

```
no dos
```

Default:

Default value is disable

Mode:

Interface Configuration

Usage Guide:

Use “**dos**” command to enable dos configuration on selected ports. Use “**no dos**” to diable on selected ports.

Example:

This example shows how to show current dos state on interface gi1

```
Switch# show dos interfaces gi1
Port | DoS Protection | Gratuitous-ARP
----------+----------------+----------------
gi1 | enabled | disabled
```

3.7.3 ip gratuitous-arps

Command:

```
ip gratuitous-arps

no ip gratuitous-arps
```

Default:

Default value is disable

Mode:

Interface Configuration

Usage Guide:

Use “**ip gratuitous-arps**” command to enable dos configuration on selected ports. Use “**no ip gratuitous-arps**” to diable on selected ports.

Example:

This example shows how to show current dos state on interface gi1

```
Switch# show dos interfaces gi1
Port | DoS Protection | Gratuitous-ARP
----------+----------------+----------------
```


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

```
gi1 | enabled | disabled
```

3.7.4 show dos

Command:

```
show dos [interfaces IF_PORTS]
```

Parameter:

IF_PORTS Enable/Disable syn-fin protection.

Mode:

Privileged EXEC

Usage Guide:

Use "**show dos**" command to show dos configuration on selected ports

Example:

This example shows how to show current dos state on interface gi1

```
Switch# show dos interfaces gi1
Port | DoS Protection | Gratuitous-ARP
----------+----------------+----------------
gi1 | enabled | disabled
```


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

3.8 Dynamic ARP Inspection

3.8.1 ip arp inspection

Command:

```
ip arp inspection

no ip arp inspection
```

Default:

Dynamic Arp inspection is disabled

Mode:

Global Configuration

Usage Guide:

Use the **ip arp inspection** command to enable Dynamic Arp Inspection function. Use the **no** form of this command to disable.

Example:

The example shows how to enable Dynamic Arp Inspection on VLAN 1. You can verify settings by the following **show ip arp inspection** command.

```
switch(config)# ip arp inspection
switch(config)# ip arp inspection vlan 1
switch(config)# show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1
```

3.8.2 ip arp inspection vlan

Command:

```
ip arp inspection vlan VLAN-LIST

no ip arp inspection vlan VLAN-LIST
```

Parameter:

VLAN-LIST	Specify VLAN ID or a range of VLANs to enable or disable dynamic Arp inspection

Default:

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

Default is disabled on all VLANs

Mode:

Global Configuration

Usage Guide:

Use the **ip arp inspection vlan** command to enable VLANs on Dynamic Arp Inspection function. Use the **no** form of this command to disable VLANs on Dynamic Arp Inspection function.

Example:

The example shows how to enable VLAN 1-100 on Dynamic Arp Inspection, and then disable VLAN 30-40 on Dynamic Arp Inspection. You can verify settings by the following **show ip arp inspection** command.

```
switch(config)# vlan 1-100
switch(config)# exit
switch(config)# ip arp inspection
switch(config)# ip arp inspection vlan 1-100
switch(config)# show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1-100
switch(config)# no ip arp inspection vlan 30-40
switch(config)# show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1-29,41-100
```

3.8.3 ip arp inspection trust

Command:

```
ip arp inspection trust

no ip arp inspection trust
```

Default:

Dynamic Arp inspection trust is disabled

Mode:

Interface Configuration

Usage Guide:

Use the **ip arp inspection trust** command to set trusted interface. The switch does not check ARP packets that are received on the trusted interface; it simply forwards it. Use the **no** form of this command to set untrusted interface.

Example:

The example shows how to set interface gi1 to trust. You can verify settings by the following **show ip arp**

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

inspection interface command.

```
switch(config)# interface gi1
switch(config)# ip arp inspection trust
switch(config)# do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
------------+--------------+--------------+----------------|-----------------+-------------------------+
gi1 | Trusted | None | disabled | disabled | disabled/disabled
```

3.8.4 ip arp inspection validate

Command:

```
ip arp inspection validate src-mac

ip arp inspection validate dst-mac

ip arp inspection validate ip [allow-zeros]

no ip arp inspection validate src-mac

no ip arp inspection validate dst-mac

no ip arp inspection validate ip [allow-zeros]
```

Default:

Default is disabled of all validation

Mode:

Interface Configuration

Usage Guide:

Use the **ip arp inspection validate** command to enable validate function on interface.

The "**src-mac**" drop ARP requests and reply packets that arp-sender-mac and ethernet-source-mac is not match. The "**dst-mac**" drop ARP reply packets that arp-target-mac and ethernet-dst-mac is not match. The "**ip**" drop ARP request and reply packets that sender-ip is invalid such as broadcast、multicast、all zero IP address and drop ARP reply packets that target-ip is invalid. The "**allow-zeros**" means won't drop all zero IP address. Use the no form of this command to disable validation.

Example:

The example shows how to set interface gi1 to validate "**src-mac**" 、 "**dst-mac**" and "**ip allow zeros**". You can verify settings by the following **show ip arp inspection interface** command.

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

```
switch(config)# interface gi1
switch(config-if)# ip arp inspection validate src-mac
switch(config-if)# ip arp inspection validate dst-ma
switch(config-if)# ip arp inspection validate ip allow-zeros
switch(config)# do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
------------+--------------+--------------+----------------|----------------+------------------------+
gi1 | Untrusted | None | enabled | enabled | enabled/ enabled
```

3.8.5 ip arp inspection rate-limit

Command:

```
ip arp inspection rate-limit <1-50>

no ip arp inspection rate-limit
```

Parameter:

<1-50>	Set 1 to 50 PPS of DHCP packet rate limitation

Default:

Default is un-limited of ARP packet

Mode:

Interface Configuration

Usage Guide:

Use the i**p arp inspection rate-limit** command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second. Use the no form of this command to return to default settings.

Example:

The example shows how to set rate limit to 30 pps on interface gi1. You can verify settings by the following **show ip arp inspection interface** command.

```
switch(config)# interface gi1
switch(config)# ip arp inspection rate-limit 30
switch(config)# do show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
```


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

```
------------+--------------+--------------+---------------|----------------+-------------------------+
gi1 | Untrusted | 30 | disabled | disabled | disabled/disabled
```

3.8.6 clear ip arp inspection statistics

Command:

```
clear ip arp inspection interfaces IF_PORTS statistics
```

Parameter:

IF_PORTS specifies ports to clear statistics

Mode:

Global Configuration

Usage Guide:

Use the **clear ip arp inspection interfaces statistics** command to clear statistics that are recorded on interface.

Example:

The example shows how to clear statistics on interface gi1. You can verify settings by the following **show ip arp inspection interface statistics** command.

```
switch# clear ip arp inspection interfaces gi1 statistics
switch# show ip arp inspection interfaces gi1 statistics
Port| Forward |Source MAC Failures|Dest MAC Failures| SIP Validation Failures|DIP
Validation Failures|IP-MAC Mismatch Failures
----+---------+------------+-------------+------------+--------------+------------------
gi1| 0 | 0 | 0 | 0 | 0 | 0
```


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

3.8.7 show ip arp inspection

Command:

```
show ip arp inspection
```

Mode:

Global Configuration

Usage Guide:

Use the **show ip arp inspection** command to show settings of Dynamic Arp Inspection

Example:

The example shows how to show settings of Dynamic Arp Inspection

```
switch(config)# show ip arp inspection
Dynamic ARP Inspection : enabled
Enable on Vlans : 1
```

3.8.8 show ip arp inspection interface

Command:

```
show ip arp inspection interfaces IF_PORTS

show ip arp inspection interfaces IF_PORTS statistics
```

Parameter:

IF_PORTS	specifies ports to show statistics

Mode:

Global Configuration

Usage Guide:

Use the **show ip arp inspection interfaces** command to show settings or statistics of interface.

Example:

The example shows how to show settings of interface gi1.

```
switch# show ip arp inspection interface gi1
Interfaces | Trust State | Rate (pps) | SMAC Check | DMAC Check | IP Check/Allow Zero |
------------+--------------+--------------+----------------|----------------+------------------------+
gi1 | Trusted | None | disabled | disabled | disabled/disabled
```


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

The example shows how to show statistics of interface gi1.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
switch# show ip arp inspection interfaces gi1 statistics
Port| Forward |Source MAC Failures|Dest MAC Failures| SIP Validation Failures|DIP
Validation Failures|IP-MAC Mismatch Failures
----+---------+------------+-------------+------------+--------------+-------------------
gi1| 0 | 0 | 0 | 0 | 0 | 0
```


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

3.9 GVRP

3.9.1 gvrp

Command:

```
gvrp

no gvrp
```

Default:

no gvrp

Mode:

Global Configuration

Usage Guide:

'no gvrp' will clear all dynamic vlan entry. do not learn vlan.

The configure can use 'show gvrp'.

Example:

The following example specifies that set global gvrp test.

```
Switch(config)# gvrp
Switch# show gvrp
GVRP Status
--------------------
GVRP : Enabled
Join time : 200 ms
Leave time : 600 ms
LeaveAll time : 10000 ms
```

3.9.2 gvrp (port)

Command:

```
Gvrp
no gvrp
```

Default:

no gvrp

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

Mode:

Interface Configuration

Usage Guide:

'no gvrp' will remove dynamic port from vlan

'gvrp' must work at port mode is trunk.

The configure can use show gvrp configuration.

Example:

The following example specifies that set port gvrp test.

The port gvrp enable must set port mode is trunk firstly.

```
Switch(config)#interface gi1
Switch(config-if)# switchport mode trunk
Switch(config)#gvrp
Switch# show gvrp configuration interfaces gi1
Port | GVRP-Status | Registration | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
gi1 Enabled Normal Disabled
```

3.9.3 gvrp port registration mode

Command:

```
gvrp registration-mode (normal | fixed | forbidden)

show gvrp configuration
```

Parameter:

(normal | fixed | forbidden)	normal: register dynamic vlan, and transmit all vlan attribute. fixed: do not register dynamic vlan, and only transmit static vlan attribute. forbidden: do not register dynamic vlan, and only transmit default vlan attribute.

Mode:

Interface Configuration

Usage Guide:

When set registration-mode is fixed or forbidden, will remove the port from vlan witch is dynamic port. And do not learning vlan.

Example:

The following example specifies that set gvrp registration mode test.

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

```
Switch(config)# interface gi1
Switch(config-if)# gvrp registration-mode fixed
Switch# show gvrp configuration interfaces gi1
Port | GVRP-Status | Registration | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
gi1 Enabled Fixed Disabled
```

3.9.4 gvrp port creation vlan forbidden

Command:

```
gvrp vlan-creation-forbid

no gvrp vlan-creation-forbid
```

Default:

no gvrp vlan-creation-forbid

Mode:

Interface Configuration

Usage Guide:

'gvrp vlan-creation-forbid' will not remove dynamic port from vlan immediate.

The configure can use show gvrp configuration.

Example:

The following example specifies that set port gvrp vlan-creation-forbid test.

```
Switch(config)#interface gi1
Switch(config-if)# gvrp vlan-creation-forbid
Switch(config-if)#exit
Switch# show gvrp configuration interfaces gi1
Port | GVRP-Status | Registration | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
gi1 Enabled Normal Disabled
```

3.9.5 clear gvrp statistics

Command:

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

```
clear gvrp (error-statistics | statistics) [interfaces IF_PORTS]
```

Parameter:

(error-statistics | statistics)	Error-statistics: error gvrp packet statistics Statistics: gvrp event message statistics
[interfaces IF_PORTS]	Specifies posts to clear statistics

Mode:

Privileged Configuration

Usage Guide:

This command will clear the ports error statistics or statistics info.

The configure can use 'show gvrp error-statistics or show gvrp statistics' to check.

Example:

The following example specifies that clear gvrp error statistics and statistics test.

```
Switch# clear gvrp statistics
Switch# clear gvrp error-statistics
Switch# show gvrp statistics
Switch# show gvrp error-statistics
```

3.9.6 show gvrp statistics

Command:

```
show gvrp statistics [interfaces IF_PORTS]
show gvrp error-statistics [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Specifies posts

Mode:

Privileged Configuration

Usage Guide:

This command will display the ports error statistics or statistics info.

Example:

The following example specifies that display gvrp error statistics and statistics test.

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

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch# show gvrp statistics
Switch# show gvrp error-statistics
INVPROT : Invalid protocoal Id
INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length
INVAVAL : Invalid Attribute Value INVEVENT: Invalid Event
Port | INVPROT | INVATYP | INVALEN | INVAVAL | INVEVENT
gi1 0 0 0 0 0
gi2 0 0 0 0 0
gi3 0 0 0 0 0
gi4 0 0 0 0 0
gi5 0 0 0 0 0
gi6 0 0 0 0 0
```

3.9.7 show gvrp

Command:

```
show gvrp
```

Mode:

privileged Configuration

Usage Guide:

This command will display the gvrp global info.

Example:

The following example specifies that display gvrp test.

```
Switch# show gvrp
GVRP Status
--------------------
GVRP : Disabled
Join time : 200 ms
Leave time : 600 ms
LeaveAll time : 10000 ms
```


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

3.9.8 show gvrp port configuration

Command:

```
show gvrp configuration [interface IF_PORTS]
```

Parameter:

[interface IF_PORTS]	Display Specifies posts configuration

Mode:

Privileged Configuration

Usage Guide:

This command will display the ports configuration info.

Example:

The following example specifies that display gvrp port configuration test.

```
Switch# show gvrp configuration
Port | GVRP-Status | Registration | Dynamic VLAN Creation
--------+---------------+---------------+----------------------
gi1 Disabled Normal Enabled
gi 2 Disabled Normal Enabled
gi 3 Disabled Normal Enabled
gi 4 Disabled Normal Enabled
gi 5 Disabled Normal Enabled
gi 6 Disabled Normal Enabled
gi 7 Disabled Normal Enabled
--More--
```


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

3.10 IGMP Snooping

3.10.1 Ip igmp snooping

Command:

```
ip igmp snooping

no ip igmp snooping
```

Mode:

Global Configuration

Usage Guide:

'no ip igmp snooping' will clear all ip igmp snooping dynamic group and dynamic router port, and make the static ip igmp group invalid. Then do not learning the dynamic group and router port by igmp message.

The configure can use 'show ip igmp snooping'.

Example:

The following example specifies that set ip igmp snooping test.

```
Switch(config)# ip igmp snooping
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Enabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Flood
Switch(config)# no ip igmp snooping
Switch# show ip igmp snooping
```

3.10.2 ip igmp snooping report-suppression

Command:

```
ip igmp snooping report-suppression

no ip igmp snooping report-suppression
```

Default:

ip igmp snooping report-suppression

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

Mode:

Global Configuration

Usage Guide:

'no ip igmp snooping report-suppression' will disable igmp v1/v2 igmp report suppression function. So when receive report will forward to the vlan router ports.

The configure can use 'show ip igmp snooping'.

Example:

The following example specifies that disable ip igmp snooping report-suppression test.

```
Switch(config)# no ip igmp snooping report-suppression
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Disabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Flood
```

3.10.3 ip igmp snooping version

Command:

```
ip igmp snooping version (2|3)
```

Parameter:

(2|3)	IP igmp snooping running version 2 or 3

Default:

ip igmp snooping version 2

Mode:

Global Configuration

Usage Guide:

'ip igmp snooping version 3', then will support v3 basic mode. When change version from v3 to v2. the all querier version will update to version 2.

The configure can use 'show ip igmp snooping'.

Example:

The following example specifies that set ip igmp snooping version 3 test.

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

```
Switch(config)# ip igmp snooping version 3
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Disabled
Operation Version : v3
Forward Method : mac
Unknown Multicast Action : Flood
```

3.10.4 ip igmp snooping unknown-multicast action

Command:

```
ip igmp snooping unknown-multicast action (drop | flood |router-port)
```

Parameter:

(drop | flood |router-port)	Unknown multicast action for drop|flood|router-port

Default:

ip igmp snooping unknown-multicast action flood

Mode:

Global Configuration

Usage Guide:

When igmp snooping and mld snooping disabled, it can't set action router-port.

When disable igmp snooping & mld snooping, it set unknown multicast action flood.

When action is router-port to flood or drop, it will delete the unknown multicast group entry.

The configure can use 'show ip igmp snooping'.

Example:

The following example specifies that set ip igmp unknown multicast action router-port test.

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping unknown-multicast action router-port
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Enabled
```


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

```
Report Suppression : Disabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Router Port
Switch(config)# no ip igmp snooping
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Disabled
Report Suppression : Disabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Flood
```

3.10.5 ip igmp snooping forward-method

Command:

```
ip igmp snooping forward-method (mac |src-dst-ip)
```

Parameter:

(mac |src-dst-ip) Multicast lookup method is DMAC OR DIP+SIP

Default:

ip igmp snooping forward-method mac

Mode:

Global Configuration

Usage Guide:

When change lookup method, it will remove all groups.

The configure can use 'show ip igmp snooping'.

Example:

The following example specifies that set ip igmp lookup method is src-dst-ip test.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# ip igmp forward-method src-dst-ip
Switch# show ip igmp snooping
IGMP Snooping Status
```


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

```
--------------------
Snooping : Disabled
Report Suppression : Disabled
Operation Version : v2
Forward Method : src-dst-ip
```

3.10.6 ip igmp snooping querier

Command:

```
ip igmp snooping vlan <VLAN-LIST> querier

no ip igmp snooping [vlan <VLAN-LIST>] querier

ip igmp snooping vlan <VLAN-LIST> querier version (2|3)
```

Parameter:

<VLAN-LIST>	specifies VLAN ID list to set
(2|3)	Query version 2 or 3

Mode:

Global Configuration

Usage Guide:

When enable ip igmp vlan querier, there will process router select, the select successful will send general and specific query.

The configure can use 'show ip igmp snooping querier'.

Example:

The following example specifies that set ip igmp snooping querier test.

Test must be create static vlan firstly.

```
Switch(config)# vlan 2
Switch(config-vlan)# exit
Switch(config)# ip igmp snooping vlan 2 querier
Switch(config)#exit
Switch#show ip igmp snooping querier
VID | State | Status | Version | Querier IP
-------+-------------+-------------+------------+--------------------
```


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

```
1 | Disabled | Non-Querier | No | ------
2 | Enabled | Querier | v2 | 192.168.1.254
Switch#configure
Switch(config)#ip igmp snooping version 3
Switch(config)# ip igmp snooping vlan 2 querier version 3
Switch(config)#do show ip igmp snooping queier
VID | State | Status | Version | Querier IP
-------+-------------+-------------+------------+--------------------
1 | Disabled | Non-Querier | No | ------
2 | Enabled | Querier | v3 | 192.168.1.254
Switch(config)#no ip igmp snooping queier
Switch(config)#do show ip igmp snooping queier
```

3.10.7 ip igmp snooping vlan

Command:

```
ip igmp snooping vlan VLAN-LIST
no ip igmp snooping vlan VLAN-LIST
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set

Default:

no ip igmp snooping vlan 1-4094

Mode:

Global Configuration

Usage Guide:

'no ip igmp snooping vlan 1' will clear vlan all ip igmp snooping dynamic group and dynamic router port, and make the static ip igmp group invalid witch vlan ID is vlan 1. Then do not learning the dynamic group and router port by igmp message for vlan 1.

The configure can use show ip igmp snooping vlan 1.

Example:

The following example specifies that set ip igmp snooping vlan test.

Test must be enable ip igmp snooping firstly.

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

```
Switch(config)# ip igmp snooping
Switch(config)# ip igmp snooping vlan 1
Switch# show ip igmp snooping vlan 1
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : enabled
IGMP Snooping operation mode : enabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 125 sec oper 125 sec
IGMP Snooping query max response : admin 10 sec oper 10 sec
IGMP Snooping last member query counter: admin 2 oper 2
IGMP Snooping last member query interval: admin 1 sec oper 1 sec
IGMP Snooping last immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
Switch(config)# no ip igmp snooping vlan 1
Switch# show ip igmp snooping vlan 1
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 125 sec oper 125 sec
IGMP Snooping query max response : admin 10 sec oper 10 sec
IGMP Snooping last member query counter: admin 2 oper 2
IGMP Snooping last member query interval: admin 1 sec oper 1 sec
IGMP Snooping last immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

3.10.8 ip igmp snooping vlan parameters

Command:

```
ip igmp snooping vlan <VLAN-LIST> last-member-query-count <1-7>

no ip igmp snooping vlan <VLAN-LIST> last-member-query-count

ip igmp snooping vlan <VLAN-LIST> last-member-query-interval <1-60>

no ip igmp snooping vlan <VLAN-LIST> last-member-query-interval

[no] ip igmp snooping vlan <VLAN-LIST> router learn pim-dvmrp
```


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

```
[no] ip igmp snooping vlan <VLAN-LIST> fastleave

ip igmp snooping vlan <VLAN-LIST> query-interval <30-18000>

no ip igmp snooping vlan <VLAN-LIST> query-interval

ip igmp snooping vlan <VLAN-LIST> response-time <5-20>

no ip igmp snooping vlan <VLAN-LIST> response-time

ip igmp snooping vlan <VLAN-LIST> robustness-variable <1-7>

no ip igmp snooping vlan <VLAN-LIST> robustness-variable
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
last-member-query-count <1-7>	specifies last member query count to set. Default is 2
last-member-query-interval <1-60>	specifies last member query interval to set. Default is 1
query-interval <30-18000>	specifies query interval to set. Default is 125
response-time <5-20>	specifies a response time to set. default is 10
robustness-variable <1-7>	specifies a robustness value to set, default is 2

Default:

no ip igmp snooping vlan 1-4094 last-member-query-count

no ip igmp snooping vlan 1-4094 last-member-query-interval

ip igmp snooping vlan 1-4094 router learn pim-dvmrp

no ip igmp snooping vlan 1-4094 fastleave

no ip igmp snooping vlan 1-4094 query-interval

no ip igmp snooping vlan 1-4094 response-time

no ip igmp snooping vlan 1-4094 robustness-variable

Mode:

Global Configuration

Usage Guide:

‘no ip igmp snooping vlan 1 (last-member-query-count | last-member-query-interval | query-interval | response-time |

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

robustness-variable)' will set the vlan parameters to default.

The cli setting will change the ip igmp vlan parameters admin settings.

The configure can use show ip igmp snooping vlan 1.

Example:

The following example specifies that set ip igmp snooping vlan parameters test.

```
Switch(config)# ip igmp snooping vlan 1 fastleave
Switch(config)# ip igmp snooping vlan 1 last-member-query-count 5
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3
Switch(config)# ip igmp snooping vlan 1 query-interval 100
Switch(config)# ip igmp snooping vlan 1 response-time 12
Switch(config)# ip igmp snooping vlan 1 robustness-variable 4
Switch# show ip igmp snooping vlan 1
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : enabled
IGMP Snooping operation mode : enabled
IGMP Snooping robustness: admin 4 oper 2
IGMP Snooping query interval: admin 100 sec oper 125 sec
IGMP Snooping query max response : admin 12 sec oper 10 sec
IGMP Snooping last member query counter: admin 5 oper 2
IGMP Snooping last member query interval: admin 3 sec oper 1 sec
IGMP Snooping last immediate leave: enabled
IGMP Snooping automatic learning of multicast router ports: enabled
```

3.10.9 ip igmp snooping static port

Command:

```
[no] ip igmp snooping vlan <VLAN-LIST> static-port IF_PORTS

[no] ip igmp snooping vlan <VLAN-LIST> forbidden-port IF_PORTS
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
IF_PORTS	specifies a port list to set or remove

Default:

None static/forbidden ports

Mode:

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

Global Configuration

Usage Guide:

'ip igmp snooping vlan 1 static-port gi1-2' will add static port gi1-2 for vlan 1.the all known vlan 1 ipv4 group will add the static ports.

'ip igmp snooping vlan 1 forbidden-port gi3-4' will add forbidden port gi3-4 for vlan 1.the all known vlan 1 ipv4 group will remove the forbidden ports.

The configure can use 'show ip igmp snooping forward-all'.

Example:

The following example specifies that set ip igmp snooping static/forbidden port test.

```
Switch(config)# ip igmp snooping vlan 1 static -port gi1-2
Switch(config)# ip igmp snooping vlan 1 forbidden -port gi3-4
Switch# show ip igmp snooping forward-all vlan 1
IGMP Snooping VLAN : 1
IGMP Snooping static port : gi1-2
IGMP Snooping forbidden port : gi3-4
```

3.10.10 ip igmp snooping vlan static router port

Command:

```
[no] ip igmp snooping vlan <VLAN-LIST> static-router-port IF_PORTS

[no] ip igmp snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
IF_PORTS	specifies a port list to set or remove

Default:

None static/forbidden router ports

Mode:

Global Configuration

Usage Guide:

'ip igmp snooping vlan 1 static-router-port gi1-2' will add static router port gi1-2 for vlan 1.

'ip igmp snooping vlan 1 forbidden-router-port gi2' will add forbidden router port gi2 for vlan 1.

This will also remove gi2 from static router port. The forbidden router port receive query will not forward.

The configure can use 'show ip igmp snooping router'.

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

Example:

The following example specifies that set ip igmp snooping static/forbidden test.

```
Switch(config)# ip igmp snooping vlan 1 static-router-port gi1-2
Switch(config)# ip igmp snooping vlan 1 forbidden-router-port gi2
Switch# show ip igmp snooping router
Dynamic Router Table
VID | Port | Expiry Time(Sec)
------+---------+------------------
Total Entry 0
Static Router Table
VID | Port Mask
------+------------------------
1 | gi1
Total Entry 1
Forbidden Router Table
VID | Port Mask
------+------------------------
1 | gi2
Total Entry 1
```

3.10.11 ip igmp snooping static group

Command:

```
[no] ip igmp snooping vlan <VLAN-LIST> static-group <ip-addr> interfaces
IF_PORTS

[no] ip igmp snooping vlan <VLAN-LIST> group <ip-addr>

show ip igmp snooping groups [(dynamic | static)]

clear ip igmp snooping groups [(dynamic | static)]
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
ip-addr	specifies multicast group ipv4 address
IF_PORTS	specifies port list to set or remove

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

Mode:

Global Configuration

Usage Guide:

'ip igmp snooping vlan 1 static-group 224.1.1.1 interfaces gi1' will add static group.

The static group will not learning others dynamic port. If the dynamic group exist, then the static group will overlap the dynamic group. If remove the last member of static group, the static group will be delete.

The static group want to valid , must igmp snooping vlan enable and ip igmp snooping enable.

The configure can use 'show ip igmp snooping group [(dynamic | static)]' to display. And can use 'no ip igmp snooping vlan 1 group 224.1.1.1' to delete the static group. Also can use 'clear ip igmp snooping groups' to delete the static group.

Example:

The following example specifies that set ip igmp snooping static group test.

```
Switch(config)# ip igmp snooping vlan 1 static-group 224.1.1.1 interfaces gi1-2
Switch# show ip igmp snooping groups
VLAN | Gourp IP Address | Type | Life(Sec) | Port
------+------------------+--------+-----------+------------------
1 | 224.1.1.1 | Static| -- | gi1-2
Total Number of Entry = 1
Switch# clear ip igmp snooping groups static
Switch# show ip igmp snooping groups
VLAN | Gourp IP Address | Type | Life(Sec) | Port
------+------------------+--------+-----------+------------------
Total Number of Entry = 0
```


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

3.10.12 ip igmp profile

Command:

```
ip igmp profile <1-128>

profile range ip <ip-addr> [ip-addr] action (permit | deny)

show ip igmp profile [<1-128>]
```

Parameter:

<1-128>	specifies profile ID
<ip-addr>	Start ipv4 multicast address
[ip-addr]	End ipv4 multicast address
(permit | deny)	Permit: allow Multicast address range ip address learning
	deny: do not allow Multicast address range ip address learning

Mode:

ip igmp profile <1-128>

Global Configuration

profile range ip <ip-addr> [ip-addr] action (permit | deny)

igmp profile config mode

Usage Guide:

Use 'ip igmp profile 1' entry to the igmp profile config mode.

User 'profile range ip 224.1.1.1 224.1.1.8 action permit' to configure the profile entry.

The profile entry is used by port filter.

The configure can use 'show ip igmp profile [<1-128>]' to display

Example:

The following example specifies that set ip igmp profile test.

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit
Switch(config-igmp-profile)#show ip igmp profile
IP igmp profile index: 1
IP igmp profile action: permit
Range low ip: 224.1.1.1
Range high ip: 224.1.1.8
Switch(config-igmp-profile)#exit
Switch(config)# ip igmp profile 10
```


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

```
Switch(config-igmp-profile)# profile range ip 224.1.1.5 224.1.1.10 action deny
Switch(config-igmp-profile)#show ip igmp profile
IP igmp profile index: 10
IP igmp profile action: deny
Range low ip: 224.1.1.5
Range high ip: 224.1.1.10
Switch(config-igmp-profile)#exit
Switch(config)# exit
Switch# show ip igmp profile
IP igmp profile index: 1
IP igmp profile action: permit
Range low ip: 224.1.1.1
Range high ip: 224.1.1.8
IP igmp profile index: 10
IP igmp profile action: deny
Range low ip: 224.1.1.5
Range high ip: 224.1.1.10
```

3.10.13 ip igmp filter

Command:

```
ip igmp filter <1-128>

[no] ip igmp filter

show ip igmp filter [interfaces IF_PORTS]
```

Parameter:

<1-128>	specifies profile ID
[interfaces IF_PORTS]	Specifies interfaces to display

Mode:

Interface Configuration

Usage Guide:

After create ip igmp profile entry. Can use ‘ip igmp filter 1’ to bind a profile for port.

When the port bind a profile. Then the port learning group will update, if the group is not match the profile rule it will

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

remove the port from the group. static group is excluded.

The configure can use 'show ip igmp filter ' to display

Example:

The following example specifies that set ip igmp filter test.

The configure must create ip igmp profile firstly.

```
Switch(config)# ip igmp profile 1
Switch(config-igmp-profile)# profile range ip 224.1.1.1 224.1.1.8 action permit
Switch(config-igmp-profile)#exit
Switch(config)# interface gi1
Switch(config-if)#ip igmp filter 1
Switch(config-if)#exit
Switch(config)# exit
Switch# show ip igmp filter
Port ID | Profile ID
---------+--------------
gi1 : 1
gi2 : None
gi3 : None
--More--
```

3.10.14 ip igmp max-group

Command:

```
ip igmp max-groups <0-256>

no ip igmp max-groups
ip igmp max-groups action (deny | replace)
show ip igmp max-group [interfaces IF_PORTS]

show ip igmp max-group action [interfaces IF_PORTS]
```

Parameter:

<1-128>	specifies profile ID
(deny | replace)	Deny: current port igmp group arrived max-groups, don't add group. Replace: current port igmp group arrived max-groups, remove port for rand group, and add port to new group.

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

Default:

no ip igmp max-groups

ip igmp max-groups action deny

Mode:

Interface Configuration

Usage Guide:

use 'ip igmp max-groups 10' to limit port learning max group num is 10.

When the port had learned more than 10 groups, then the more than 10 group will be remove the port form group.

static group is excluded.

The configure can use 'show ip igmp max-group & show ip igmp max-group action ' to display

Example:

The following example specifies that set ip igmp max-groups and action is replace test.

```
Switch(config)# interface gi1
Switch(config-if)#ip igmp max-groups 10
Switch(config-if)#ip igmp max-groups action replace
Switch(config-if)#exit
Switch(config)# exit
Switch# show ip igmp max-group
Port ID | Max Group
---------+--------------
gi1 : 10
gi2 : 256
gi3 : 256
--More--
Switch# show ip igmp max-group action
Port ID | Max-groups Action
---------+---------------------
gi1 : replace
gi2 : deny
gi3 : deny
gi4 : deny
gi5 : deny
gi6 : deny
--More--
```

3.10.15 clear ip igmp snooping groups

Command:

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

```
clear ip igmp snooping groups [(dynamic | static)]
```

Parameter:

(dynamic | static) IP igmp group type is dynamic or static

Mode:

Privileged Configuration

Usage Guide:

This command will clear the ip igmp groups for dynamic or static or all of type.

The configure can use 'show ip igmp snooping groups' to check.

Example:

The following example specifies that clear ip igmp snooping groups test.

```
Switch# clear ip igmp snooping groups static
Switch# show ip igmp snooping groups
Switch# clear ip igmp snooping groups
Switch# show ip igmp snooping groups
```

3.10.16 clear ip igmp snooping statistics

Command:

```
clear ip igmp snooping statistics
```

Mode:

Privileged Configuration

Usage Guide:

This command will clear the igmp statistics.

The configure can use show ip igmp snooping.

Example:

The following example specifies that clear ip igmp snooping statistics test.

```
Switch# clear ip igmp snooping statistics
Switch# show ip igmp snooping
```

3.10.17 show ip igmp snooping counters

Command:

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

```
show ip igmp snooping groups counters
```

Mode:

Privileged Configuration

Usage Guide:

This command will display the ip igmp group counter include static group.

Example:

The following example specifies that display ip igmp snooping group counter test.

```
Switch# show ip igmp snooping counters
Total ip igmp snooping group number: 0
```

3.10.18 show ip igmp snooping groups

Command:

```
show ip igmp snooping groups [(dynamic | static)]
```

Parameter:

(dynamic | static)	Display Ip igmp group type is dynamic or static

Mode:

Privileged Configuration

Usage Guide:

This command will display the ip igmp groups for dynamic or static or all of type.

Example:

The following example specifies that show ip igmp snooping groups test.

```
Switch# show ip igmp snooping groups
Switch# show ip igmp snooping groups dynamic
Switch# show ip igmp snooping groups static
```

3.10.19 show ip igmp snooping router

Command:

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

```
show ip igmp snooping router [(dynamic | forbidden |static )]
```

Parameter:

(dynamic | forbidden | static)	Display Ip igmp router info for different type

Mode:

Privileged Configuration

Usage Guide:

This command will display the ip igmp router info.

Example:

The following example specifies that show ip igmp snooping router test.

```
Switch# show ip igmp snooping router
Switch# show ip igmp snooping router dynamic
Switch# show ip igmp snooping rotuer static
Switch# show ip igmp snooping rotuer forbidden
```

3.10.20 show ip igmp snooping querier

Command:

```
show ip igmp snooping querier
```

Mode:

Privileged Configuration

Usage Guide:

This command will display all of the static vlan ip igmp querier info.

Example:

The following example specifies that show ip igmp snooping querier test.

```
Switch# show ip igmp snooping querier
VID | State | Status | Version | Querier IP
-------+-------------+-------------+------------+--------------------
1 | Disabled | Non-Querier | No | ------
Total Entry 1
```


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

3.10.21 show ip igmp snooping

Command:

```
show ip igmp snooping
```

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp snooping global info.

Example:

The following example specifies that show ip igmp snooping test.

```
Switch# show ip igmp snooping
IGMP Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Enabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Flood
Packet Statistics
Total RX : 0
Valid RX : 0
Invalid RX : 0
Other RX : 0
Leave RX : 0
Report RX : 0
General Query RX : 0
Specail Group Query RX : 0
Specail Group & Source Query RX : 0
Leave TX : 0
Report TX : 0
General Query TX : 0
Specail Group Query TX : 0
Specail Group & Source Query TX : 0
```


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

3.10.22 show ip igmp snooping vlan

Command:

```
show ip igmp snooping vlan [VLAN-LIST]
```

Parameter:

[VLAN-LIST]	Show specifies vlan ip igmp snooping info

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp snooping vlan info.

Example:

The following example specifies that show ip igmp snooping vlan test.

```
Switch# show ip igmp snooping vlan
IGMP Snooping is globaly enabled
IGMP Snooping VLAN 1 admin : disabled
IGMP Snooping operation mode : disabled
IGMP Snooping robustness: admin 2 oper 2
IGMP Snooping query interval: admin 125 sec oper 125 sec
IGMP Snooping query max response : admin 10 sec oper 10 sec
IGMP Snooping last member query counter: admin 2 oper 2
IGMP Snooping last member query interval: admin 1 sec oper 1 sec
IGMP Snooping last immediate leave: disabled
IGMP Snooping automatic learning of multicast router ports: enabled
```


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

3.10.23 show ip igmp snooping forward-all

Command:

```
show ip igmp snooping forward-all [vlan VLAN-LIST]
```

Parameter:

[vlan VLAN-LIST] Show specifies vlan of ip igmp forward info.

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp snooping forward all info.

Example:

The following example specifies that show ip igmp snooping forward-all test.

```
Switch# show ip igmp snooping forward-all
IGMP Snooping VLAN : 1
IGMP Snooping static port : None
IGMP Snooping forbidden port : None
```

3.10.24 show ip igmp profile

Command:

```
show ip igmp profile [<1-128>]
```

Parameter:

[<1-128>] Show specifies index profile info

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp profile info.

Example:

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

The following example specifies that show ip igmp profile test.

```
Switch# show ip igmp profile
IP igmp profile index: 1
IP igmp profile action: permit
Range low ip: 224.1.1.1
Range high ip: 224.1.1.8
IP igmp profile index: 2
IP igmp profile action: deny
Range low ip: 225.1.1.0
Range high ip: 225.1.2.1
```

3.10.25 show ip igmp port filter

Command:

```
show ip igmp filter [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports filter

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp port filter info.

Example:

The following example specifies that show ip igmp filter test.

```
Switch# show ip igmp filter
Port ID | Profile ID
---------+--------------
gi1 : 1
gi2 : None
gi3 : None
gi4 : None
gi5 : None
```


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

```
--More--
```

3.10.26 show ip igmp port max-group

Command:

```
show ip igmp max-group [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports max-group

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp port max-group.

Example:

The following example specifies that show ip igmp max-group test.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)#interface gi1
Switch(config-if)#ip igmp max-groups 50
Switch(config-if)#exit
Switch(config)#exit
Switch# show ip igmp max-group
Port ID | Max Group
---------+--------------
gi1 : 50
gi2 : 256
gi3 : 256
gi4 : 256
gi5 : 256
--More--
```

3.10.27 show ip igmp port max-group action

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

Command:

```
show ip igmp max-group action [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports max-group action

Mode:

Privileged Configuration

Usage Guide:

This command will display ip igmp port max-group action.

Example:

The following example specifies that show ip igmp max-group action test.

```
Switch(config)#interface gi1
Switch(config-if)#ip igmp max-groups action replace
Switch(config-if)#exit
Switch(config)#exit
Switch# show ip igmp max-group action
Port ID | Max-groups Action
---------+---------------------
gi1 : replace
gi2 : deny
gi3 : deny
gi4 : deny
gi5 : deny
--More--
```


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

3.11 IP Source Guard

3.11.1 ip source verify

Command:

```
ip source verify

ip source verify mac-and-ip

no ip source verify
```

Mode:

Interface Configuration

Usage Guide:

Use the **ip source verify** command to enable IP Source Guard function. Default IP Source Guard filter source IP address. The "**mac-and-ip**" filters not only source IP address but also source IP address. Use the **no** form of this command to disable

Example:

The example shows how to enable IP Source Guard with source IP address filtering on interface gi1.

```
Switch(config)# interface gi1
switch(config-if)# ip source verify
```

The example shows how to enable IP Source Guard with source IP and MAC address filtering on interface gi2. You can verify settings by the following **show ip source interfaces** command.

```
Switch(config)# interface gi2
switch(config-if)# ip source verify mac-and-ip
switch(config-if)# do show ip source interfaces gi1-2
Port | Status | Max Entry | Current Entry
----------+--------------------+-------------+---------------
gi1 | Verify MAC+IP | No Limit | 0
gi2 | disabled | No Limit | 0
```

3.11.2 ip source binding

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

Command:

```
ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT

no ip source binding A:B:C:D:E:F vlan <1-4094> A.B.C.D interface IF_PORT
```

Parameter:

A:B:C:D:E:F	Specify a MAC address of a binding entry
VLAN <1-4094>	Specify a VLAN ID of a binding entry
A.B.C.D	Specify IP address and MASK of a binding entry.
IF_PORT	Specify interface of a binding entry.

Mode:

Global Configuration

Usage Guide:

Use the **ip source binding** command to create a static IP source binding entry has an IP address, its associated MAC address、VLAN ID、interface. Use the **no** form of this command to delete static entry.

Example:

The example shows how to add a static IP source binding entry. You can verify settings by the following **show ip source binding** command.

```
Switch(config)# ip source binding 00:11:22:33:44:55 vlan 1 192.168.1.55 interface gi1
switch(config)# do show ip source binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address | IP | Type | Lease Time
--------+------+--------------------+--------------------------------------+-------------+-----------
gi1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255)| Static | NA
```

3.11.3 show ip source interface

Command:

```
show ip source interfaces IF_PORTS
```

Parameter:

IF_PORTS	specifies ports to show

Mode:

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

Global Configuration

Usage Guide:

Use the **show ip source interface** command to show settings of IP Source Guard of interface

Example:

The example shows how to show settings of IP Source Guard of interface gi1

```
switch# show ip source interfaces gi1
Port | Status | Max Entry | Current Entry
----------+--------------------+-------------+---------------
gi1 | Verify MAC+IP | No Limit | 0
```

3.11.4 show ip source binding

Command:

```
show ip source binding [(dynamic|static)]
```

Parameter:

dynamic	Show entries that added by DHCP snooping learn
static	Show entries that added by user

Mode:

Global Configuration

Usage Guide:

Use the **show ip source binding** command to show binding entries of IP Source Guard.

Example:

The example shows how to show static binding entries of IP Source Guard.

```
switch# show ip source binding
Bind Table: Maximun Binding Entry Number 192
Port | VID | MAC Address | IP | Type | Lease Time
--------+------+--------------------+-------------------------------------+-------------+-----------
gi1 | 1 | 00:11:22:33:44:55 | 192.168.1.55(255.255.255.255)| Static | NA
```

3.12 Link Aggregation

3.12.1 lag load-balance

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

Command:

```
lag load-balance (src-dst-mac | src-dst-mac-ip)
```

Parameter:

src-dst-mac	Specify algorithm to balance traffic by using source and destination MAC address for all packets.
src-dst-mac-ip	Specify algorithm to balance traffic by using source and destination IP address for IP packets and using source and destination MAC address for non-IP packets.

Default:

Default load balance algorithm is src-dst-mac

Mode:

Global Configuration

Usage Guide:

Link aggregation group port should transmit packets spread to all ports to balance traffic loading. There are two algorithm supported and this command allow you to select the algorithm.

Example:

This example shows how to change load balance algorithm to src-dst-mac-ip.

```
Switch(config)# lag load-balance src-dst-mac-ip
```

This example shows how to show current load balance algorithm.

```
Switch# show lag
Load Balancing: src-dst-mac-ip.
Group ID | Type | Ports
---------+----------+---------------------------------------
1 | --------- |
2 | --------- |
3 | --------- |
4 | --------- |
5 | --------- |
6 | --------- |
7 | --------- |
8 | --------- |
```

3.12.2 lacp system-priority

Command:

```
lacp system-priority <1-65535>
```


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

```
no lacp system-priority
```

Parameter:

<1-65535> Specify system priority value

Default:

Default system priority is 1.

Mode:

Global Configuration

Usage Guide:

LACP system priority is used for two connected DUT to select master switch. Lower system priority value has higher priority. And the DUT with higher priority can decide which ports are able to join the LAG.

Use "**no lacp system-priority**" to restore to the default priority value. The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure lacp system priority to 1000.

```
Switch(config)# lacp system-priority 1000
```

3.12.3 lacp port-priority

Command:

```
lacp port-priority <1-65535>
```

Parameter:

<1-65535> Specify port priority value

Default:

Default port priority is 1.

Mode:

Interface Configuration

Usage Guide:

LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. And the port with higher priority will be selected into LAG first.

The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure interface fa1 lacp port priority to 100.

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

```
Switch(config)# interface gi1
Switch(config-if)# lacp port-priority 100
```

3.12.4 lacp timeout

Command:

```
lacp timeout (long | short)
```

Parameter:

long	Send LACP packet every 30 seconds.
short	Send LACP packet every 1 seconds.

Default:

Default LACP timeout is long.

Mode:

Interface Configuration

Usage Guide:

LACP need to send LACP packet to partner switch to check the link status. This command configure the interval of sending LACP packets.

The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure interface gi1 lacp timeout to short.

```
Switch(config)# interface gi1
Switch(config-if)# lacp timeout short
```

3.12.5 lag

Command:

```
lag <1-8> mode (static | active | passive)

no lag
```


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

Parameter:

<1-8>	Specify the LAG id for the interface
static	Specify the LAG to be static mode and join the interface into this LAG.
active	Specify the LAG to be dynamic mode and join the interface into this LAG with LACP active port.
passive	Specify the LAG to be dynamic mode and join the interface into this LAG with LACP passive port.

Mode:

Interface Configuration

Usage Guide:

Link aggregation group function allows you to aggregate multiple physical ports into one logic port to increase bandwidth. This command makes normal port join into the specific LAG logic port with static or dynamic mode. And use "**no lag**" to leave the LAG logic port.

Example:

This example shows how to create a dynamic LAG and join gi1-gi3 to this LAG.

```
Switch(config)# lag load-balance src-dst-mac-ip
Switch(config)# interface range gi1-3
Switch(config-if)# lag 1 mode active
```

This example shows how to show current LAG status.

```
Switch# show lag
Load Balancing: src-dst-mac-ip.
Group ID | Type | Ports
---------+--------+---------------------------------------
1 | LACP | Inactive: gi1-3
2 | ------ |
3 | ------ |
4 | ------ |
5 | ------ |
6 | ------ |
7 | ------ |
8 | ------ |
```

3.12.6 show lag

Command:

```
Show lag
```

Mode:

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

Usage Guide:

Use “**show lag**” command to show current LAG load balance algorithm and members active/inactive status.

Example:

This example shows how to show current LAG status.

```
Switch# show lag
Load Balancing: src-dst-mac-ip.
Group ID | Type | Ports
---------+--------+----------------------------------------
1 | LACP | Inactive: gi1-3
2 | ------ |
3 | ------ |
4 | ------ |
5 | ------ |
6 | ------ |
7 | ------ |
8 | ------ |
```


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

3.13 LLDP

3.13.1 lldp

Command:

```
lldp

no lldp
```

Mode:

Global Configuration

Usage Guide:

The “lldp” command globally enable LLDP RX/TX ability. “no lldp run” command disables the LLDP RX/TX ability and the behavior when receiving LLDP PDU would be decided by “lldp lldpdu” command. The LLDP enable status is displayed by “show lldp” command.

Example:

The following example sets LLDP enable/disable.

```
Switch(config)# lldp
Switch# show lldp
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Switch(config)# no lldp
Switch# show lldp
State: Disabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

3.13.2 lldp tx-interval

Command:

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

```
lldp tx-interval <5-32768>
```

Parameter:

<5-32768>	Specify the LLDP PDU TX interval in unit of second.

Default:

lldp tx-interval 30

Mode:

Global Configuration

Usage Guide:

This command globally configures the LLDP TX interval. It should be noticed that both “lldp tx-interval” and “lldp tx-delay” affects the LLDP PDU TX time. The larger value of the two configuration decides the TX interval. The configuration could be shown by “show lldp” command.

Example:

This example sets LLDP TX interval to 10 seconds.

```
Switch(config)# lldp tx-interval 10
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

3.13.3 lldp reinit-delay

Command:

```
lldp reinit-delay <1-10>
```

Parameter:

<1-10>	Specify the LLDP re-initial delay time in unit of second.

Default:

lldp reinit-delay 2

Mode:

Global Configuration

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

Usage Guide:

This command globally configures the LLDP re-initial delay. This delay avoids LLDP generate too many PDU if the port is up and down frequently. The delay starts to count when the port links down. The port would not generate LLDP PDU until the delay counts to zero. The configuration could be shown by “show lldp” command.

Example:

This example sets LLDP re-initial delay to 5 seconds.

```
Switch(config)# lldp reinit-delay 5
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 5 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

3.13.4 lldp holdtime-multiplier

Command:

```
lldp holdtime-multiplier <2-10>
```

Parameter:

<2-10>	Specify the LLDP hold time multiplier.

Default:

lldp holdtime-multiplier 4

Mode:

Global Configuration

Usage Guide:

This command globally configures the LLDP PDU hold multiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by “show lldp” command.

Example:

This example sets LLDP hold time multiplier to 3.

```
Switch(config)# lldp holdtime-multiplier 3
Switch# show lldp
```


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

```
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
```

3.13.5 lldp tx-delay

Command:

```
lldp tx-delay <1-8192>
```

Parameter:

<1-8192>	Specify the LLDP tx delay in unit of seconds.

Default:

lldp tx-delay 2

Mode:

Global Configuration

Usage Guide:

This command globally configures the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown by “show lldp” command.

Example:

This example sets LLDP PDU TX delay to 10.

```
Switch(config)# lldp tx-delay 10
Switch# show lldp
State: Disabled
Timer: 10 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 10 Seconds
LLDP packet handling: Flooding
```


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

3.13.6 lldp tlv-select

Command:

```
lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]
no lldp tlv-select
```

Parameter:

TLV	Specify the selected optional TLV. Available optional TLVs are : sys-name (system name), sys-desc (system description), sys-cap (system capability), mac-phy (802.3 MAC-PHY), lag (802.3 link aggregation), max-frame-size (802.3 max frame size), and management-addr (management address).

Mode:

Interface Configuration

Usage Guide:

This command per port configures the selected TLV attaching in PDU. The “no lldp tlv-select” command would remove all selected TLV. The configuration could be shown by “show lldp” command.

Example:

This example selects system name, system description, system capability, 802.3 MAC-PHY, 802.3 link aggregation, 802.3 max frame size, and management address TLVs for interface gi1 and gi3.

```
Switch(config)# interface range gi 1,3
Switch(config-if-range)# lldp tlv-select port-desc sys-name sys-desc sys-cap mac-
phy lag max-frame-size management-addr
Switch(config-if-range)# exit
Switch(config)# show lldp interfaces gi1,3
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
-------- + ------ + -------------- + --------
gi1 | RX,TX | PD, SN, SD, SC |192.168.1.254
gi3 | RX,TX | PD, SN, SD, SC |192.168.1.254
Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-addr
```


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

```
802.1 optional TLVs
PVID: Enabled
Port ID: gi3
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-addr
802.1 optional TLVs
PVID: Enabled
```

3.13.7 lldp tlv-select pvid

Command:

```
lldp tlv-select pvid (disable|enable)
```

Parameter:

(disable|enable) Specifies the LLDP 802.1 PVID TLV attach enable status.

Default:

lldp tlv-select pvid enable

Mode:

Interface Configuration

Usage Guide:

This command per port configures the 802.1 PVID TLV attach enable status. The configuration could be shown by "show lldp" command.

Example:

This example sets port gi1 PVID TLV attach status to disable and port gi2 to enable.

```
Switch(config)# interface gi1
Switch(config-if-range)# lldp tlv-select pvid disable
Switch(config-if-range)# exit
Switch(config)# interface gi2
Switch(config-if-range)# lldp tlv-select pvid enable
Switch(config-if-range)# exit
Switch(config)# show lldp interfaces gi1,gi2
State: Disabled
Timer: 10 Seconds
```


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

```
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
-------- + ------ + -------------- + --------
gi1 | RX,TX | |192.168.1.254
gi2 | RX,TX | |192.168.1.254
Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled
Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

3.13.8 lldp tlv-select vlan-name

Command:

```
lldp tlv-select vlan-name (add|remove) VLAN-LIST
```

Parameter:

(add|remove)	Specifies to add or remove VLAN list for LLDP 802.1 VLAN-NAME TLV.
VLAN-LIST	Specify VLAN list. The configured ports should be member of all the specified VLANs or the VLAN-LIST is not valid.

Mode:

Interface Configuration

Usage Guide:

The commands per port configure to add or remove VLAN list for 802.1 VLAN-NAME TLV. The configuration could be shown by “show lldp” command.

Example:

This example add VLAN 1, 100, 4000 to VLAN-NAME TLV for port gi10.

```
Switch(config)# vlan 100
```


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

```
Switch(config-vlan)# exit
Switch(config)# vlan 4000
Switch(config-vlan)# exit
Switch(config)# interface gi10
Switch(config-if-range)# switchport trunk allowed vlan add all
Switch(config-if-range)# lldp tlv-select pvid enable
Switch(config-if-range)# exit
Switch(config)# show lldp interfaces gi1,gi2
State: Disabled
Timer: 10 Seconds
Hold multiplier: 3
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
-------- + ------ + -------------- + --------
gi1 | RX,TX | |192.168.1.254
gi2 | RX,TX | |192.168.1.254
Port ID: gi1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled
Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```


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

3.13.9 lldp lldpdu

Command:

```
lldp lldpdu (filtering|flooding|bridging)
```

Parameter:

(filtering|flooding|bridging)	Specifies that when LLDP is globally disabled, received LLDP packets are filtered (dropped), flooded (forwarded to all interfaces) or bridged (flooded to VLAN member ports).

Default:

Lldp lldpdu flooding

Mode:

Global Configuration

Usage Guide:

This command globally configures the LLDP PDU handling behavior when LLDP is globally disabled. It should be noticed that if LLDP is globally enabled and per port LLDP RX status is configured to disabled, the received LLDP PDU would be dropped instead of taking the global disable behavior. The configuration could be shown by “show lldp” command.

Example:

This example sets LLDP disable action to bridging.

```
Switch(config)# lldp lldpdu bridging
Switch(config)# show lldp
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging
```


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

3.13.10 lldp tx/rx

Command:

```
lldp rx

no lldp rx

lldp tx

no lldp tx
```

Mode:

Interface Configuration

Usage Guide:

The command per port configures the LLDP PDU RX and TX ability. The configuration could be shown by “show lldp” command.

Example:

This example sets port gi1 to enable LLDP RX and TX, port gi2 to disable RX but enable TX, port gi3 to enable RX but disable TX, port gi4 to disable RX and TX.

```
Switch(config)# interface gi1
Switch(config-if)# lldp rx
Switch(config-if)# lldp tx
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# no lldp rx
Switch(config-if)# lldp tx
Switch(config-if)# exit
Switch(config)# interface gi3
Switch(config-if)# lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# exit
Switch(config)# interface gi4
Switch(config-if)# no lldp rx
Switch(config-if)# no lldp tx
Switch(config-if)# exit
Switch(config)# show lldp interfaces gi1-4
State: Enabled
```


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

```
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging
Port | State | Optional TLVs | Address
-------- + ------ + -------------- + --------
gi1 | RX,TX | |192.168.1.254
gi2 | TX | |192.168.1.254
gi3 | RX | |192.168.1.254
gi4 |Disable | |192.168.1.254
```

3.13.11 lldp med

Command:

```
lldp med

no lldp med
```

Mode:

Interface Configuration

Usage Guide:

The command per port configures the LLDP MED enable status. If LLDP MED is enabled, LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by “show lldp med” command.

Example:

This example sets port gi1-4 to enable LLDP MED, port gi5-8 to disable LLDP MED.

```
Switch(config)# interface range gi1-4
Switch(config-if)# lldp med
Switch(config-if)# exit
Switch(config)# interface range gi5-8
Switch(config-if)# no lldp med
Switch(config-if)# exit
Switch(config)# show lldp interfaces gi1-8 med
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
```


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

```
gi1 | Yes | Yes | No | No | No
gi2 | Yes | Yes | No | No | No
gi3 | Yes | Yes | No | No | No
gi4 | Yes | Yes | No | No | No
gi5 | No | Yes | No | No | No
gi6 | No | Yes | No | No | No
gi7 | No | Yes | No | No | No
gi8 | No | Yes | No | No | No
```

3.13.12 lldp med tlv-select

Command:

```
lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]

no lldp med tlv-select
```

Parameter:

MEDTLV	MED optional TLV. Available optional TLVs are : network-policy, location, poe-pse, inventory.

Default:

lldp med tlv-select network-policy

Mode:

Interface Configuration

Usage Guide:

The command per port configures the LLDP MED TLV selection. “no lldp med tlv-select” command would remove all selected MED TLV over the dedicated ports. It should be noticed that even no MED TLV is selected, MED capability TLV would be attached if LLDP MED is enable. The configuration could be shown by “show lldp med” command.

Example:

This example sets port gi1-2 to select LLDP MED network policy, location, POE-PSE, inventory TLVs, and it sets port gi3-4 to un-select all LLDP MED TLVs.

```
Switch(config)# interface range gi1-2
Switch(config-if)# lldp med tlv-select network-policy location poe-pse inventory
Switch(config-if)# exit
```


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

```
Switch(config)# interface range gi3-4
Switch(config-if-range)# no lldp med tlv-select
Switch(config-if-range)# exit
Switch(config)# show lldp interfaces gi1-4 med
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
gi1 | Yes | Yes | Yes | Yes | Yes
gi2 | Yes | Yes | Yes | Yes | Yes
gi3 | Yes | No | No | No | No
gi4 | Yes | No | No | No | No
```

3.13.13 lldp med fast-start-report-count

Command:

```
lldp med fast-start-repeat-count <1-10>
```

Parameter:

<1-10>	LLDP PDU fast start TX repeat counts.

Default:

lldp med fast-start-repeat-count 3

Mode:

Global Configuration

Usage Guide:

The command globally configures the LLDP PDU fast start TX repeat count. When port links up, it will send LLDP PDU immediately to notify link partner. The number of LLDP PDU sends when it links up depends on fast-start-repeat-count configuration. The LLDP PDU fast-start transmits in interval of one second. The fast start behavior works no matter LLDP MED is enabled or not. The configuration could be shown by “show lldp med” command.

Example:

This example sets fast start repeat count to 10.

```
Switch(config)# lldp med fast-start-repeat-count 10
Switch(config)# show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
```

3.13.14 lldp med network-policy

Command:

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

```
lldp med network-policy <1-32> app (voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice| video-conferencing|streaming-video|video-signaling) vlan <1-4094> vlan-type (tag|untag) priority <0-7> dscp <0-63>

no lldp med network-policy <1-32>
```

Parameter:

<1-32>	Specify the network policy index
(voice|voice-signaling|guest-voice|guest-voice-signaling|softphone-voice| video-conferencing|streaming-video|video-signaling)	Specify the network policy application type.
<1-4094>	Specify the VLAN ID
(tag|untag)	Specify the VLAN tag status
<0-7>	Specify the L2 priority
<0-63>	Specify the DSCP value

Mode:

Global Configuration

Usage Guide:

The commands globally configures the LLDP MED network policy table. The “lldp med network-policy” command created a network policy entry that can be bind to ports. If LLDP MED network policy voice auto mode is enabled, “voice” type network policy can not be created since it is in auto mode. The “no lldp med network-policy” command clear the network policy entry of the specified index. A network policy can be cleared only when it is not bind to any port. The network policy table configuration could be shown by “show lldp med” command.

Example:

This example create 2 network policies.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# lldp med network-policy 1 app voice-signaling vlan 2 vlan-type tag priority 3 dscp 4
Switch(config)# lldp med network-policy 32 app video-conferencing vlan 5 vlan-type tag priority 1 dscp 63
Switch(config)# show lldp med
```


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

```
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
Network policy 1
-------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4
Network policy 32
-------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63
```

3.13.15 lldp med network-policy add | remove

Command:

```
lldp med network-policy (add|remove) <1-32>
```

Parameter:

(add|remove)	Add or remove network policy binding for ports.
<1-32>	Specify the network policy index

Mode:

Interface Configuration

Usage Guide:

The command per port configures the network policy binding for port interface. The binded network policy of one port should be with different types. If network policy TLV is selected over a port, the binded network policies would be attached in LLDP MED PDU. The configuration of network policy binding could be shown by “show lldp med” command.

Example:

This example binds network policy for interface gi1 and gi2.

```
Switch(config)# show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
```


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

```
Network policy 1
-------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4
Network policy 32
-------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63
Switch(config)# interface range gi1,2
Switch(config-if-range)# lldp med network-policy add 1,32
Switch(config)# show lldp interfaces gi1,2 med
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
gi1 | Yes | Yes | Yes | Yes | Yes
gi2 | Yes | Yes | Yes | Yes | Yes
Port ID: gi1
Network policies: 1, 32
Port ID: gi2
Network policies: 1, 32
```

3.13.16 lldp med network-policy auto

Command:

```
lldp med network-policy auto

no lldp med network-policy auto
```

Mode:

Global Configuration

Usage Guide:

The command globally configures the network policy voice auto mode enable status. In voice auto mode, if network-policy TLV is selected, a voice type network policy would be attached to PDU that contents comes from voice VLAN configuration. This works for voice VLAN module to exchange voice VLAN information with link partner. If voice auto mode is enabled, user can not manually create an voice type network policy; if an voice type network policy is

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

created, the voice auto mode can not be enabled. The configuration of network policy auto mode could be shown by "show lldp med" command.

Example:

This example sets network policy auto mode to enable and then disable.

```
Switch(config)# lldp med network-policy auto
Switch(config)# show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: auto
Switch(config)# no lldp med network-policy auto
Switch(config)# show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: manual
```

3.13.17 lldp med location

Command:

```
lldp med location (coordination|civic-address|ecs-elin) ADDR

no lldp med location (coordination|civic-address|ecs-elin)
```

Parameter:

(coordination|civic-address|ecs-elin)	Location type to be configured. "ecs-elin" is abbreviation of emergency call service – emergency location identifier number
ADDR	Specify the location data. Input format is hexadecimal values without colon (for example: 1234AB). For coordination location type, the length of ADDR is 16 bytes. For civic-address, the length is 6 to 160 bytes. For ecs-elin, the length is 10 to 25 bytes.

Mode:

Interface Configuration

Usage Guide:

The command per port configures the LLDP MED location data. The "no lldp med location" command clear the location data. The "coordinate", "civic-address", "ecs-elin" locations are independent, so at most three location TLVs could be sent if their data are not empty. The configuration of location could be shown by "show lldp interface PORT med" command.

Example:

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

This example sets location data for interface gi1.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
Switch(config)# interface gi1
Switch(config-if)# lldp med location coordinate
112233445566778899AABBCCDDEEFF00
Switch(config-if)# lldp med location civic-address 112233445566
Switch(config-if)# lldp med location ecs-elin 112233445566778899AA
Switch(config)# show lldp interfaces gi1 med
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
gi1 | Yes | Yes | Yes | Yes | Yes
Port ID: gi1
Network policies: 1, 32
Location:
Coordinates: 112233445566778899AABBCCDDEEFF00
Civic-address: 112233445566
Ecs-elin: 112233445566778899AA
```

3.13.18 show lldp

Command:

```
show lldp

show lldp interface IF_NMLPORTS
```

Parameter:

IF_NMLPORTS	Specify the ports to display information

Mode:

Global Configuration

Privileged Configuraiton

Usage Guide:

The “show lldp” and “show lldp interface” command displays LLDP global information including LLDP enable status, LLDP PDU TX interval, hold time multiplier, re-initial delay, TX delay, and LLDP packet handling when LLDP is disabled. The per port information displayed includes port LLDP RX/TX enable status, selected TLV to TX and IP address. The abbreviations in optional TLVs are: port description (PD), system name (SN), system description (SD), and system capability (SC).

Example:

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

This example displays lldp information of port gi1 and gi2

```
Switch# show lldp interfaces gi1,gi2
State: Disabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Flooding
Port | State | Optional TLVs | Address
-------- + ------ + -------------- + --------
gi1 | RX,TX | PD, SN, SD, SC |192.168.1.254
gi1 | RX,TX | |192.168.1.254
Port ID: gi1
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size, management-addr
802.1 optional TLVs
PVID: Enabled
Port ID: gi2
802.3 optional TLVs:
802.1 optional TLVs
PVID: Enabled
```

3.13.19 show lldp local-device

Command:

```
show lldp local-device

show lldp interfaces IF_NMLPORTS local-device
```

Parameter:

IF_NMLPORTS	Specify the ports to display information

Mode:

Privileged Configuration

Global Configuration

Usage Guide:

The commands show the local configuration of LLDP PDU. By the commands, a user can view the contents of

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

LLDP/ LLDP-MED TLVs that would be attached in LLDP PDU.

Example:

This example displays the local device information.

```
Switch(config)# show lldp local-device
LLDP Local Device Information:
Chassis Type : Mac Address
Chassis ID : 00:12:12:12:12:12
System Name : Switch
System Description :
System Capabilities Support : Bridge
System Capabilities Enable : Bridge
Management Address : 192.168.1.254(IPv4)
Switch(config)# show lldp interfaces gi1 local-device
Device ID: 00:12:12:12:12:12
Port ID: gi1
System Name: Switch
Capabilities: Bridge
System description:
Port description:
Management address: 192.168.1.254
Time To Live: 120
802.3 MAC/PHY Configur/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 10BASE-T half duplex, 10BASE-T full duplex,
100BASE-TX half duplex, 100BASE-TX full duplex
Operational MAU type: Other or unknown
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 0
802.3 Maximum Frame Size: 1522
802.1 PVID: 1
LLDP-MED capabilities: Capabilities, Network Policy, Location, Extended PSE, Inventory
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice Signaling
Flags: Unknown Policy
```


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

```
VLAN ID: 2
Layer 2 priority: 3
DSCP: 4
LLDP-MED Network policy
Application type: Conferencing
Flags: Unknown Policy
VLAN ID: 5
Layer 2 priority: 1
DSCP: 63
Hardware revision: 1123
Firmware revision: 2.5.0-beta.32801
Software revision: 2.5.0-beta.32801
Serial number: abc
Manufacturer Name:
Model name: Switch
Asset ID:
LLDP-MED Location
Coordinates: 11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00
Civic-address: 11:22:33:44:55:66
Ecs-elin: 11:22:33:44:55:66:77:88:99:AA
```

3.13.20 show lldp neighbor

Command:

```
show lldp neighbor

show lldp interfaces IF_NMLPORTS neighbor
```

Parameter:

IF_NMLPORTS	Specify the ports to display information

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

When LLDP PDU is received on LLDP RX enable ports, system would store the PDU information in database until time to live of the PDU counts down to zero. The commands display the received neighbor LLDP PDU information.

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

Example:

This example displays the neighbor information.

```
Switch(config)# show lldp neighbor
Port | Device ID | Port ID | SysName | Capabilities | TTL
---- + ---------------- + ---------------- + ---------------- + -------------- + -----
gi3 | 00:12:12:12:12:12 | gi1 | Switch | Bridge | 111
gi11 | TREEBASE |00:1A:4D:26:EB:E8 | TREEBASE | Station Only | 33
Switch(config)# show lldp interfaces gi3 neighbor
Device ID: 00:12:12:12:12:12
Port ID: gi1
System Name: Switch
Capabilities: Bridge
System description:
Port description:
Management address: 192.168.1.254
Time To Live: 98
802.3 MAC/PHY Configur/Status
Auto-negotiation support: Supported
Auto-negotiation status: Enabled
Auto-negotiation Advertised Capabilities: 10BASE-T half duplex, 10BASE-T full duplex,
100BASE-TX half duplex, 100BASE-TX full duplex
Operational MAU type: 100BASE-TX full duplex mode
802.3 Link Aggregation
Aggregation capability: Capable of being aggregated
Aggregation status: Not currently in aggregation
Aggregation port ID: 0
802.3 Maximum Frame Size: 1522
802.1 PVID: 1
LLDP-MED capabilities: Capabilities, Network Policy, Location, Extended PSE, Inventory
LLDP-MED Device type: Network Connectivity
LLDP-MED Network policy
Application type: Voice Signaling
Flags: Unknown Policy
VLAN ID: 2
Layer 2 priority: 3
DSCP: 4
LLDP-MED Network policy
Application type: Conferencing
```


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

```
Flags: Unknown Policy
VLAN ID: 5
Layer 2 priority: 1
DSCP: 63
LLDP-MED Power over Ethernet
Device Type: Power Sourcing Entity
Power Source: Primary Power Source
Power priority: Low
Power value: 13.0 Watts
Hardware revision: 1123
Firmware revision: 2.5.0-beta.32801
Software revision: 2.5.0-beta.32801
Serial number: abc
Manufacturer Name:
Model name: Switch
Asset ID:
LLDP-MED Location
Coordinates: 11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF:00
Civic-address: 11:22:33:44:55:66
Ecs-elin: 11:22:33:44:55:66:77:88:99:AA
```

3.13.21 show lldp med

Command:

```
show lldp med

show lldp interfaces IF_NMLPORTS med
```

Parameter:

IF_NMLPORTS	Specify the ports to display information

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

The commands display the LLDP MED configuration information.

Example:

This example display the LLDP MED information.

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

```
Switch(config)# show lldp med
Fast Start Repeat Count: 10
lldp med network-policy voice: manual
Network policy 1
-------------------
Application type: Voice Signaling
VLAN ID: 2 tagged
Layer 2 priority: 3
DSCP: 4
Network policy 32
-------------------
Application type: Conferencing
VLAN ID: 5 tagged
Layer 2 priority: 1
DSCP: 63
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
gi1 | Yes | Yes | Yes | Yes | Yes
gi2 | Yes | Yes | Yes | Yes | Yes
gi3 | Yes | No | No | No | No
gi4 | Yes | No | No | No | No
gi5 | No | Yes | No | No | No
gi6 | No | Yes | No | No | No
gi7 | No | Yes | No | No | No
gi8 | No | Yes | No | No | No
gi9 | Yes | Yes | No | No | No
gi10 | Yes | Yes | No | No | No
gi11 | Yes | Yes | No | No | No
gi12 | Yes | Yes | No | No | No
gi13 | Yes | Yes | No | No | No
gi14 | Yes | Yes | No | No | No
gi15 | Yes | Yes | No | No | No
gi16 | Yes | Yes | No | No | No
gi17 | Yes | Yes | No | No | No
gi18 | Yes | Yes | No | No | No
gi19 | Yes | Yes | No | No | No
gi20 | Yes | Yes | No | No | No
gi21 | Yes | Yes | No | No | No
gi22 | Yes | Yes | No | No | No
```


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

```
gi23 | Yes | Yes | No | No | No
gi24 | Yes | Yes | No | No | No
gi25 | Yes | Yes | No | No | No
gi26 | Yes | Yes | No | No | No
gi27 | Yes | Yes | No | No | No
gi28 | Yes | Yes | No | No | No
Switch(config)# show lldp interfaces gi1 med
Port | Capabilities | Network Policy | Location | Inventory | POE
------ + ------------- + -------------- + -------- + ----------+ -----
gi1 | Yes | Yes | Yes | Yes | Yes
Port ID: gi1
Network policies: 1, 32
Location:
Coordinates: 112233445566778899AABBCCDDEEFF00
Civic-address: 112233445566
Ecs-elin: 112233445566778899AA
Switch(config)#
```

3.13.22 show lldp statistics

Command:

```
show lldp statistics

show lldp interfaces IF_NMLPORTS statistics
```

Parameter:

IF_NMLPORTS	Specify the ports to display information

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

The commands display the LLDP RX/TX statistics.

Example:

This example display the LLDP statistics.

```
Switch(config)# show lldp statistics
```


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

```
LLDP Global Statistics:
Insertions : 3
Deletions : 0
Drops : 0
Age Outs : 1
| TX Frames | RX Frames | RX TLVs | RX Ageouts
Port | Total | Total | Discarded | Errors | Discarded | Unrecognized | Total
--------+-----------+-------+-----------+--------+-----------+--------------+----------
gi1 | 50 | 0 | 0 | 0 | 0 | 0 | 0
gi2 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi3 | 0 | 50 | 0 | 0 | 0 | 0 | 1
gi4 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi5 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi6 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi7 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi8 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi9 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi10 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi11 | 3377 | 10129 | 0 | 0 | 0 | 0 | 0
gi12 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi13 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi14 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi15 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi16 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi17 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi18 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi19 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi20 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi21 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi22 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi23 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi24 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi25 | 3377 | 0 | 0 | 0 | 0 | 0 | 0
gi26 | 3377 | 0 | 0 | 0 | 0 | 0 | 0
gi27 | 0 | 0 | 0 | 0 | 0 | 0 | 0
gi28 | 0 | 0 | 0 | 0 | 0 | 0 | 0
Switch(config)# show lldp interfaces gi1 statistics
LLDP Port Statistics:
| TX Frames | RX Frames | RX TLVs | RX Ageouts
```


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

```
Port | Total | Total | Discarded | Errors | Discarded | Unrecognized | Total
--------+-----------+-------+-----------+--------+-----------+--------------+----------
gi1 | 51 | 0 | 0 | 0 | 0 | 0 | 0
```

3.13.23 show lldp tlv-overloading

Command:

```
show lldp interfaces IF_NMLPORTS tlvs-overloading
```

Parameter:

IF_NMLPORTS Specify the ports to display information

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

The LLDP PDU is composed by TLVs and selected number TLVs may compose a large PDU that the system can not handle. The maximum PDU length is to take the smaller number of jumbo frame size minus 30 bytes (30 bytes kept for header) or 1488 bytes. The commands display the length of LLDP TLVs and if the TLVs overload the PDU length. The TLVs with status marked “overload” would not be transmitted.

Example:

This example display the LLDP TLVs overloading status of port gi1.

```
Switch(config)# show lldp interfaces gi1 tlvs-overloading
gi1:
TLVs Group | Bytes | Status
---------------------------- + ------- + ----------------
Mandatory | 21 | Transmitted
LLDP-MED Capabilities | 9 | Transmitted
LLDP-MED Location | 53 | Transmitted
LLDP-MED Network Policies | 20 | Transmitted
LLDP-MED POE | 9 | Transmitted
802.3 | 30 | Transmitted
Optional | 38 | Transmitted
LLDP-MED Inventory | 97 | Transmitted
```


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

802.1 | 8 | Transmitted

Total: 285 bytes

Left: 1203 bytes

SEC.RU | Короткий путь к информации

Скачано с sec.ru

3.14 Logging

3.14.1 logging

Command:

```
logging

no logging
```

Mode:

Global Configuration

Usage Guide:

Enable/Disable the logging service.

logging

Enable the logging service. It is the global option of logging service. The status of the logging service is available from the command “show logging”.

no logging

Disable the logging service. When the logging service is disabled, all messages will stop logging to the system.

show logging

Display the global logging status. It will show the logging configuration of the system, including the global logging status, and the lists of logging services.

Example:

```
Switch(config)# show logging
Switch(config)# no logging
Switch(config)# show logging
Logging service is disabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+---------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
Switch(config)# logging
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+---------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
```


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

3.14.2 logging flash | buffered

Command:

```
logging (flash|buffered) [severity <0-7>]

no logging (flash|buffered)
```

Parameter:

flash	Specify logging to flash.
buffer	Specify logging to RAM.
severity	Specify the minimum severity mask of logging message.

Default:

Severity = 6 (emerg, alert, crit, error, warning, notice, info)

Mode:

Global Configuration

Usage Guide:

Enable/Disable the local capability to log message to RAM/flash with the minimum severity. The minimum severity value is “6”, including messages of severity emergency, alert, critical, error, warning, notice, and info.

logging flash

Enable the capability to log message to flash, and the default minimum severity is 6. When the service is enables, messages will start to be logged to the flash. All logging messages will be saved when the system shutdown. Only when the local logging capability of flash is enabled, the status of logging flash service will be shown by the command “show logging”.

logging buffered

Enable the capability to log message to RAM, and the default minimum severity is 6. When the service is enabled, the messages will start to be logged to RAM. All logging message will be lost when the system shutdown.

no logging flash

Disable the capability to log message to flash. Once the logging capability of flash is disabled, the status of logging flash service will be removed from the service list shown by the command “show logging”.

no logging buffered

Disable the capability to log message to RAM.

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

show logging

Display the logging status. It will show the logging configuration of the system, including the global logging status, and the lists of logging services. When the local logging capability is enabled, the status of the local logging (flash or buffered) will be shown by the command “show logging”; Otherwise, the logging entry will be removed from the service list.

Example:

```
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+---------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
Switch(config)# no logging buffer
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+---------------------------------
Switch(config)# logging buffered
Switch(config)# logging flash severity 5
Switc(config)h# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+---------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
flash | enabled | | |emerg, alert, crit, error, warning, notice
```

3.14.3 logging host

Command:

```
logging host <ip-addr> [port <0-65535>] [severity <0-7>] [facility
(local0|local1|local2|local3|local4|local5|local6|local7)]

no logging <ip-addr>
```

Parameter:

ip-addr	Specify the IP address of remote logging server.
port	Specify the port number of remote logging server.

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

severity	Specify the minimum severity mask of logging message.
facility	Specify the facility of logging messages.

Default:

Port = 514,

Severity = 6 (emerg, alert, crit, error, warning, notice, info)

Facility = Local7

Mode:

Global Configuration

Usage Guide:

Enable/Disable the capability to log message to the remote syslog server.

logging host 192.168.1.100

Enable the capability to log messages to the remote server. The default values of the parameter port is “514”, severity is “6” (emerg, alert, crit, error, warning, notice, info), and the facility is “local7”. All logging message will be sent to the remote server. Only when the remote logging capability is enabled, the status of remote logging service will be shown by the command “show logging”. When an existed entry is set twice, the old setting will be replaced and modified with the new one.

no logging host 192.168.1.100

Disable the capability to log messages to the remote server. When the remote logging service is disabled, the log will not be sent to the remote syslog server, and the status of remote logging entry will be removed from service list shown by the command “show command”.

show logging

Display the logging status. It will show the logging configuration of the system, including the global logging status, and the lists of logging services. When the remote logging capability is enabled, the status of remote logging will be shown by the command “show logging”; Otherwise, the remote logging entry will be removed from the service list.

Example:

```
Switch(config)# logging host 192.168.1.100
Switch(config)# logging host 192.168.1.100 port 2048 severity 3 facility local1
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+-------------------------------+----------+---------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
flash | enabled | | |emerg, alert, crit, error, warning, notice
host | enabled | 192.168.1.100( 2048)| local1 |emerg, alert, crit, error
```


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

```
Switch(config)# no logging host 192.168.1.100
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+----------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
flash | enabled | | |emerg, alert, crit, error, warning, notice
```

3.14.4 show logging

Command:

```
show logging
```

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

show logging

Show the logging configuration. The information includes the global logging service status, and the list of logging service.

Status of global logging service can be determined by the command “logging/no logging”. The list of logging service shows all the active logging service.

Example:

```
Switch(config)# show logging
Logging service is enabled
TARGET | STATUS | Server (PORT) | FACILITY | LOG LEVEL
----------+----------+--------------------------------+----------+----------------------------------
buffered | enabled | | |emerg, alert, crit, error, warning, notice, info
```


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

3.14.5 show logging flash | buffered

Command:

```
show logging (flash|buffered)
```

Parameter:

flash	Specify showing the messages logged to flash.
buffered	Specify showing the messages logged to RAM.

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

Show the messages logged to flash/RAM.

show logging flash

Show the messages logged to the flash. When the capability of the service is enabled, it will show all message logged to the flash. All messages will be logged in inverse chronological order.

show logging buffered

Show the messages logged to the RAM. When the capability of the service is enabled, it will show all message logged to the RAM. Logs will be lost after system shutdown. All messages will be logged in inverse chronological order.

Example:

```
Switch(config)# show logging buffered
Log messages in buffered
NO.| Timestamp | Category | Severity | Message
---------------------+----------------+----------+---------------------------------------
1| Jan 01 08:00:57| STP| info| Port 1 STP port state is set to Forwarding
2| Jan 01 08:00:42| STP| info| Port 1 STP port state is set to Learning
3| Jan 01 08:00:30| AAA| info| User '' enter privileged mode from telnet with level '15'
success
4| Jan 01 08:00:28| AAA| info| User '' is authorized with privilege level 1
5| Jan 01 08:00:28| AAA| info| User '' login from telnet success
6| Jan 01 08:00:24| System| info| Sysinfo variable 'resetdefault' is set to value '0'
7| Jan 01 08:00:23| System| notice| System Startup!
```


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

3.14.6 clear logging flash | buffered

Command:

```
clear logging (flash|buffered)
```

Parameter:

flash	Specify showing the messages logged to flash.
buffered	Specify showing the messages logged to RAM.

Mode:

Global Configuration

Privileged Configuration

Usage Guide:

Clear the message logged to flash/RAM.

clear logging flash

Clear the messages logged to flash.

clear logging buffered

Clear the messages logged to RAM.

Example:

```
Switch# show logging buffered
Log messages in buffered
NO.| Timestamp | Category | Severity | Message
---------------------+----------------+----------+---------------------------------------
1| Jan 01 08:00:57| STP| info| Port 1 STP port state is set to Forwarding
2| Jan 01 08:00:42| STP| info| Port 1 STP port state is set to Learning
3| Jan 01 08:00:30| AAA| info| User '' enter privileged mode from telnet with level '15'
success
4| Jan 01 08:00:28| AAA| info| User '' is authorized with privilege level 1
5| Jan 01 08:00:28| AAA| info| User '' login from telnet success
6| Jan 01 08:00:24| System| info| Sysinfo variable 'resetdefault' is set to value '0'
7| Jan 01 08:00:23| System| notice| System Startup!
Switch# clear logging buffered
Switch# show logging buffered
Log messages in buffered
NO.| Timestamp | Category | Severity | Message
---------------------+----------------+----------+---------------------------------------
```


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

3.15 MAC Address Table

3.15.1 clear mac address-table

Command:

```
clear mac address-table dynamic [interfaces IF_PORTS] [vlan <1-4094>]
```

Parameter:

IF_PORTS	Delete all dynamic addresses on the specified interface.
<1-4094>	Delete all dynamic addresses on the specified VLAN

Mode:

Privileged Configuration

Usage Guide:

Use the **clear mac address-table Privileged EXEC** command to delete dynamic mac entry on specified interface or VLAN or all dynamic mac entry in mac address table

You can verify your setting by entering the **show mac address-table dynamic Privileged EXEC** command

Example:

This example shows how to delete dynamic MAC address entries on gi1

```
Switch# show mac address-table dynamic
VID | MAC Address | Type | Ports
-------+---------------------------+------------------------+----------
1 | 00:30:4F:00:00:12 | Dynamic | gi11
1 | 00:30:4F:3B:1E:E6 | Dynamic | gi1
Total number of entries: 2
Switch(config)# clear mac address-table dynamic interfaces gi1
Switch# show mac address-table dynamic
VID | MAC Address | Type | Ports
-------+---------------------------+------------------------+----------
1 | 00:30:4F:00:00:12 | Dynamic | gi11
Total number of entries: 1
```

3.15.2 mac address-table aging-time

Command:

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

```
mac address-table aging-time <10-630>
```

Parameter:

<10-630>	Specify aging time value of second.

Default:

In default aging out time is 300s.

Mode:

Global Configuration

Usage Guide:

Use the mac address-table aging-time Global configuration command to set the aging time of the address table

You can verify your setting by entering the **show mac address-table aging-time Privileged EXEC** command

Example:

The following example show how to configure dynamic mac entry aging out time

```
Switch(config)# mac address-table aging-time 100
Switch# show mac address-table aging-time
Mac Address Table aging time: 100 sec
```

3.15.3 mac address-table static

Command:

```
mac address-table static A:B:C:D:E:F vlan <1-4094> interfaces IF_PORTS

no mac address-table static A:B:C:D:E:F vlan <1-4094>
```

Parameter:

A:B:C:D:E:F	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
<1-4094>	Specify the VLAN for which the packet with the specified MAC address is received.
IF_PORTS	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Mode:

Global Configuration

Usage Guide:

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table.

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

Use the **no** form of this command to remove static entries from the table.

You can verify your setting by entering the **show mac address-table static** Privileged EXEC command

Example:

This example shows how to add static addresses to the MAC address table.

```
Switch(config)# mac address-table static 0:1:2:3:4:5 vlan 1 interfaces gi5
Switch(config)# mac address-table static 1:6:7:9:a:b vlan 100 interfaces gi1,gi5,gi10
Switch# show mac address-table static
VID | MAC Address | Type | Ports -----+-----------------------+---------------- ---------+------------
---- 1 | 00:30:4F:03:04:05 | Static | gi5
100 | 00:30:4F:09:0A:0B | Static | gi1,gi5,gi10
Total number of entries: 2
```

3.15.4 mac address-table static drop

Command:

```
mac address-table static A:B:C:D:E:F vlan <1-4094> drop
```

Parameter:

A:B:C:D:E:F	Unicast source or destination MAC address. Packets with this MAC address are dropped.
<1-4094>	Specify the VLAN for which the packet with the specified MAC address is received.

Default:

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

Mode:

Global Configuration

Usage Guide:

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address.

Use the **no** form of this command to return to the default setting.

You can verify your setting by entering the **show mac address-table static** Privileged EXEC command

Example:

This example shows how to add filter mac addresses to the MAC address table.

```
Switch(config)# mac address-table static a:b:c:d:e:f vlan 20 drop
```


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

```
Switch# show mac address-table static
VID | MAC Address | Type | Ports -----+-------------------------+-----------`------ ---------+-----------
----- 1 | 00:30:4F:03:04:05 | Static | gi5
100 | 00:30:4F:09:0A:0B | Static | gi1,gi5,gi10 20 | 00:30:4F:0D:0E:0F | Filtering | All
Total number of entries: 3
```

3.15.5 show mac address-table

Command:

```
show mac address-table [(static|dynamic)] [interfaces IF_PORTS] [vlan <1-4094>]

show mac address-table A:B:C:D:E:F [vlan <1-4094>]
```

Parameter:

static	Add/Edit login authentication list
dynamic	Displays only static MAC address table entries.
IF_PORTS	Displays entries for a specific interface ID. The interface ID can be one of the following types: Ethernet port or port-channel.
<1-4094>	Displays entries for a specific VLAN.
A:B:C:D:E:F	Displays entries for a specific MAC address.

Mode:

Privileged EXEC

Usage Guide:

Use the show mac address-table command in EXEC mode to view entries in the MAC address table.

Example:

This example shows all MAC address entries in mac address table.

```
Switch# show mac address-table
VID | MAC Address | Type | Ports
------+-------------------------+-------------------------+----------------
1 | DE:AD:BE:EF:01:02 | Management | CPU 1 | 00:00:E3:00:00:12 | Dynamic | gi11
1 | 00:01:02:03:04:05 | Static | gi5
1 | 00:14:78:3B:1E:E6 | Dynamic | gi1
100 | 01:06:07:09:0A:0B | Static | gi1,gi5,gi10 20 | 0A:0B:0C:0D:0E:0F | Static | All
Total number of entries: 6
```


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

```
The following example displays address table entries containing the specified MAC address.
Switch# show mac address-table 0:1:2:3:4:5
VID | MAC Address | Type | Ports
------+-------------------+------------+----------------
1 | 00:01:02:03:04:05 | Static | gi5
Total number of entries: 1
```

3.15.6 show mac address-table counters

Command:

```
show mac address-table counters
```

Mode:

Privileged EXEC

Usage Guide:

Use the **show mac address-table counters** command in EXEC mode to display the number of addresses present in mac address-table

Example:

This example shows how to display total mac entry counters

```
Switch# show mac address-table counters
Total number of entries: 5
```

3.15.7 show mac address-table aging-time

Command:

```
show mac address-table aging-time
```

Mode:

Privileged EXEC

Usage Guide:

Use the **show mac address-table aging-time** command in EXEC mode to display the aging time for dynamic mac entries.

Example:

This example shows how to display aging time of dynamic mac address entry

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

```
Switch# show mac address-table aging-time
Mac Address Table aging time: 300 sec
```

3.16 Mirror

3.16.1 mirror session

Command:

```
mirror session <1-4> source interfaces IF_PORTS (both | rx | tx)

no mirror session <1-4> source interfaces IF_PORTS (both|rx|tx)

mirror session <1-4> source vlan <1-4094>

no mirror session <1-4> source vlan

mirror session <1-4> destination interface IF_NMLPORT [allow-ingress]

no mirror session <1-4> destination interface IF_NMLPORT

no mirror session (<1-4> | all)
```

Parameter:

<1-4>	Specify the mirror session to configure
IF_PORTS	Specify the source interface, Valid interfaces include physical ports and port channels.
both,rx,tx	Specify the traffic direction to mirror.
<1-4094>	Specify the mirrored VLAN ID
IF_NMLPORT	Specify the SPAN destination. A destination must be a physical port
allow-ingress	Enable ingress traffic forwarding.

Mode:

Global Configuration

Usage Guide:

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) source or destination session

Use the **no** form of this command to remove the SPAN session or to remove source or destination interfaces or filters from the SPAN session

You can verify your setting by entering the **show mirror** Privileged EXEC command

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

Example:

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port gi1.

```
Switch(config)# mirror session 1 source interface gi2-5 both
Switch(config)# mirror session 1 destination interface gi1
Switch(config)# show mirror session 1
Session 1 Configuration
Source RX Port : gi2-5
Source TX Port : gi2-5
Destination port : gi1
Ingress State: disabled
Switch(config)# mirror session 2 source vlan 100
Switch(config)# mirror session 2 destination interface gi1 allow-ingress
Switch(config)# show mirror session 2
Session 2 Configuration
Mirrored VLAN: 100
Destination port : gi1
Ingress State: enable
```

3.16.2 show mirror

Command:

```
show mirror [session <1-4>]
```

Parameter:

<1-4>	Specify the mirror session to display

Mode:

Privileged EXEC

Usage Guide:

Use the **show mirror** command in EXEC mode to display mirror session configuration

Example:

This example shows how to display mirror session configuration

```
Switch(config)# show mirror
```


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

```
Session 1 Configuration
Source RX Port : gi2-5
Source TX Port : gi2-5
Destination port : gi1
Ingress State: disabled
Session 2 Configuration
Mirrored source : Not Config
Destination port : Not Config
Session 3 Configuration
Mirrored source : Not Config
Destination port : Not Config
Session 4 Configuration
Mirrored source : Not Config
Destination port : Not Config
```


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

3.17 MLD Snooping

3.17.1 ipv6 mld snooping

Command:

```
ipv6 mld snooping

no ipv6 mld snooping

show ipv6 mld snooping
```

Default:

Disabled

Mode:

Global Configuration

Usage Guide:

'**no ipv6 mld snooping**' will clear all ipv6 mld snooping dynamic group and dynamic router port, and make the static ipv6 mld group invalid. Then do not learning the dynamic group and router port by mld message.

The configure can use '**show ipv6 mld snooping**'

Example:

This example shows how to specify that set ipv6 mld snooping test.

```
Switch(config)# ipv6 mld snooping
Switch# show ipv6 mld snooping
MLD Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Enabled
Operation Version : v1
Forward Method : mac
Unknown Multicast Action : Flood
Switch(config)# no ipv6 mld snooping
Switch# show ipv6 mld snooping
MLD Snooping Status
--------------------
Snooping : Disabled
Report Suppression : Enabled
Operation Version : v1
Forward Method : mac
Unknown Multicast Action : Flood
```


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

3.17.2 ipv6 mld snooping report-suppression

Command:

```
ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression
```

Default:

Enabled

Mode:

Global Configuration

Usage Guide:

'**no ipv6 mld snooping report-suppression**' will disable mld v1 report suppression function. So when receive report will forward to the vlan router ports. The configure can use '**show ipv6 mld snooping**'.

Example:

This example shows how to specify that disable ipv6 mld snooping report-suppression test.

```
Switch(config)# no ipv6 mld snooping report-suppression
Switch# show ipv6 mld snooping
MLD Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Disabled
Operation Version : v1
Forward Method : mac
Unknown Multicast Action : Flood
```

3.17.3 ipv6 mld snooping version

Command:

```
ipv6 mld snooping version (1|2)
```

Parameter:

(1|2)	Ipv6 mld snooping running version 1 or 2

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

Default:

Version 1

Mode:

Global Configuration

Usage Guide:

When ipv6 mld snooping version is 1 ,the version 2 packet is not process.The configure can use '**show ipv6 mld snooping**'.

Example:

This example shows how to set ipv6 mld snooping version 2.

```
Switch(config)# ipv6 mld snooping version 2
Switch# show ipv6 mld snooping
MLD Snooping Status
--------------------
Snooping : Enabled
Report Suppression : Disabled
Operation Version : v2
Forward Method : mac
Unknown Multicast Action : Flood
```

3.17.4 ipv6 mld snooping vlan

Command:

```
ipv6 mld snooping vlan VLAN-LIST

no ipv6 mld snooping vlan VLAN-LIST
show ipv6 mld snooping vlan [VLAN-LIST]
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set

Default:

Disabled

Mode:

Global Configuration

Usage Guide:

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

'**no ipv6 mld snooping vlan 1**' will clear vlan all ipv6 mld snooping dynamic group and dynamic router port, and make the static ipv6 mld group invalid witch vlan ID is vlan 1. Then do not learning the dynamic group and router port by mld message for vlan 1.

The configure can use 'show ipv6 mld snooping vlan 1'.

Example:

This example shows how to set ipv6 mld snooping vlan.

```
Switch(config)# ipv6 mld snooping
Switch(config)# ipv6 mld snooping vlan 1
Switch# show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : enabled
MLD Snooping oper mode : enabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper 10 sec
MLD Snooping last member query counter: admin 2 oper 2
MLD Snooping last member query interval: admin 1 sec oper 1 sec
MLD Snooping last immediate leave: disabled
MLD Snooping automatic learning of multicast router ports: enabled
Switch(config)# no ipv6 mld snooping vlan 1
Switch# show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper 10 sec
MLD Snooping last member query counter: admin 2 oper 2
MLD Snooping last member query interval: admin 1 sec oper 1 sec
MLD Snooping last immediate leave: disabled
MLD Snooping automatic learning of multicast router ports: enabled
```


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

3.17.5 ipv6 mld snooping vlan parameters

Command:

```
ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count <1-7>

no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-count

ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval <1-60>

no ipv6 mld snooping vlan <VLAN-LIST> last-member-query-interval

[no] ipv6 mld snooping vlan <VLAN-LIST> router learn pim-dvmrp

[no] ipv6 mld snooping vlan <VLAN-LIST> fastleave

ipv6 mld snooping vlan <VLAN-LIST> query-interval <30-18000>

no ipv6 mld snooping vlan <VLAN-LIST> query-interval

ipv6 mld snooping vlan <VLAN-LIST> response-time <5-20>

no ipv6 mld snooping vlan <VLAN-LIST> response-time

ipv6 mld snooping vlan <VLAN-LIST> robustness-variable <1-7>

no ipv6 mld snooping vlan <VLAN-LIST> robustness-variable
```

Parameter:

login	Add/Edit login authentication list
VLAN-LIST	Specify VLAN ID list to set
last-member-query-count <1-7>	Specify last member query count to set. Default is 2
last-member-query-interval <1-60>	Specify last member query interval to set. Default is 1
query-interval <30-18000>	Specify query interval to set. Default is 125
response-time <5-20>	Specify a response time to set. default is 10
robustness-variable <1-7>	Specify a robustness value to set, default is 2

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

Mode:

Global Configuration

Usage Guide:

'**no ipv6 mld snooping vlan 1 (last-member-query-count | last-member-query-interval | query-interval | response-time | robustness-variable)**' will set the vlan parameters to default.

The cli setting will change the ipv6 mld vlan parameters admin settings.

The configure can use '**show ipv6 mld snooping vlan 1**'.

Example:

This example shows how to set ipv6 mld snooping vlan parameters.

```
Switch(config)# ipv6 mld snooping vlan 1 fastleave
Switch(config)# ipv6 mld snooping vlan 1 last-member-query-count 5
Switch(config)# ipv6 mld snooping vlan 1 last-member-query-interval 3
Switch(config)# ipv6 mld snooping vlan 1 query-interval 100
Switch(config)# ipv6 mld snooping vlan 1 response-time 12
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 4
Switch# show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 4 oper 2
MLD Snooping query interval: admin 100 sec oper 125 sec
MLD Snooping query max response : admin 12 sec oper 10 sec
MLD Snooping last member query counter: admin 5 oper 2
MLD Snooping last member query interval: admin 3 sec oper 1 sec
MLD Snooping last immediate leave: enabled
MLD Snooping automatic learning of multicast router ports: enabled
```

3.17.6 ipv6 mld snooping vlan static-port

Command:

```
[no] ipv6 mld snooping vlan <VLAN-LIST> static-port IF_PORTS

[no] ipv6 mld snooping vlan <VLAN-LIST> forbidden-port IF_PORTS
```

Parameter:

VLAN-LIST	Specify VLAN ID list to set
IF_PORTS	Specify a port list to set or remove

Default:

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

None static/forbidden ports

Mode:

Global Configuration

Usage Guide:

'**ipv6 mld snooping vlan 1 static-port gi1-2**' will add static port gi1-2 for vlan 1. The all known vlan 1 ipv6 group will add the static ports.

'**ipv6 mld snooping vlan 1 forbidden-port gi3-4**' will add forbidden port gi3-4 for vlan 1. The all known vlan 1 ipv6 group will remove the forbidden ports.

The configuration can use '**show ipv6 mld snooping forward-all**'.

Example:

This example shows how to set ipv6 mld snooping static/forbidden port

```
Switch(config)# ipv6 mld snooping vlan 1 static -port gi1-2
Switch(config)# ipv6 mld snooping vlan 1 forbidden -port gi3-4
Switch# show ipv6 mld snooping forward-all vlan 1
MLD Snooping VLAN : 1
MLD Snooping static port : gi1-2
MLD Snooping forbidden port : gi3-4
```

3.17.7 ipv6 mld snooping vlan static-router-port

Command:

```
[no] ipv6 mld snooping vlan <VLAN-LIST> static-router-port IF_PORTS

[no] ipv6 mld snooping vlan <VLAN-LIST> forbidden-router-port IF_PORTS
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
IF_PORTS	specifies a port list to set or remove

Default:

None static/forbidden router ports

Mode:

Global Configuration

Usage Guide:

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

'**ipv6 mld snooping vlan 1 static-router-port gi1-2**' will add static router port gi1-2 for vlan 1.

'**ipv6 mld snooping vlan 1 forbidden-router-port gi2**' will add forbidden router port gi2 for vlan 1.

This will also remove gi2 from static router port. The forbidden router port received query will not forward.

The configure can use show ipv6 mld snooping router.

Example:

This example shows how to set ipv6 mld snooping static/forbidden.

```
Switch(config)# ipv6 mld snooping vlan 1 static-router-port gi1-2
Switch(config)# ipv6 mld snooping vlan 1 forbidden-router-port gi2
Switch# show ipv6 mld snooping router
Dynamic Router Table
VID | Port | Expiry Time(Sec)
------+---------+------------------
Total Entry 0
Static Router Table VID | Port Mask
------+------------------------
1 | gi1
Total Entry 1
Forbidden Router Table
VID | Port Mask
------+------------------------
1 | gi2
Total Entry 1
```

3.17.8 ipv6 mld snooping vlan static-group

Command:

```
[no] ipv6 mld snooping vlan <VLAN-LIST> static-group <ip-addr> interfaces
IF_PORTS

[no] ipv6 mld snooping vlan <VLAN-LIST> group <ip-addr>
```

Parameter:

VLAN-LIST	specifies VLAN ID list to set
ip-addr	specifies multicast group ipv4 address
IF_PORTS	specifies port list to set or remove

Mode:

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

Usage Guide:

'**ipv6 mld snooping vlan 1 static-group ff12::1 interfaces gi1**' will add static group.

The static group will not learning others dynamic port. If the dynamic group exist, then the static group will overlap the dynamic group. If remove the last member of static group, the static group will be delete.

The static group want to valid , must mld snooping vlan enable and ipv6 mld snooping enable.

The configure can use '**show ipv6 mld snooping groups [(dynamic | static)]**' to display. And can use '**no ipv6 mld snooping vlan 1 group ff12::1**' to delete the static group. Also can use '**clear ipv6 mld snooping groups**' to delete the static group.

Example:

This example shows how to set ipv6 mld snooping static group.

```
Switch(config)# ipv6 mld snooping vlan 1 static-group ff12::1 interfaces gi1-2
Switch# show ipv6 mld snooping groups
VLAN | Gourp IP Address | Type | Life(Sec) | Port
------+----------------------------------------+--------+-----------+-----------------
1 | ff12::1 | Static| -- | gi1-2
Total Number of Entry = 1
Switch# clear ipv6 mld snooping groups static
Switch# show ipv6 mld snooping groups
VLAN | Gourp IP Address | Type | Life(Sec) | Port
------+----------------------------------------+--------+-----------+-----------------
Total Number of Entry = 0
```

3.17.9 ipv6 mld profile

Command:

```
ipv6 mld profile <1-128>
profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)
show ipv6 mld profile [<1-128>]
```

Parameter:

<1-128>	specifies profile ID
<ipv6-addr>	Start ipv6 multicast address
[ipv6-addr]	End ipv6 multicast address
(permit | deny)	permit: allow Multicast address range ipv6 address learning

Mode:

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

ipv6 mld profile <1-128>

Global Configuration

profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)

mld profile config mode

Usage Guide:

Use '**ipv6 mld profile 1**' entry to the mld profile config mode.

User '**profile range ipv6 ff12::1 ff12::8 action permit**' to configure the profile entry.

The profile entry is used by port filter.

The configure can use '**show ipv6 mld profile [<1-128>]**' to display

Example:

This example shows how to set ipv6 mld profile.

```
Switch(config)# ipv6 mld profile 1
Switch(config-mld-profile)# profile range ipv6 ff13::1 ff13::10 action permit
Switch(config-mld-profile)#show ipv6 mld profile
IPv6 mld profile index: 1
IPv6 mld profile action: permit
Range low ip: ff13::1
Range high ip: ff13::10
Switch(config-mld-profile)#exit
Switch(config)# ipv6 mld profile 5
Switch(config-mld-profile)# profile range ipv6 ff12::1 ff12::12 action deny
Switch(config-mld-profile)#show ipv6 mld profile
IPv6 mld profile index: 5
IPv6 mld profile action: deny
Range low ip: ff12::1
Range high ip: ff12::12
Switch(config-mld-profile)#exit
Switch(config)# exit
Switch# show ipv6 mld profile
IPv6 mld profile index: 1
IPv6 mld profile action: permit
Range low ip: ff13::1
Range high ip: ff13::10
IPv6 mld profile index: 5
IPv6 mld profile action: deny
Range low ip: ff12::1
Range high ip: ff12::12
```


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

3.17.10 ipv6 mld filter

Command:

```
ipv6 mld profile <1-128>

profile range ipv6 <ipv6-addr> [ipv6-addr] action (permit | deny)

show ipv6 mld profile [<1-128>]
```

Parameter:

<1-128>	specifies profile ID
[interfaces IF_PORTS]	Specifies interfaces to display

Mode:

Interface mode

Usage Guide:

After create ipv6 mld profile entry. Can use '**ipv6 mld filter 1**' to bind a profile for port.

When then port bind a profile. Then the port learning group will update, if the group is not match the profile rule it will remove the port from the group. Static group is excluded.

The configure can use '**show ipv6 mld filter** ' to display

Example:

This example shows how to set ipv6 mld filter

```
Switch(config)# ipv6 mld profile 1
Switch(config-igmp-profile)# profile range ipv6 ff13::1 ff13::10 action permit
Switch(config-igmp-profile)#exit
Switch(config)# interface gi1
Switch(config-if)# ipv6 mld filter 1
Switch(config-if)#exit
Switch(config)# exit
Switch# show ipv6 mld filter
Port ID | Profile ID
---------+--------------
gi1 : 1
gi2 : None
gi3 : None
gi4 : None gi5 : None
```


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

3.17.11 ipv6 mld max-groups

Command:

```
ipv6 mld max-groups <0-256>

no ipv6 mld max-groups

ipv6 mld max-groups action (deny | replace)

show ipv6 mld max-group [interfaces IF_PORTS]

show ipv6 mld max-group action [interfaces IF_PORTS]
```

Parameter:

<1-128>	specifies profile ID
(deny | replace)	Deny: current port ipv6 group arrived max-groups, don't add group.

Default:

no ipv6 mld max-groups

ipv6 mld max-groups action deny

Mode:

Interface mode

Usage Guide:

use '**ipv6 mld max-groups 10**' to limit port learning max group num is 10.

When then port had learned more than 10 groups, then the more than 10 group will be remove the port form group.

static group is excluded.

The configure can use '**show ipv6 mld max-group & show ipv6 mld max-group action** ' to display

Example:

This example shows how to set ipv6 mld max-groups and action is replace

```
Switch(config)# interface gi1
Switch(config-if)# ipv6 mld max-groups 10
Switch(config-if)# ipv6 mld max-groups action replace
Switch(config-if)#exit
Switch(config)# exit
Switch# show ipv6 mld max-group
Port ID | Max Group
---------+--------------
```


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

```
gi1 : 10 gi2 : 256
gi3 : 256
gi4 : 256
gi5 : 256
--More--
Switch# show ipv6 mld max-group action
Port ID | Max-groups Action
---------+--------------------- gi1 : replace
gi2 : deny
gi3 : deny gi4 : deny
gi5 : deny
--More--
```

3.17.12 clear ipv6 mld snooping groups

Command:

```
clear ipv6 mld snooping groups [(dynamic | static)]
```

Parameter:

None	Clear ipv6 mld groups include dynamic and static
(dynamic | static)	ipv6 mld group type is dynamic or static

Default:

clear all ipv6 mld groups

Mode:

Privileged mode

Usage Guide:

This command will clear the ipv6 mld groups for dynamic or static or all of type.

The configuration can use '**show ipv6 mld snooping groups**' to check.

Example:

This example shows how to clear ipv6 mld snooping groups

```
Switch# clear ipv6 mld snooping groups static

Switch# show ipv6 mld snooping groups

Switch# clear ipv6 mld snooping groups

Switch# show ipv6 mld snooping groups
```

3.17.13 clear ipv6 mld snooping statistics

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

Command:

```
clear ipv6 mld snooping statistics
```

Mode:

privileged mode

Usage Guide:

This command will clear the mld statistics.

The configure can use show ipv6 mld snooping.

Example:

This example shows how to clear ipv6 mld snooping statistics

```
Switch# clear ipv6 mld snooping statistics
Switch# show ipv6 mld snooping
```

3.17.14 show ipv6 mld snooping groups counters

Command:

```
show ipv6 mld snooping groups counters
```

Mode:

privileged mode

Usage Guide:

This command will display the ipv6 mld group counter include static group.

Example:

This example shows how to display ipv6 mld snooping group counter

```
Switch# show ipv6 mld snooping counters
```


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

3.17.15 show ipv6 mld snooping groups

Command:

```
show ipv6 mld snooping groups [(dynamic | static)]
```

Parameter:

none	Show ipv6 mld groups include dynamic and static
(dynamic | static)	Display ipv6 mld group type is dynamic or static

Mode:

Privileged mode

Usage Guide:

This command will display the ipv6 mld groups for dynamic or static or all of type.

Example:

This example shows show ipv6 mld snooping groups

```
Switch# show ipv6 mld snooping groups
Switch# show ipv6 mld snooping groups dynamic
Switch# show ipv6 mld snooping groups static
```

3.17.16 show ipv6 mld snooping router

Command:

```
show ipv6 mld snooping router [(dynamic | forbidden |static )]
```

Parameter:

none	Show ipv6 mld router include dynamic and static and forbidden
(dynamic | forbidden | static)	Display ipv6 mld router info for different type

Mode:

privileged mode

Usage Guide:

This command will display the ipv6 mld router info.

Example:

This example shows how to show ipv6 mld snooping router

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

```
Switch# show ipv6 mld snooping router
Switch# show ipv6 mld snooping router dynamic
Switch# show ipv6 mld snooping rotuer static
Switch# show ipv6 mld snooping rotuer forbidden
```

3.17.17 show ipv6 mld snooping

Command:

```
show ipv6 mld snooping
```

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld snooping global info.

Example:

This example shows how to show ipv6 mld snooping

```
Switch# show ipv6 mld snooping
MLD Snooping Status
--------------------
Snooping : Disabled
Report Suppression : Enabled
Operation Version : v1
Forward Method : mac
Unknown Multicast Action : Flood
Packet Statistics
Total RX : 0
Valid RX : 0
Invalid RX : 0
Other RX : 0
Leave RX : 0
Report RX : 0
General Query RX : 0
Specail Group Query RX : 0
Specail Group & Source Query RX : 0
```


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

```
Leave TX : 0
Report TX : 0
General Query TX : 0
Specail Group Query TX : 0
Specail Group & Source Query TX : 0
```

3.17.18 show ipv6 mld snooping vlan

Command:

```
show ipv6 mld snooping vlan [VLAN-LIST]
```

Parameter:

[VLAN-LIST]	Show specifies vlan ipv6 mld snooping info

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld snooping vlan info.

Example:

This example shows how to show ipv6 mld snooping vlan

```
Switch# show ipv6 mld snooping vlan
MLD Snooping is globaly disabled
MLD Snooping VLAN 1 admin : disabled
MLD Snooping oper mode : disabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper 10 sec
MLD Snooping last member query counter: admin 2 oper 2
MLD Snooping last member query interval: admin 1 sec oper 1 sec
MLD Snooping last immediate leave: disabled
MLD Snooping automatic learning of multicast router ports: enabled
```


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

3.17.19 show ipv6 mld snooping forward-all

Command:

```
show ipv6 mld snooping forward-all [vlan VLAN-LIST]
```

Parameter:

[vlan VLAN-LIST] Show specifies vlan of ipv6 mld forward info.

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld snooping forward all info.

Example:

This example shows how to show ipv6 mld snooping forward-all

```
Switch# show ipv6 mld snooping forward-all
MLD Snooping VLAN : 1
MLD Snooping static port : None
MLD Snooping forbidden port : None
```

3.17.20 show ipv6 mld profile

Command:

```
show ipv6 mld profile [<1-128>]
```

Parameter:

[<1-128>] Show specifies index profile info

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld profile info.

Example:

This example shows how to show ipv6 mld profile

```
Switch# show ipv6 mld profile
```


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

```
IPv6 mld profile index: 1
IPv6 mld profile action: permit
Range low ip: ff13::1
Range high ip: ff13::10
```

3.17.21 show ipv6 mld filter

Command:

```
show ipv6 mld filter [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports filter

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld port filter info.

Example:

This example shows how to show ipv6 mld filter

```
Switch# show ipv6 mld filter
Port ID | Profile ID
---------+--------------
gi1 : 1
gi2 : None
gi3 : None
gi4 : None gi5 : None
--More--
```


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

3.17.22 show ipv6 mld max-group

Command:

```
show ipv6 mld max-group [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports max-group

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld port max-group.

Example:

This example shows how to show ipv6 mld max-group.

```
Switch(config)#interface gi1
Switch(config-if)# ipv6 mld max-groups 50
Switch(config-if)#exit
Switch(config)#exit
Switch# show ipv6 mld max-group
Port ID | Max Group
---------+--------------
gi1 : 50 gi2 : 256
gi3 : 256
gi4 : 256
gi5 : 256
--More--
```

3.17.23 show ipv6 mld max-group action

Command:

```
show ipv6 mld max-group action [interfaces IF_PORTS]
```

Parameter:

[interfaces IF_PORTS]	Show specifies ports max-group action

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

Mode:

privileged mode

Usage Guide:

This command will display ipv6 mld port max-group action.

Example:

This example shows how to show ipv6 mld max-group action.

```
Switch(config)#interface gi1
Switch(config-if)# ipv6 mld max-groups action replace
Switch(config-if)#exit
Switch(config)#exit
Switch# show ipv6 mld max-group action
Port ID | Max-groups Action
---------+--------------------- gi1 : replace
gi2 : deny
gi3 : deny gi4 : deny
gi5 : deny
--More--
```


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

3.18 Port Security

3.18.1 port-security

Command:

```
port-security

no port-security
```

Default:

Default is disabled

Mode:

Global Configuration

Usage Guide:

The "**port-security**" command enables the port security functionality on this port.

Use the **no** form of this command to disable

Example:

This example shows how to enable port security on port 1 and set the learning limit number to 10.

```
switch(config)# interface gi1
switch(config-if)# port-security address-limit 10 action discard
switch(config-if)# port-security
switch(config)# show port-security interfaces gi1
Port | Mode | Security | CurrentAddr | Action
-------------+------------+----------------------+---------------+----------------------
gi1 | Dynamic | Enabled ( 10) | 0 | Discard
```

3.18.2 port-security address-limit

Command:

```
port-security address-limit <1-256> action (forward|discard|shutdown)

no dot1x port-control address-limit
```

Parameter:

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

<1-256>	The learning-limit number. It specifies how many MAC addresses this port can learn
forward	Forward this packet whose SMAC is new to system and exceed the learning-limit number
discard	Discard this packet whose SMAC is new to system and exceed the learning-limit number.
shutdown	Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

Default:

The address-limit default is 10 and action is “discard”.

Mode:

Interface Configuration

Usage Guide:

Use the “**port-security address-limit**” command to set the learning-limit number and the violation action. Use the **no** form of this command to restore the default settings.

Example:

The following example shows how to enable port security on port 1 and set the learning limit number to 10.

```
switch(config)# interface gi1
switch(config-if)# port-security address-limit 10 action discard
switch(config-if)# port-security
switch(config)# show port-security interfaces gi1
Port | Mode | Security | CurrentAddr | Action
-------------+------------+----------------------+---------------+----------------------
gi1 | Dynamic | Enabled ( 10) | 0 | Discard
```

3.18.3 show port-security

Command:

```
show port-security interface IF_PORTS
```

Parameter:

IF_PORTS	Select port to show port-security configurations.

Mode:

Privileged EXEC

Usage Guide:

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

Use “**show port-security interfaces**” command to show port-security information of the specified port.

Example:

This example shows how to show port-security configurations on interface gi1.

```
Switch# show port-security interfaces gi1
Port | Mode | Security | CurrentAddr | Action
-------------+------------+----------------------+---------------+----------------------
gi1 | Dynamic | Enabled ( 10) | 0 | Discard
```


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

3.19 Port Error Disable

3.19.1 errdisable recovery cause

Command:

```
errdisable recovery cause (all | acl | arp-inspection | broadcast-flood | bpduguard |
dhcp-rate-limit | psecure-violation | unicast-flood | udld | unknown-multicast-flood |
selfloop)

no errdisable recovery cause (all | acl | arp-inspection | broadcast-flood |
bpduguard | dhcp-rate-limit | psecure-violation | unicast-flood | udld | unknown-
multicast-flood | selfloop)
```

Parameter:

all	Enable/Disable to auto recovery for port error disabled by all reasons
acl	Enable/Disable to auto recovery for port error disabled by ACL shutdown port reason.
arp-inspection	Enable/Disable to auto recovery for port error disabled by arp-inspection reason.
broadcast-flood	Enable/Disable to auto recovery for port error disabled by storm control broadcast flood reason.
bpduguard	Enable/Disable to auto recovery for port error disabled by STP BPDU Guard reason.
dhcp-rate-limit	Enable/Disable to auto recovery for port error disabled by dhcp-rate-limit reason.
psecure-violation	Enable/Disable to auto recovery for port error disabled by violate port security rule reason.
unicast-flood	Enable/Disable to auto recovery for port error disabled by storm control unicast flood reason.
udld	Enable/Disable to auto recovery for port error disabled by udld reason.
unknown-multicast-flood	Enable/Disable to auto recovery for port error disabled by storm control unknown multicast flood reason.
selfloop	Enable/Disable to auto recovery for port error disabled by self loop detect reason.

Default:

Default auto recover state for all reasons are disabled.

Mode:

Global Configuration

Usage Guide:

Port will be disabled by some invalid actions detected by protocols. Administrator can enabled these error disabled

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

port manually by "**no shutdown**" command in Interface Mode, or just turn on the auto recovery mechanism by this command to auto enable the error disabled port after auto recovery interval.

Example:

This example shows how to enable auto recovery with reason bpduguard and broadcast-flood.

```
Switch(config)# errdisable recovery cause bpduguard
Switch(config)# errdisable recovery cause broadcast-flood
```

This example shows how to show current auto recovery state of each reason and port error disabled status.

```
Switch# show errdisable recovery
ErrDisable Reason | Timer Status
--------------------------+---------------
bpduguard | enabled
udld | disabled
selfloop | disabled
broadcast-flood | enabled
unknown-multicast-flood | disabled
unicast-flood | disabled
acl | disabled
psecure-violation | disabled
dhcp-rate-limit | disabled
arp-inspection | disabled
Timer Interval : 300 seconds
Interfaces that will be enabled at the next timeout:
Port | Error Disable Reason | Time Left
-----+----------------------------+------------
```

3.19.2 errdisable recovery interval

Command:

```
errdisable recovery interval <0-86400>
```

Parameter:

<0-86400>	Specify the auto recovery interval with unit second.

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

Default:

Default auto recovery interval is 300 second.

Mode:

Global Configuration

Usage Guide:

Port will be disabled by some invalid actions detected by protocols. Auto recovery mechanism will enable these error disabled port after a while. This command configures how long the port will be enabled after error disabled.

Example:

This example shows how to configure the auto recovery interval to 600 seconds.

```
Switch(config)# errdisable recovery interval 600
```

This example shows how to show current auto recovery interval

```
Switch# show errdisable recovery
ErrDisable Reason | Timer Status
-------------------------+---------------
bpduguard | enabled
udld | disabled
selfloop | disabled
broadcast-flood | enabled
unknown-multicast-flood | disabled
unicast-flood | disabled
acl | disabled
psecure-violation | disabled
dhcp-rate-limit | disabled
arp-inspection | disabled
Timer Interval : 600 seconds
Interfaces that will be enabled at the next timeout:
Port | Error Disable Reason | Time Left
-----+----------------------------+------------
```

3.19.3 show errdisable recovery

Command:

```
show errdisable recovery
```


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

Mode:

Privileged EXEC

Usage Guide:

Use "**show errdisable recovery**" command to show each error disable state, error disable recovery interval and current error disabled port status.

Example:

This example shows how to show current auto recovery interval

```
Switch# show errdisable recovery
ErrDisable Reason | Timer Status
-------------------------+---------------
bpduguard | enabled
udld | disabled
selfloop | disabled
broadcast-flood | enabled
unknown-multicast-flood | disabled
unicast-flood | disabled
acl | disabled
psecure-violation | disabled
dhcp-rate-limit | disabled
arp-inspection | disabled
Timer Interval : 600 seconds
Interfaces that will be enabled at the next timeout:
Port | Error Disable Reason | Time Left
-----+----------------------------+------------
```


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

3.20 Port

3.20.1 description

Command:

```
description WORD<1-32>

no description
```

Parameter:

WORD<1-32> Specifiy port description string

Mode:

Interface Configuration

Usage Guide:

Use "**description**" command to give the port a name to identify it easily.

If description includes space character, please use double quoted to wrap it.

Use no form to restore description to empty string.

Example:

This example shows how to modify port descriptions.

```
Switch(config)# interface gi1
Switch(config-if)# description userport
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# description "uplink port"
```

This example shows how to show current port description on interface fa1 and fa2

```
Switch# show interfaces gi1-2 status
Port Name Status Vlan Duplex Speed Type
gi1 userport notconnect 1 auto auto Copper
gi2 uplink port notconnect 1 auto auto Copper
```


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

3.20.2 speed

Command:

```
speed (10 | 100 | 1000)

speed auto [(10 | 100 | 1000 | 10/100)]
```

Parameter:

10	Specify port speed to force 10Mbits/s or auto with 10Mbits/s ability.
100	Specify port speed to force 100Mbits/s or auto with 100Mbits/s ability.
1000	Specify port speed to force 1000Mbits/s or auto with 1000Mbits/s ability.
10/100	Specify port speed to auto with 10Mbits/s and 100Mbits/s

Default:

Default port speed is auto with all available abilities.

Mode:

Interface Configuration

Usage Guide:

Use "**speed**" command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 1000 is not available.

Example:

This example shows how to modify port speed configuration.

```
Switch(config)# interface gi1
Switch(config-if)# speed 100
Switch(config-if)# exit
Switch(config)# interface gi2
Switch(config-if)# speed auto 10/100
```

This example shows how to show current speed configuration

```
Switch# show running-config interfaces gi1-2
interface gi1
speed 100
interface gi2
speed auto 10/100
```

This example shows how to show current interface link speed

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

```
Switch# show interfaces gi1-2 status
Port Name Status Vlan Duplex Speed Type
gi1 connected 1 a-full a-100M Copper
gi2 connected 1 a-full a-100M Copper
```

3.20.3 duplex

Command:

```
duplex (auto | full | half)
```

Parameter:

auto	Specify port duplex to auto negotiation.
full	Specify port duplex to force full duplex.
half	Specify port duplex to force half duplex.

Default:

Default port duplex is auto.

Mode:

Interface Configuration

Usage Guide:

Use "**duplex**" command to change port duplex configuration.

Example:

This example shows how to add a login authentication list to authenticate with order tacacs+, radius, local.

```
Switch(config)# aaa authentication login test1 tacacs+ radius local
```

3.20.4 flow-control

Command:

```
flow-control (off | on)
no flow-control
```

Parameter:

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

off	Disable port flow control.
on	Enable port flow control.

Default:

Default port flow control is off.

Mode:

Interface Configuration

Usage Guide:

Use "**flow-control**" command to change port flow control configuration.

Use no form to restore flow control to default (off) configuration.

Example:

This example shows how to modify port duplex configuration.

```
Switch(config)# interface gi1
Switch(config-if)# flow-control on
```

This example shows how to show current flow control configuration

```
Switch# show interfaces gi1
Hardware is Gigabit
Full-duplex, Auto-speed, media type is Copper
flow-control is on
0 packets input, 0 bytes, 0 throttles
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
379 packets output, 31981 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```


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

3.20.5 shutdown

Command:

```
shutdown

no shutdown
```

Mode:

Interface Configuration

Usage Guide:

Use "**shutdown**" command to disable port and use "**no shutdown**" to enable port. If port is error disabled by some reason, use "no shutdown" command can also recovery the port manually.

Example:

This example shows how to modify port duplex configuration.

```
Switch(config)# interface gi1
Switch(config-if)# shutdown
```

This example shows how to show current admin state configuration

```
Switch# show running-config interfaces gi1
interface gi1
shutdown
```

3.20.6 jumbo-frame

Command:

```
jumbo-frame <64-9216>
```

Parameter:

<64-9216>	Specify the maximum frame size.

Default:

Default maximum frame size is 1522.

Mode:

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

Interface Configuration

Usage Guide:

Use "**jumbo-frame**" command to modify maximum frame size.

The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to modify maximum frame size on gi1 to 9216 bytes.

```
Switch(config)# interface gi1
Switch(config-if)# jumbo-frame 9216
```

This example shows how to show current jumbo-frmae size

```
Switch# show running-config interface gi1
interface gi1
jumbo-frame 9216
```

3.20.7 protected

Command:

```
protected

no protected
```

Mode:

Interface Configuration

Usage Guide:

Use "**protected**" command to make port to be protected. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port.

Use no form to make port unprotected.

Example:

This example shows how to configure port fa1 and fa2 to be protected port.

```
Switch(config)# interface range gi1-2
Switch(config-if-range)# protected
```


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

This example shows how to show current protected port state.

```
Switch# show interfaces gi1-2 protected
Port | Protected State
-------+-----------------
gi1 |enabled
gi2 |enabled
```

3.20.8 eee

Command:

```
eee

no eee
```

Default:

Default eee state is disabled.

Mode:

Interface Configuration

Usage Guide:

Use "**eee**" command to make port to enable the energy efficient Ethernet feature and use "**no eee**" command to disable it.

The only way to show this configuration is using "**show running-config**" command.

Example:

This example shows how to configure port gi1 to be protected port.

```
Switch(config)# interface gi1
Switch(config-if)# eee
```

This example shows how to show current jumbo-frmae size

```
Switch# show running-config interface gi1
interface gi1
eee
```


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

3.20.9 clear interface

Command:

```
clear interfaces IF_PORTS counters
```

Parameter:

IF_PORTS	Specifiy port to clear counters.

Mode:

Privileged EXEC

Usage Guide:

Use "**clear interface**" command to clear counters on specific ports.

Example:

This example shows how to clear counters on port gi1.

```
Switch(config)# clear interfaces gi1 counters
```

This example shows how to show current counters

```
Switch# show interfaces gi1
Hardware is gigabit
Auto-duplex, Auto-speed, media type is Copper
flow-control is off
0 packets input, 0 bytes, 0 throttles
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```


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

3.20.10 show interface

Command:

```
show interfaces IF_PORTS

show interfaces IF_PORTS status

show interfaces IF_PORTS potected
```

Parameter:

IF_PORTS	Specifiy port to show.

Mode:

Privileged EXEC

Usage Guide:

Use "**show interface**" command to show port counters, parameters and status.

Example:

This example shows how to show current counters

```
Switch# show interfaces gi1
Hardware is Gigabit
Auto-duplex, Auto-speed, media type is Copper
flow-control is off
0 packets input, 0 bytes, 0 throttles
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underrun
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 PAUSE output
```


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

This example shows how to show current protected port state.

```
Switch# show interfaces gi1-2 protected
Port | Protected State
-------+-----------------
gi1 |enabled
gi2 |enabled
```

This example shows how to show current port status

```
Switch# show interfaces gi1 status
Port Name Status Vlan Duplex Speed Type
gi1 connected 1 full a-100M Copper
```


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

3.21 QoS

3.21.1 qos

Command:

```
qos basic

no qos
```

Parameter:

basic	Specify the device to qos basic mode

Mode:

Global Configuration

Usage Guide:

QoS have following 2 modes, use this command is able to switch between them.

Disable:

QoS function is disabled and all packets will go through lowest priority queue. It means first in will be first out, no QoS is guarantee.

Basic:

According to basic trust type to assign queue for packets, and packets with higher priority are able to send first.

Example:

This example shows how to change qos to basic mode.

```
Switch(config)# qos basic
```

This example shows how to change qos to disabled mode.

```
Switch(config)# no qos
```

This example shows how to check current qos mode

```
Switch# show qos
QoS Mode: basic
Basic trust: cos
```


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

3.21.2 qos trust

Command:

```
qos trust (cos | cos-dscp | dscp | precedence)
```

Parameter:

cos	Specify the device to trust CoS
cos-dscp	Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets.
dscp	Specify the device to trust DSCP
precedence	Specify the device to trust IP Precedence

Default:

Default qos basic mode trust type is cos.

Mode:

Global Configuration

Usage Guide:

In QoS basic mode, there are 4 trust types for device to judge the appropriate queue of the packets. This command is able to switch between these trust types.

CoS:

IEEE 802.1p defined 3bits priority value in vlan tag. Trust this value in packets and assign queue according to cos-queue map.

DSCP:

IETF RFC2474 defined 6bits priority value in IP packet (highest 6bits in ToS field). Trust this value in packets and assign queue according to dscp-queue map.

IP Precedence:

The highest 3bits priority value in IP packet ToS field. Trust this value in packets and assign queue according to precedence-queue map.

CoS-DSCP:

Trust DSCP for IP packets and assign queue according to dscp-queue map. Trust CoS for non-IP packets and assign queue according to cos-queue map.

Example:

This example shows how to change qos basic mode trust types.

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

```
Switch(config)# qos trust cos
Switch(config)# qos trust cos-dscp
Switch(config)# qos trust dscp
Switch(config)# qos trust precedence
```

This example shows how to check current qos trust type.

```
Switch# show qos
QoS Mode: basic
Basic trust: cos
```

3.21.3 qos map

Command:

```
qos map (cos-queue | dscp-queue | precedence-queue) SEQUENCE to <1-8>

qos map (queue-cos | queue-precedence) SEQUENCE to <0-7>

qos map queue-dscp SEQUENCE to <0-63>
```

Parameter:

cos-queue	Configure or show CoS to queue map
dscp-queue	Configure or show DSCP to queue map
precedence-queue	Configure or show IP Precedence to queue map.
queue-cos	Configure or show queue to CoS map
queue-dscp	Configure or show queue to DSCP map
queue-precedence	Configure or show queue to IP Precedence map
SEQUENCE	Specify the cos, dscp, precedence or queue with one or multiple values.
<1-8>	Specify th queue id
<0-7>	Specify the cos or precedence values
<0-63>	Specify the dscp values

Default:

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

The default values of cos-queue are showing in the following table.

CoS	Queue ID
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

The default values of dscp-queue are showing in the following table.

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

The default values of ip precedence are showing in the following table.

IP Precedence	Queue ID
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

The default values of queue-cos are showing in the following table.

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

Queue ID	CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

The default values of queue-dscp are showing in the following table.

Queue ID	DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

The default values of queue-precedence are showing in the following table.

Queue ID	DSCP
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Mode:

Global Configuration

Usage Guide:

According to different trust type, packets will be assigned to different queue based on the specific qos map. For example, if the trust type is trust cos, the device will get the cos value in packet and reference the cos-queue mapping to assign the correct queue.

The queue to cos, dscp or precedence maps are used by remarking function. If the port remarking feature is enabled, the remarking function will reference these 3 tables to remark packets.

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

Example:

This example shows how to map cos 6 and 7 to queue 1.

```
Switch(config)# qos map cos-queue 6 7 to 1
Switch# show qos map cos-queue
CoS to Queue mappings
COS 0 1 2 3 4 5 6 7
--------------------------------
Queue 2 1 3 4 5 6 1 1
```

This example shows how to map queue 4 and 5 to cos 7.

```
Switch(config)# qos map queue-cos 4 5 to 7
Switch# show qos map queue-cos
Queue to CoS mappings
Queue 1 2 3 4 5 6 7 8
--------------------------------
CoS 1 0 2 7 7 5 6 7
```

3.21.4 qos queue

Command:

```
qos queue strict-priority-num <0-8>

qos queue weight SEQUENCE

show qos queueing
```

Parameter:

strict-priority-num *<0-8>*	Specify the strict priority queue number
weight *SEQUENCE*	Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127.

Default:

Default strict priority queue number is 8, it means all queues are strict priority queue.

The default queue weight for each queue is shown in following table.

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

Queue ID	Queue Weight
1	1
2	2
3	3
4	4
5	5
6	9
7	13
8	15

Mode:

Global Configuration

Usage Guide:

The device support total 8 queues for QoS queueing. It is able to set the queue to be strict priority queue or weighted queue to prevent starvation. The queue with higher id value has higher priority.

First, you need to decide how many strict priority queue you need. The strict priority queue will always occupy the higher priority queue. For example, if you specify the strict priority number to be 2, then the queue 7 and 8 will be the strict priority queues and the others are weighted queues.

After you setup the number of strict priority queue, you need to setup the weight for the weighted queues by using "qos queue weight" command. And the bandwidth will shared by the weight you configured between these weighted queues.

Example:

This example shows how to setup device with 3 strict priority queues and give other weighted queues with weight 5, 10, 15, 20, 25.

```
Switch(config)# qos queue strict-priority-num 3
Switch(config)# qos queue weight 5 10 15 20 25
Switch# show qos queueing
qid-weights Ef - Priority
1 - 5 dis- N/A
2 - 10 dis- N/A
3 - 15 dis- N/A
4 - 20 dis- N/A
5 - 25 dis- N/A
6 - N/A ena- 6
7 - N/A ena- 7
8 - N/A ena- 8
```

3.21.5 qos cos

Command:

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

```
qos cos <0-7>
```

Parameter:

cos <*0-7*> Specify the CoS value for the interface.

Default:

Default CoS value for interface is 0.

Mode:

Interface Configuration

Usage Guide:

Sometimes, there is no qos information in the packets, such as CoS, DSCP, IP Precedence. But we still can give the priority for packets by configuring the interface default cos value. If there is no qos information in the packets, the device will use this default cos value and find the cos-queue map to get the final destination queue.

Use "**qos cos**" command to assign port default cos value.

Example:

This example shows how to configure default cos value 7 on interface gi1.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# qos cos 7
Switch(config-if)# end
Switch# show qos interface GigabitEthernet 1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
--------+-------+---------------+------------+-------------+----------------
gi1 | 7 | enabled | disabled | disabled | disabled |
```

3.21.6 qos trust

Command:

```
qos trust

no qos trust
```

Default:

Default interface qos trust state is enabled.

Mode:

Interface Configuration

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

Usage Guide:

After QoS function is enabled in basic mode, the device also support per interface enable/disable the qos function. If the trust state on interface is enabled, all ingress packets of this interface will remap according to the trust type and the qos maps. Otherwise, all ingress packets will assign to queue 1.

Use "**qos trust**" to enable trust state on interface and use "**no qos trust**" to disable trust state on interface.

Example:

This example shows how to disable qos trust state on interface gi1.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# no qos trust
Switch(config-if)# end
Switch# show qos interface GigabitEthernet 1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
--------+-------+---------------+------------+-------------+----------------
gi1 | 0 | disabled | disabled | disabled | disabled |
```

3.21.7 qos remark

Command:

```
qos remark (cos | dscp | precedence)

no qos remark (cos | dscp | precedence)
```

Parameter:

cos	Enable/Disable cos remarking.
dscp	Enable/Disable dscp remarking.
precedence	Enable/Disable precedence remarking.

Default:

Default CoS remarking is disabled.

Default DSCP remarking is disabled.

Default IP Precedence remarking is disabled.

Mode:

Interface Configuration

Usage Guide:

QoS remarking feature allow you to change priority information in packets based on egress queue. For example, you want all packets egress from interface fa1 queue 1 to remark the cos value to be 5 for next tier of device, you can enable the cos remarking feature on fa1 and configure the queue-cos map for queue 1 map to cos 5.

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

Use “**qos remark**” command to enable remarking feature on specific type. And use “**no qow remark**” command to disable it.

Example:

This example shows how to enable remarking features on interface gi1.

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# qos remark cos
Switch(config-if)# qos remark dscp
Switch(config-if)# qos remark precedence
Switch(config-if)# end
Switch# show qos interface GigabitEthernet 1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
--------+-------+---------------+------------+-------------+----------------
gi1 | 0 | enabled | enabled | enabled | enabled
```

3.21.8 show qos

Command:

```
show qos
```

Mode:

Privileged EXEC

Usage Guide:

Use “**show qos**” command to show qoe mode and trust type.

Example:

This example shows how to check current qos mode.

```
Switch# show qos
QoS Mode: basic
Basic trust: cos
```

3.21.9 show qos map

Command:

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

show qos map [(cos-queue | dscp-queue | precedence-queue | queue-cos | queue-dscp | queue-precedence)]

Parameter:

cos-queue	Show CoS to queue map.
dscp-queue	Show DSCP to queue map
precedence-queue	Show IP Precedence to queue map.
queue-cos	Show queue to CoS map.
queue-dscp	Show queue to DSCP map.
queue-precedence	Show queue to IP Precedence map.

Mode:

Privileged EXEC

Usage Guide:

Use "**show qos map**" command to show all kinds of mapping for qos remapping and remarking features.

Example:

This example shows how to show all qos maps.

```
Switch(config)# show qos map
CoS to Queue mappings
COS 0 1 2 3 4 5 6 7
--------------------------------
Queue 2 1 3 4 5 6 7 8
DSCP to Queue mappings
d1: d2 0 1 2 3 4 5 6 7 8 9
---------------------------------------
0: 1 1 1 1 1 1 1 1 2 2
1: 2 2 2 2 2 2 3 3 3 3
2: 3 3 3 3 4 4 4 4 4 4
3: 4 4 5 5 5 5 5 5 5 5
4: 6 6 6 6 6 6 6 6 7 7
5: 7 7 7 7 7 7 8 8 8 8
6: 8 8 8 8
IP Precedence to Queue mappings
IP Precedence 0 1 2 3 4 5 6 7
----------------------------------------
Queue 1 2 3 4 5 6 7 8
Queue to CoS mappings
```


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

```
Queue 1 2 3 4 5 6 7 8
--------------------------------
CoS 1 0 2 3 4 5 6 7
Queue to DSCP mappings
Queue 1 2 3 4 5 6 7 8
--------------------------------
DSCP 0 8 16 24 32 40 48 56
Queue to IP Precedence mappings
Queue 1 2 3 4 5 6 7 8
--------------------------------
ipprec 0 1 2 3 4 5 6 7
```

3.21.10 show qos interface

Command:

show qos interface *IF_PORTS*

Parameter:

IF_PORTS Select port to show qos configurations.

Mode:

Privileged EXEC

Usage Guide:

Use "**show qos interfaces**" command to show port default cos ,remarking state and remarking type state informations.

Example:

This example shows how to show qos configurations on interface gi1.

```
Switch# show qos interface GigabitEthernet 1
Port | CoS | Trust State | Remark Cos | Remark DSCP | Remark IP Prec
--------+-------+---------------+------------+-------------+----------------
gi1 | 7 | enabled | disabled | disabled | disabled |
```


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

3.22 Rate Limit

3.22.1 rate limit

Command:

```
rate-limit ingress burst <1-65535>

no rate-limit ingress burst

rate-limit egress burst <4578-50000>

rate-limit egress queue burst <1-8> <1-65535>

no rate-limit egress burst [<1-8>]
```

Parameter:

burst	Specify the maximum permitted excess burst size (CBS) in bytes
<1-8>	Specify the egress shaper queue number

Default:

Rate limiting is disabled.

Mode:

Global Configuration

Usage Guide:

Use the **rate-limit ingress burst** Global Configuration mode command to limit the incoming traffic rate for all ports.

Use the no form of this command to disable the rate limit

Use the **rate-limit egress burst** Global Configuration mode command to configure the egress ports or queue shaper. Use the no form of this command to disable the shaper

You can verify your setting by entering the **show running-config** Privileged EXEC command

Example:

The following example show how to configure ingress port rate limit and egress port & queue shaper.

```
Switch(config)# rate-limit ingress burst 5000
Switch(config)# rate-limit egress burst 6000
Switch(config)# rate-limit egress queue burst 7000
Switch# show running-config
rate-limit ingress burst 5000
rate-limit egress burst 6000
rate-limit egress queue burst 7000
```

3.22.2 rate limit (interface)

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

Command:

```
rate-limit ingress <0-1000000>

no rate-limit ingress

rate-limit egress <0-1000000>

rate-limit egress queue <1-8> <0-1000000>

no rate-limit egress [<1-8>]
```

Parameter:

Cir	Specify the maximum number of kilobits per second of ingress traffic on a port. The range is 100 –max port speed.
<1-8>	Specify the egress shaper queue number

Mode:

Interface Configuration

Usage Guide:

Use the **rate-limit ingress** Interface Configuration mode command to limit the incoming traffic rate on a port. Use the no form of this command to disable the rate limit

Use the **rate-limit egress** Interface Configuration mode command to configure the egress port or queue shaper. Use the no form of this command to disable the shaper

You can verify your setting by entering the **show running-config** interfaces Privileged EXEC command

Example:

The following example show how to configure ingress port rate limit and egress port & queue shaper.

```
Switch(config)# interfaces gi7
Switch(config-if)# rate-limit ingress 128
Switch(config-if)# rate-limit egress 2048
Switch(config-if)# rate-limit egress queue 1 512
Switch# show running-config interfaces gi7
interface gi7
rate-limit ingress 128
rate-limit egress 2048 165
rate-limit egress queue 1 512
```


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

3.23 RMON

3.23.1 Rmon event

Command:

```
rmon event <1-65535> [log] [trap COMMUNITY] [description DESCRIPTION] [owner
NAME]

no rmon event <1-65535>
```

Parameter:

<1-65535>	Specify event index to create or modify
[log]	(Optional)Specify to show syslog.
[trap COMMUNITY]	(Optional)Specify SNMP community to show SNMP trap.
[description DESCRIPTION]	(Optional)Specify description of event
[owner NAME]	(Optional)Specify owner of event.

Mode:

Global Configuration

Usage Guide:

Use the **rmon alarm** command to add or modify a RMON alarm entry. Use the **no** form of this command to delete.

Example:

The example shows how to add RMON event entry with log and trap action and then modify it action to log only. You can verify settings by the following **show rmon event** command.

```
switch(config)# rmon event 1 log trap public description test owner admin
switch(config)# show rmon event 1
Rmon Event Index : 1
Rmon Event Type : Log and Trap
Rmon Event Community : public
Rmon Event Description : test
Rmon Event Last Sent :
Rmon Event Owner : admin
switch(config)# rmon event 1 log description test owner admin
switch(config)# show rmon event 1
Rmon Event Index : 1
Rmon Event Type : Log
```


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

```
Rmon Event Community : public
Rmon Event Description : test
Rmon Event Last Sent :
Rmon Event Owner : admin
```

3.23.2 Rmon alarm

Command:

```
rmon alarm <1-65535> interface IF_PORT (drop-events|octets|pkts|broadcast-pkts| multicast-
pkts|crc-align-errors|undersize-pkts|oversize-pkts|fragments|jabbers|collisions
|pkts64octets|pkts65to127octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets
|pkts1024to1518octets) <1-2147483647> (absolute|delta) rising <0-2147483647> <0-65535>
falling <0-2147483647> <0-65535> startup (rising|rising-falling|falling) [owner NAME]

no rmon alarm <1-65535>
```

Parameter:

<1-65535>	Specify alarm index to create or modify
IF_PORT	Specify the interface to sample
(drop-events|octets|pkts|broadcast-pkts| multicast-pkts|crc-align-errors|undersize-pkts|oversize-pkts|fragments|jabbers|collisions |pkts64octets|pkts65to127octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets |pkts1024to1518octets)	Specify a mib object to sample
<1-2147483647>	Specify the time in seconds that the alarm monitors the MIB variable
(absolute|delta)	Specify absolute to compare sample counter absolutely. Specify delta to compare delta counter between samples
<0-2147483647>	Specify a number which the alarm trigger rising event
<0-65535>	Specify event index when the rising threshold exceeds.

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

<0-2147483647>	Specify a number which the alarm trigger falling event
<0-65535>	Specify event index when the falling threshold exceeds.
(rising|rising-falling|falling)	Specify only to how rising or falling startup event. Or show either rising or falling startup event.
[owner NAME]	(Optional) Specify owner of alarm.

Mode:

Global Configuration

Usage Guide:

Use the **rmon event** command to add or modify a RMON event entry. Before add alarm entry, at least one event entry must be added. Use the **no** form of this command to delete.

Example:

The example shows how to add RMON alarm entry that sample interface fa1 packets delta count every 300 seconds. Trigger event index 1 if over than rising threshold 10000, trigger event index 2 if lower than falling threshold.

You can verify settings by the following **show rmon alarm** command.

```
switch(config)# rmon event 1 log
switch(config)# rmon event 2 log
switch(config)# show rmon event all
Rmon Event Index : 1
Rmon Event Type : Log
Rmon Event Community :
Rmon Event Description :
Rmon Event Last Sent :
Rmon Event Owner :
Rmon Event Index : 2
Rmon Event Type : Log
Rmon Event Community :
Rmon Event Description :
Rmon Event Last Sent :
Rmon Event Owner :
Switch(config)# rmon alarm 1 interface gi1 pkts 300 delta rising 10000 1 falling 100 1
startup rising-falling owner admin
Rmon Alarm Index : 1
Rmon Alarm Sample Interval : 300
Rmon Alarm Sample Interface : gi1
Rmon Alarm Sample Variable : Pkts
Rmon Alarm Sample Type : delta
```


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

```
Rmon Alarm Type : Rising or Falling
Rmon Alarm Rising Threshold : 10000
Rmon Alarm Rising Event : 1
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event : 1
Rmon Alarm Owner : admin
```

3.23.3 rmon history

Command:

```
rmon history <1-65535> interface IF_PORT [buckets <1-65535>] [interval <1-3600>]
[owner NAME]

no rmon history <1-65535>
```

Parameter:

<1-65535>	Specify history index to create or modify.
IF_PORT	Specify the interface to sample
[bucket <1-65535>]	(Optional) Specify the maximum number of buckets.
[interval <1-3600>]	(Optional) Specify time interval for each sample
[owner NAME]	(Optional)Specify owner of history

Mode:

Global Configuration

Usage Guide:

Use the **rmon history** command to add or modify a RMON history entry. Use the **no** form of this command to delete

Example:

The example shows how to add RMON history entry that monitor interface gi1 every 60 seconds and then modify it to monitor every 30 seconds. You can verify settings by the following **show rmon history** command.

```
switch(config)# rmon history 1 interface gi1 interval 60 owner admin
switch(config)# show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: gi1
```


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

```
Rmon History Bucket : 50
Rmon history Interval : 60
Rmon History Owner : admin
switch(config)# rmon history 1 interface gi1 interval 30 owner admin
switch(config)# show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: gi1
Rmon History Bucket : 50
Rmon history Interval : 30
Rmon History Owner : admin
```

3.23.4 clear rmon interfaces statistics

Command:

```
clear rmon interfaces IF_PORTS statistics
```

Parameter:

IF_PORTS	specifies ports to clear

Mode:

Global Configuration

Usage Guide:

Use the **clear rmon interfaces statistics** command to clear RMON etherStat statistics those are recorded on interface.

Example:

The example shows how to clear RMON etherStat statistics on interface gi1. You can verify settings by the following **show rmon interface statistics** command.

```
switch# clear rmon interfaces gi1 statistics
switch# show rmon interfaces gi1 statistics
==== Port gi1 ============================
etherStatsDropEvents : 0
etherStatsOctets : 0
etherStatsPkts : 0
etherStatsBroadcastPkts : 0
etherStatsMulticastPkts : 0
```


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

```
etherStatsCRCAlignErrors : 0
etherStatsUnderSizePkts : 0
etherStatsOverSizePkts : 0
etherStatsFragments : 0
etherStatsJabbers : 0
etherStatsCollisions : 0
etherStatsPkts64Octets : 0
etherStatsPkts65to127Octets : 0
etherStatsPkts128to255Octets : 0
etherStatsPkts256to511Octets : 0
etherStatsPkts512to1023Octets : 0
etherStatsPkts1024to1518Octets : 0
```

3.23.5 show rmon event

Command:

```
show rmon event (<1-65535> | all)
```

Parameter:

<1-65535>	specifies event index to show
all	Show all existed event

Mode:

Global Configuration

Usage Guide:

Use the **show rmon event** command to show existed RMON event entry.

Example:

The example shows how to show rmon event entry.

```
switch(config)# rmon event 1 log trap public description test owner admin
switch(config)# show rmon event 1
Rmon Event Index : 1
Rmon Event Type : Log and Trap
Rmon Event Community : public
Rmon Event Description : test
```


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

```
Rmon Event Last Sent :
Rmon Event Owner : admin
```

3.23.6 show rmon event log

Command:

```
show rmon event <1-65535> log
```

Parameter:

<1-65535>	specifies event index to show event log

Mode:

Global Configuration

Usage Guide:

Use the **show rmon event log** command to show log triggered by RMON alarm.

Example:

The example shows how to show rmon event log.

```
switch(config)# show rmon event 1 log
=====================================================
Index : 1
Alarm Index : 1
Action : Startup Falling
Time : (32918334) 3 days, 19:26:23.34
Description : gi1.Pkts=0 <= 100
```


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

3.23.7 show rmon alarm

Command:

```
show rmon alarm (<1-65535> | all)
```

Parameter:

<1-65535>	specifies alarm index to show
all	Show all existed alarm

Mode:

Global Configuration

Usage Guide:

Use the **show rmon alarm** command to show existed RMON alarm entry.

Example:

The example shows how to show rmon alarm entry.

```
Switch(config)# rmon alarm 1 interface gi1 pkts 300 delta rising 10000 1 falling 100 1
startup rising-falling owner admin
Rmon Alarm Index : 1
Rmon Alarm Sample Interval : 300
Rmon Alarm Sample Interface : gi1
Rmon Alarm Sample Variable : Pkts
Rmon Alarm Sample Type : delta
Rmon Alarm Type : Rising or Falling
Rmon Alarm Rising Threshold : 10000
Rmon Alarm Rising Event : 1
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event : 1
Rmon Alarm Owner : admin
```

3.23.8 show rmon history

Command:

```
show rmon history (<1-65535> | all)
```

Parameter:

<1-65535>	specifies history index to show
all	Show all existed history

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

Mode:

Global Configuration

Usage Guide:

Use the **show rmon history** command to show existed RMON history entry

Example:

The example shows how to show RMON history entry.

```
switch(config)# rmon history 1 interface gi1 interval 30 owner admin
switch(config)# show rmon history 1
Rmon History Index : 1
Rmon Collection Interface: gi1
Rmon History Bucket : 50
Rmon history Interval : 30
Rmon History Owner : admin
```

3.23.9 show rmon history statistics

Command:

```
show rmon history <1-65535> statistic
```

Parameter:

<1-65535>	specifies history index to show history statistic

Mode:

Global Configuration

Usage Guide:

Use the **show rmon history statistic** command to show statistics that are recorded by RMON history..

Example:

The example shows how to show RMON history statistics

```
switch(config)# show rmon history 1 statistics
=========================================================
Sample Index : 2
Interval Start : (32940466) 3 days, 19:30:04.66
DropEvents : 0
Octets : 117226
```


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

```
Pkts : 763
BroadcastPkts : 9
MulticastPkts : 0
CRCAlignErrors : 0
UnderSizePkts : 0
OverSizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 1
=====================================================
Sample Index : 1
Interval Start : (32939462) 3 days, 19:29:54.62
DropEvents : 0
Octets : 220
Pkts : 3
BroadcastPkts : 1
MulticastPkts : 0
CRCAlignErrors : 0
UnderSizePkts : 0
OverSizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 0
```


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

3.24 SNMP

3.24.1 snmp

Command:

```
snmp

no snmp
```

Mode:

Global Configuration

Usage Guide:

'no snmp' will disable snmp.

'snmp' will enable snmp.

The configure can use show snmp

Example:

The following example specifies that set global snmp test

```
Switch(config)# snmp
Switch# show snmp
SNMP is enabled
```

3.24.2 snmp trap

Command:

```
[no] snmp trap (auth|linkUpDown|warm-start|cold-start|port-security)
```

Default:

snmp trap auth

snmp trap linkUpDown

snmp trap warm-start

snmp trap cold-start

snmp trap port-security

Mode:

Global Configuration

Usage Guide:

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

'no snmp trap auth' snmp will not send auth failure trap.

'no snmp trap linkUpDown' snmp will not send linkup and link down trap.

'no snmp trap warm-start snmp will not send warm start trap.

'no snmp trap cold-start' snmp will not send cold start trap.

'no snmp trap port-security' snmp will not send port-security trap.

The configure can use show snmp trap.

Example:

The following example specifies that set trap auth disable test.

```
Switch(config)#no snmp auth
Switch# show snmp trap
SNMP auth failed trap : Disable
SNMP linkUpDown trap : Enable
SNMP warm-start trap : Enable
SNMP cold-start trap : Enable
SNMP port security trap: Enable
```

3.24.3 snmp view

Command:

```
snmp view NAME subtree OID oid-mask (all | MASK) viewtype (included | excluded)

no snmp view NAME subtree (all |OID)
```

Parameter:

NAME	View Name
OID	View subtree OID
(all | MASK)	View subtree OID mask. All: all mask bit is '1'
(included | excluded)	View subtree is accessed or not allowed accesse
(all |OID)	Delete the View name all subtree OID or specifies OID

Default:

Default View is "all" and subtree is .1 the type is include.

Mode:

Global Configuration

Usage Guide:

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

The default view can't delete and create by user

The min view is sysUpTime.

The exclude view must in range of include view.otherwise, it is not invalid.

The configure use 'show snmp view' to check

Example:

The following example specifies that set view systemView test.

```
Switch(config)# snmp view systemView subtree 1.3.6.1.2.1.1 oid-mask all viewtype
included
Switch# show snmp view
View Name Subtree OID OID Mask View Type
--------------- -------------- ----------------- ----------------------
all .1 all included
systemView .1.3.6.1.2.1.1 all included
```

3.24.4 snmp access group

Command:

```
snmp group NAME version (1 |2c |3) (noauth | auth | priv) read-view NAME write-
view NAME [notify-view NAME]

no snmp group NAME security-mode version (1 |2c | 3)
```

Parameter:

NAME	Access group name
(1 |2c |3)	Access model for snmp v1/v2c/v3
(noauth | auth |	Noauth for snmp v1/v2c/v3
priv)	Auth and priv group for snmp v3
read-view NAME	Access group specifies read view
write-view NAME	Access group specifies write view
notify-view NAME	Access group specifies notify view

Mode:

Global Configuration

Usage Guide:

The group version 1 and 2c only for snmp community use. And version 3 group only for snmp user use.

When group version is 1 or 2c , can only use noauth

The read/write/notify view must exist.

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

The configure use 'show snmp group' to check

Example:

The following example specifies that set snmp group test.

```
Switch(config)#snmp group group1 version 1 noauth read-view all write-viw ""
Switch(config)#snmp group group2 version 2c noauth read-view all write-view all
Switch(config)# snmp group group3 version 3 auth read-view all write-view all
Switch# show snmp group
Group Name Model Level ReadView WriteView NotifyView
----------------------- ------ ------ ------------- -------------- -------------
group1 v1 noauth all --- ---
group2 v2c noauth all all ---
group3 v3 auth all all ---
```

3.24.5 snmp community

Command:

```
snmp community NAME [view NAME] (ro|rw)

snmp community NAME group NAME

no snmp community NAME
```

Parameter:

community NAME	Snmp v1/v2 community name
group NAME	Snmp community specifies access group name for advance mode
[view NAME]	Snmp community specifies view for basic mode
(ro|rw)	Snmp community read or readwrite attribute for basic mode

Mode:

Global Configuration

Usage Guide:

The community support basic & advace mode.

Basic: community assigned view and read/write right.

Advace: community assigned access group.

The community specifies the group witch must exist.

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

The community specifies the view witch must exist. It will generate the no exist v1 or v2 access group for community.

The configure can use 'show snmp community' to check

Example:

The following example specifies that configure community test.

```
Switch(config)# snmp communit public rw
Switch(config)# snmp communit test1 view all ro
Switch(config)# snmp group group2 version 2c noauth read-view all write-view ""
Switch(config)# snmp community test2 group group2
Switch# show snmp comunity
Commnunity Name Group Name View
Access
-------------------- ------------------------------ ------------------------------ ------------
public all rw
test2 group2
test1 all ro
```

3.24.6 snmp user

Command:

```
snmp user USERNAME GROUPNAME [auth (md5|sha) AUTHPASSWD]

snmp user USERNAME GROUPNAME auth (md5|sha) AUTHPASSWD priv
PRIVPASSWD

no snmp user NAME
```

Parameter:

USERNAME	Snmp user name
GROUPNAME	Snmp user specifies group
[auth (md5|sha)]	Snmp user auth protocol
AUTHPASSWD	Snmp user auth password
PRIVPASSWD	Snmp user priv password

Mode:

Global Configuration

Usage Guide:

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

The group version must be v3 , and the security level must match the snmp user configure.

AUTHPASSWD and PRIVPASSWD min length is 8.max length is 32 and 64

The configure can use 'show snmp user' to check

Example:

The following example specifies that set auth snmp user test.

```
Switch(config)# snmp group group3 version 3 auth read-view all write-view all
Switch(config)# snmp user user1 group3 auth md5 12345678
Switch# show snmp user
Username: user1
Password: ********
Privilege Mode: rw
Access GroupName: group3
Authentication Protocol: md5
Encryption Protocol: none
Access SecLevel: auth
```

3.24.7 snmp engineID

Command:

```
snmp engineid (default | ENGINEID)

snmp engineid remote (A.B.C.D|X:X::X:X) ENGINEID

no snmp engineid remote (A.B.C.D|X:X::X:X)
```

Parameter:

(default |	Default is MAC address.
ENGINEID)	ENGINEID is 10~64 hex characters
(A.B.C.D|X:X::X:X)	Host ipv4/ipv6 address

Mode:

Global Configuration

Usage Guide:

Default engineid is DUT MAC address.

The configure can use 'show snmp engineid'

Example:

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

The following example specifies that set remote engine id test.

```
Switch(config)# snmp engineid remote 192.168.1.100 112233445566
Switch# show snmp engineid
Local SNMPV3 Engine id: DEADBEEF0114
IP address Remote SNMP engineID
------------------- ---------------------------------------------
192.168.1.100 112233445566
```

3.24.8 snmp host

Command:

```
snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] [version (1|2c)] NAME
[udp-port <1-65535>] [timeout <1-300>] [retries <1-255>]

snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] version 3 [(auth |
noauth | priv)] NAME [udp-port <1-65535>] [timeout <1-300>] [retries <1-255>]

no snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [(traps | informs)] [version (1|2c|3)]
```

Parameter:

(A.B.C.D|X:X::X:X|HOSTNAME)	Snmp trap host ipv4/ipv6 address or host name
[(traps | informs)]	Snmp notification type is traps or informs
[version (1|2c|3)]	V1/v2c/v3 traps
[(auth | noauth | priv)]	V3 trap for auth/noauth/priv
NAME	Snmp community name or user name
[udp-port <1-65535>]	The manage receive trap udp port num
[timeout <1-300>]	The notify type is inform timeout value
[retries <1-255>]	The notify type is inform retries

Mode:

Global Configuration

Usage Guide:

This command can’t configure version 1 inform

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

When use traps, this command can't configure udp-port and retries.

The host use NAME witch is snmp community or user NAME must exist.

The host use host security level must match the snmp user security level

The configure can use 'show snmp host' to check

Example:

The following example specifies that snmp community configure test.

```
Switch(config)# snmp community public ro
Switch(config)# snmp community private rw
Switch(config)# snmp group group3 version 3 auth read-view all write-view all
Switch(config)# snmp user user1 group3 auth md5 12345678
Switch(config)# snmp host 192.168.1.100 version 2c public
Switch(config)# snmp host 192.168.1.100 informs version 2c private
Switch(config)# snmp host 192.168.1.100 version 3 auth user1
Switch# show snmp host
Server Community Name Notification Version Notification Type UDP Port Retries Timeout
-----------------------------------------------------------------------------------------------------------
192.168.1.100 public v2c trap 162 -- --
192.168.1.100 private v2c inform 200 3 10
192.168.1.100 user1 v3 trap 162 -- --
```

3.24.9 show snmp

Command:

```
show snmp
```

Mode:

privileged mode

Usage Guide:

This command will snmp status.

Example:

The following example specifies that show snmp test

```
Switch# show snmp
```


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

3.24.10 show snmp trap

Command:

```
show snmp trap
```

Mode:

privileged mode

Usage Guide:

This command will display snmp trap class auth/linkupdown/cold-start/warm-start/port-security/. Status.

Example:

The following example specifies that display snmp trap test

```
Switch# show snmp trap
```

3.24.11 show snmp view

Command:

```
show snmp view
```

Mode:

privileged mode

Usage Guide:

This command will display the snmp view entry.

Example:

The following example specifies that display snmp view test.

```
Switch# show snmp view
```

3.24.12 show snmp group

Command:

```
show snmp group
```


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

Mode:

privileged mode

Usage Guide:

This command will display the snmp group

Example:

The following example specifies that display snmp group test.

```
Switch# show snmp group
```

3.24.13 show snmp community

Command:

```
show snmp community
```

Mode:

privileged mode

Usage Guide:

This command will display the snmp community entry.

Example:

The following example specifies that display snmp community test

```
Switch# show snmp community
```

3.24.14 show snmp host

Command:

```
show snmp host
```

Mode:

privileged mode

Usage Guide:

This command will display the snmp host entry.

Example:

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

The following example specifies that display snmp host test.

```
Switch# show snmp host
```

3.24.15 show snmp user

Command:

```
show snmp user
```

Mode:

privileged mode

Usage Guide:

This command will display the snmp user entry.

Example:

The following example specifies that display snmp user test.

```
Switch# show snmp user
```

3.24.16 show snmp engineid

Command:

```
show snmp engineid
```

Mode:

privileged mode

Usage Guide:

This command will display the snmp local/remote engine id

Example:

The following example specifies that display snmp local/remote engine id test.

```
Switch# show snmp engineid
```


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

3.25 Storm Control

3.25.1 Storm-control unit

Command:

```
storm-control unit (bps | pps)
```

Parameter:

bps	Storm control rate calculates by octet-based
pps	Storm control rate calculates by packet-based

Default:

Default storm control unit is bps.

Mode:

Global Configuration

Usage Guide:

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. This command allows you to change the unit of calculating method

Example:

This example shows how to configure storm control rate unit as pps.

```
Switch(config)# storm-control unit pps
```

This example shows how to show storm control global configuration

```
Switch# show storm-control
Storm control preamble and IFG: Excluded
Storm control unit: pps
.....
```


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

3.25.2 storm-control ifg

Command:

```
storm-control ifg (include | exclude)
```

Parameter:

include	Include preamble & IFG (20 bytes) when count ingress storm control rate.
exclude	Exclude preamble & IFG (20 bytes) when count ingress storm control rate

Default:

Default storm control inter frame gap is excluded.

Mode:

Global Configuration

Usage Guide:

Storm control mechanism will try to calculate ingress packets is exceed configured rate or not and do corresponding action. This command allows you to decide to include/exclude the preamble and inter frame gap into the calculating or not.

Example:

This example shows how to configure storm control rate unit as pps.

```
Switch(config)# storm-control ifg include
```

This example shows how to show storm control global configuration.

```
Switch# show storm-control
Storm control preamble and IFG: Included
Storm control unit: pps
.........................................
```

3.25.3 storm-control

Command:

```
storm-control

no storm-control

storm-control (broadcast | unknown-unicast | unknown-multicast)
```


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

```
no storm-control (broadcast | unknown-unicast | unknown-multicast)

storm-control (broadcast | unknown-unicast | unknown-multicast) level <0-1000000>

no storm-control (broadcast | unknown-unicast | unknown-multicast) level
```

Parameter:

broadcast	Select broadcast storm control type
unknown-unicast	Select unknown unicast storm control type
unknown-multicast	Select unknown multicast storm control type
level *<0-1000000>*	Specify the storm control rate for selected type

Default:

Default broadcast storm control is disabled.

Default unknown multicast storm control is disabled

Default unknown unicast storm control is disabled

Default broadcast storm control rate is 10000.

Default unknown multicast storm control rate is 10000.

Default unknown unicast storm control rate is 10000.

Mode:

Interface Configuration

Usage Guide:

Storm control function is able to enable/disable on each single port. Use the "**storm control**" command to enable storm control feature on the selected ports. And use "**no storm control**" command to disable storm control feature. Not only port is able to enable/disable on the port. Each storm control type is also able to enable/disable on each single port. Use the "**storm-control (broadcast | unknown-unicast | unknown-multicast)**" command to enable the storm control type you need and use no form to disable it.

Each control type is allowed to have different storm control rate. Use "**storm-control (broadcast | unknown-unicast | unknown-multicast) level**" command to configure it and use no form to restore to default value.

Example:

This example shows how to enable storm control on interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control
```

This example shows how to enable broadcast storm control and configure broadcast storm control rate to 200.

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

```
Switch(config)# interface gi1
Switch(config-if)# storm-control broadcast
Switch(config-if)# storm-control broadcast level 200
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1
Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action
| | pps | pps | pps |
---------+-------+------------+--------------------+-----------------|-----------
gi1 enable 200 Off( 10000) Off( 10000) Shutdown
```

3.25.4 storm-control action

Command:

```
storm-control action (drop | shutdown)

no storm-control action
```

Parameter:

(drop | shutdown) Storm-control action for drop|flood|router-port

Default:

Default storm control action is drop.

Mode:

Interface Configuration

Usage Guide:

The storm control mechanism allows you to drop packets which exceed storm control rate or just shutdown port.

Use no form to restore to default action.

Example:

This example shows how to configure storm control action to shutdown port on interface gi1.

```
Switch(config)# interface gi1
Switch(config-if)# storm-control action shutdown
```

This example shows how to show storm control action on interface gi1.

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

```
Switch# show storm-control interfaces gi1
Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action
| | pps | pps | pps |
---------+-------+------------+--------------------+-----------------|-----------
gi1 disable Off( 10000) Off( 10000) Off( 10000) Shutdown
```

3.25.5 show storm-control

Command:

```
show storm-control

show storm-control interface IF_PORTS
```

Parameter:

IF_PORTS	Specify port to show.

Mode:

Privileged EXEC

Usage Guide:

Use "**show storm-control**" command to show all storm control related configurations including global configuration and per port configurations.

Use "**show storm-control interface**" command to show selected port storm control configurations.

Example:

This example shows how to show storm control global configuration.

```
Switch# show storm-control
Storm control preamble and IFG: Excluded
Storm control unit: pps
.........................................
```

This example shows how to show current storm control configuration on interface gi1

```
Switch# show storm-control interfaces gi1
Port | State | Broadcast | Unkown-Multicast | Unknown-Unicast | Action
| | pps | pps | pps |
---------+-------+------------+--------------------+-----------------|-----------
fa1 enable 200 Off( 10000) Off( 10000) Shutdown
```


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

3.26 Spanning Tree

3.26.1 spanning-tree

Command:

```
spanning-tree

no spanning-tree
```

Mode:

Global Configuration

Usage Guide:

Enable or Disable Spanning-Tree Protocol. Using `spanning-tree` command to enable STP or `no spanning-tree` command to disable STP

Example:

The following example sets the STP status to enable and disable.

```
Switch# configure
Switch(config)# spanning-tree
Switch(config)# exit
Switch# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 32768
Address 00:03:4F:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 1 last change occurred 01:49:43 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role EdgePort Type
--------- -------- -------- -------- ------ ---- -------- ------------------
gi1 enabled 128.1 20000 Frw Desg No P2P
(RSTP)
Switch#
```


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

3.26.2 spanning-tree bpdu

Command:

```
spanning-tree bpdu ( filtering | flooding )
```

Parameter:

(filtering | flooding)	Specify the forwarding action of BPDU to filtering or flooding.

Default:

spanning-tree bpdu flooding

Mode:

Global Configuration

Usage Guide:

Configure the BPDU forwarding action when STP is disabled.

Example:

This example sets the BPDU forwarding action to filtering.

```
Switch# configure
Switch(config)# no spanning-tree
Switch(config)# spanning-tree bpdu filtering
Switch(config)# exit
Switch# show spanning-tree
Spanning tree disabled (BPDU filtering) mode RSTP
Default port cost method: long
Switch#
```

3.26.3 spanning-tree mode

Command:

```
spanning-tree mode ( stp | rstp | mstp )
```

Parameter:

stp	Specify the mode to Spanning Tree Protocol
rstp	Specify the mode to Rapid Spanning Tree Protocol
mstp	Specify the mode to Multiple Spanning Tree Protocol.

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

Default:

spanning-tree mode stp

Mode:

Global Configuration

Usage Guide:

Configure the force-version of Spanning-Tree Protocol. The configuration could be shown by “show spanning-tree” command.

Example:

This example sets STP mode to STP (Classic Spanning Tree Protocol).

```
Switch# configure
Switch(config)# spanning-tree mode stp
Switch(config)# exit
Switch# show spanning-tree
Spanning tree enabled mode STP
Default port cost method: long
Root ID Priority 32768
Address 00:30:4F:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 1 last change occurred 00:05:13 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role EdgePort Type
--------- -------- -------- -------- ------ ---- -------- ------------------
gi1 enabled 128.1 200000 Dscd Desg No P2P (STP)
Switch#
```

3.26.4 spanning-tree priority

Command:

```
spanning-tree priority <0-61440>
```

Parameter:

<0-61440>	Specify the bridge priority, it must multiples of 4096

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

Default:

spanning-tree priority 32768

Mode:

Global Configuration

Usage Guide:

This command configures the bridge priority. The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the bridge priority to 16384.

```
Switch# configure
Switch(config)# spanning-tree priority 16384
Switch(config)# exit
Switch# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 16384
Address 00:30:4F:28:55:00
This switch is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 00:03:37 ago
Times: hold 0, topology change 0, notification 0
hello 2, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role EdgePort Type
--------- -------- -------- -------- ------ ---- -------- ------------------
gi1 enabled 128.1 20000 Frw Desg No P2P (RSTP)
Switch#
```

3.26.5 spanning-tree hello-time

Command:

```
spanning-tree hello-time <1-10>
```

Parameter:

<1-10>	Specify the hello-time interval (second).

Default:

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

spanning-tree hello-time = 2

Mode:

Global Configuration

Usage Guide:

This command configures the BPDU hello-time interval (second). The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the BPDU hello-time to 5 sec.

```
Switch# configure
Switch(config)# spanning-tree hello-time 5
Switch(config)# exit
Switch# show spanning-tree
Spanning tree enabled mode RSTP
Default port cost method: long
Root ID Priority 16384
Address 00:30:4F:28:55:00
This switch is the root
Hello Time 5 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 2 last change occurred 00:00:01 ago
Times: hold 0, topology change 0, notification 0
hello 5, max age 20, forward delay 15
Interfaces
Name State Prio.Nbr Cost Sts Role EdgePort Type
--------- -------- -------- -------- ------ ---- -------- ------------------
gi1 enabled 128.1 20000 Frw Desg No P2P (RSTP)
Switch#
```

3.26.6 spanning-tree max-hops

Command:

```
spanning-tree max-hops <1-40>
```

Parameter:

<1-40>	Specify the max-hops value

Default:

spanning-tree max-hops = 20

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

Mode:

Global Configuration

Usage Guide:

This command configures the maximum hops value for MSTP. The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the max-hops to 15.

```
Switch# configure
Switch(config)# spanning-tree max-hops 15
```

3.26.7 spanning-tree forward-delay

Command:

```
spanning-tree forward-delay <4-30>
```

Parameter:

<4-30>	Specify the forward-delay interval (second).

Default:

spanning-tree forward-delay = 15

Mode:

Global Configuration

Usage Guide:

This command configures the BPDU forward-delay interval (second). The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the BPDU forward-delay to 30 sec.

```
Switch# configure
Switch(config)# spanning-tree forward-delay 30
```

3.26.8 spanning-tree maximum-age

Command:

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

```
spanning-tree maximum-age <6-40>
```

Parameter:

<6-40>	Specify the maximum-age time (second).

Default:

spanning-tree maximum-age = 20

Mode:

Global Configuration

Usage Guide:

This command configures the BPDU maximum-age interval (second). The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the BPDU maximum-age to 10 sec.

```
Switch# configure
Switch(config)# spanning-tree maximum-age 10
```

3.26.9 spanning-tree tx-hold-count

Command:

```
spanning-tree tx-hold-count <1-10>
```

Parameter:

<1-10>	Specify the tx-hold-count value.

Default:

spanning-tree tx-hold-count = 6

Mode:

Global Configuration

Usage Guide:

This command configures the BPDU tx-hold-count.

Example:

This example sets the BPDU tx hold count to 10

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

```
Switch# configure
Switch(config)# spanning-tree tx-hold-count 10
```

3.26.10 spanning-tree pathcost method

Command:

```
spanning-tree pathcost method ( long | short )
```

Parameter:

long	Specify the type of pathcost value to 32 bits (long).
short	Specify the type of pathcost value to 16 bits (short).

Default:

spanning-tree pathcost method = long

Mode:

Global Configuration

Usage Guide:

This command configures the BPDU pathcost value type to 16bits (short) or 32 bits (long). The configuration could be shown by “show spanning-tree” command.

Example:

This example sets the type of pathcost value to short.

```
Switch# configure
Switch(config)# spanning-tree pathcost method short
```

3.26.11 spanning-tree port-priority

Command:

```
spanning-tree port-priority <0-240>
```

Parameter:

<0-240>	Specify the STP port priority. It must multiples of 16.

Default:

spanning-tree port-priority = 128

Mode:

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

Port Configuration

Usage Guide:

This command per port configures the STP port priority. The configuration could be shown by “show spanning-tree interface” command.

Example:

This example sets port gi1 STP port priority to 64.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree port-priority 64
```

3.26.12 spanning-tree cost

Command:

```
spanning-tree cost <0-200000000>
```

Parameter:

<0-200000000>	Specify the STP port cost. In short pathcost method, the range is from 0 to 65535. (0 = Auto)

Default:

spanning-tree cost = 0

Mode:

Port Configuration

Usage Guide:

This command per port configures the STP port cost. The configuration could be shown by “show spanning-tree interface” command.

Example:

This example sets port gi1 STP port cost to 100.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree cost 100
```

3.26.13 spanning-tree edge

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

Command:

```
spanning-tree edge

no spanning-tree edge
```

Mode:

Port Configuration

Usage Guide:

This command per port configures the STP edge port function. The configuration could be shown by “show spanning-tree interface” command.

Example:

This example sets port gi1 STP edge port to enable.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree edge
```

3.26.14 spanning-tree bpdu-filter

Command:

```
spanning-tree bpdu-filter

no spanning-tree bpdu-filter
```

Mode:

Port Configuration

Usage Guide:

This command per port configures the STP BPDU Filter status. The configuration could be shown by “show spanning-tree interface” command.

Example:

This example sets port gi1 STP BPDU Filter status to enable.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree bpdu-filter
```


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

3.26.15 spanning-tree bpdu-guard

Command:

```
spanning-tree bpdu-guard

no spanning-tree bpdu-guard
```

Mode:

Port Configuration

Usage Guide:

This command per port configures the STP BPDU Guard status. The configuration could be shown by “show spanning-tree interface” command.

Example:

This example sets port gi1 STP BPDU Guard status to enable.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree bpdu-guard
```

3.26.16 spanning-tree link-type

Command:

```
spanning-tree link-type ( point-to-point | shared )

no spanning-tree link-type
```

Parameter:

(point-to-point | shared)	Specify the STP port link-type to Point-to-Point or Shared medium.

Mode:

Port Configuration

Usage Guide:

This command per port configures the STP port link-type. The configuration could be shown by “show spanning-tree interface” command.

Example:

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

This example sets port gi1 STP port link-type to be Shared.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree link-type shared
```

3.26.17 spanning-tree mst configuration

Command:

```
spanning-tree mst configuration

    name NAME

    revision <0-65535>

instance <0-15> vlan [ VLAN-LIST ]
```

Parameter:

NAME	Specify the MSTP bridge name of MST Configuration ID. (Max. 32 chars)
<0-65535>	Specify the MSTP revision number of MST Configuration ID.
<0-15>	Specify the MST instance ID.
VLAN-LIST	Specify the VLAN list to be mapped to this specified instance.

Default:

name (Switch's MAC address)

revision 0

instance 0 vlan all

Mode:

Global Configuration

Usage Guide:

This command configures the MSTP Configuration ID. The configuration could be shown by "show spanning-tree mst configuration" command.

Example:

This example sets MSTP Configuration ID, name to `Region1`, revision to `123` and VLAN 100 mapped to instance 1.

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

```
Switch# configure
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Region1
Switch(config-mst)# revision 123
Switch(config-mst)# instance 1 vlan 100
Switch(config-mst)# exit
Switch(config)# exit
Switch# show spanning-tree mst configuration
Name [Region1]
Revision 123 Instances configured 2
Instance Vlans mapped
-------- ---------------------------------------------------------------------
0 1-99,101-4094
1 100
---------------------------------------------------------------------------
```

3.26.18 spanning-tree mst priority

Command:

```
spanning-tree mst <0-15> priority <0-61440>
```

Parameter:

<0-15>	Specify the MST instance ID to configure.
<0-61440>	Specify the bridge priority, it must multiples of 4096.

Default:

spanning-tree mst = 0 ; priority = 32768

Mode:

Global Configuration

Usage Guide:

This command configures the MST instance priority. The configuration could be shown by “show spanning-tree mst” command.

Example:

This example sets the priority of MST instance 1 to 4096.

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

```
Switch# configure
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst 1 priority 4096
```

3.26.19 spanning-tree mst cost

Command:

```
spanning-tree mst <0-15> cost <0-200000000>
```

Parameter:

<0-15>	Specify the MST instance ID to configure.
<0-200000000>	Specify the STP port cost. In short pathcost method, the range is from 0 to 65535. (0 = Auto)

Default:

spanning-tree mst = 0 ; cost = 0

Mode:

Port Configuration

Usage Guide:

This command configures the MSTP port cost for this MST instance. The configuration could be shown by “show spanning-tree mst interface” command.

Example:

This example sets port gi1 STP pathcost of MST instance 1 to 100.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree mst 1 cost 100
```

3.26.20 spanning-tree mst port-priority

Command:

```
spanning-tree mst <0-15> priority <0-240>
```

Parameter:

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

<0-15>	Specify the MST instance ID to configure.
<0-240>	Specify the STP port priority. It must multiples of 16.

Default:

spanning-tree mst = 0; port-priority = 128

Mode:

Port Configuration

Usage Guide:

This command configures the MST port priority. The configuration could be shown by “show spanning-tree mst interface” command.

Example:

This example sets port gi1 MST port priority of MST instance 0 to 32.

```
Switch# configure
Switch(config)# interface gi1
Switch(config-if)# spanning-tree mst 1 cost 0
Switch(config-if)# exit
Switch(config)# interface gi1
Switch(config-if)# spanning-tree mst 1 port-priority 32
```


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

3.27 System File

3.27.1 boot system

Command:

```
boot system (image0 | image1)
```

Parameter:

image0	Boot from flash image partition 0
image1	Boot from flash image partition 1

Default:

Default boot image is image0.

Mode:

Global Configuration

Usage Guide:

Dual image allow user to have a backup image in the flash partition. Use “**boot system**” command to select the active firmware image. And another firmware image will become a backup one.

Example:

This example shows how to select image1 as active image.

```
Switch(config)# boot system image1
Select "image1" Success
This example shows how to show active image partition.
Switch# show flash
File Name File Size Modified
------------------------ ---------------- ------------------------
startup-config 1191 2000-01-01 00:00:23
rsa1 974 2000-01-01 00:00:18
rsa2 1675 2000-01-01 00:00:18
dsa2 668 2000-01-01 00:00:18
ssl_cert 993 2000-01-01 00:00:18
image0 (backup) 4372401 2012-09-24 01:57:29
image1 (active) 5555970 2012-06-12 12:17:46
```


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

3.27.2 save

Command:

```
save
```

Mode:

Privileged EXEC

Usage Guide:

Use "**save**" command to save running configuration to startup configuration file. This command is equal to "**copy running-config startup-config**".

Example:

This example shows how to save running configuration to startup configuration.

```
Switch# save
Success
```

3.27.3 copy

Command:

```
copy (flash:// | tftp://) (flash:// | tftp://)

copy tftp:// (backup-config | running-config | startup-config)

copy (backup-config | running-config | startup-config) tftp://

copy (backup-config | startup-config) running-config

copy (backup-config | running-config) startup-config

copy (running-config | startup-config) backup-config
```

Parameter:

flash://	Specify the file stored in flash to operation. Available files are: flash://startup-config flash://backup-config

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

	flash://image0
	flash://image1
	flash://ram.log
	flash://flash.log
tftp://	Specify remote tftp server and remote file name. The format is "tftp://192.168.1.111/remote_file_name"
running-config	Running configuration file
startup-config	Startup configuration file
backup-config	Edit default authentication list

Mode:

Privileged EXEC

Usage Guide:

There are many types of files in system. These files are very important for administrator to manage the switch. The most common file operation is copy. By using these copy commands, we can upgrade, backup following type of files.

- Firmware Image
- Configuration Files
- Syslog Files

Example:

This example shows how to copy running configuration to startup configuration.

```
Switch# copy running-config startupst-config
```

This example shows how to backup running configuration to remote tftp server 192.168.111 with file name test1.cfg.

```
Switch# copy running-config tftp://192.168.1.111/test1.cfg
Uploading file...Please Wait...
Uploading Done
```

This example shows how to upgrade startup configuration from remote tftp server 192.168.1.111 with file name test2.cfg.

```
Switch# copy tftp://192.168.1.111/test2.cfg startup-config
Downloading file...Please Wait...
Downloading Done
Upgrade config success. Do you want to reboot now? (y/n)n
```

This example shows how to backup security file dsa2 to remote tftp server 192.168.1.111 with file name dsa2.

```
Switch# copy flash://dsa2 tftp://192.168.1.111/dsa2
Uploading file...Please Wait...
Uploading Done
```


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

3.27.4 delete

Command:

```
delete (startrup-config | backup-config | flash://)

delete system (image0 | image1)
```

Parameter:

flash://	Specify the configuration file stored in flash to delete. Available files are: flash://startup-config flash://backup-config
startup-config	Delete startup configuration file
backup-config	Delete backup configuration file
image0	Delete flash image0.
Image1	Delete flash image1.

Mode:

Privileged EXEC

Usage Guide:

Use "**delete**" command to delete configuration files or use "**delete system**" command to delete firmware image stored in flash.

The "**delete startup-config**" command is using to restore factory default and it is equal to command "**restore-defaults**".

Example:

This example shows how to delete backup configuration file.

```
Switch# delete backup-config
```

This example shows how to delete backup firmware image from flash.

```
Switch# delete system image1
```


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

3.27.5 restore-default

Command:

```
restore-default
```

Mode:

Privileged EXEC

Usage Guide:

Use "**restore-defaults**" command to restore factory default of all system. The command is equal to "**delete startup-config**"

Example:

This example shows how to restore factory defaults.

```
Switch# restore-defaults
Restore Default Success. Do you want to reboot now? (y/n)n
```

3.27.6 show config

Command:

```
show (running-config | startrup-config | backup-config)
```

Parameter:

running-config	Show running configuration on terminal
startrup-config	Show startup configuration on terminal
backup-config	Show backup configuration on terminal

Mode:

Privileged EXEC

Usage Guide:

Our configuration file is text based. Therefore, we can show the configuration on terminal and read it by this command.

Example:

This example shows how to show running configuration

```
Switch# show running-config
! System Description: Switch
! System Version: v2.5.0-beta.32811
! System Name: SwitchEF0102
```


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

```
! System Up Time: 0 days, 5 hours, 23 mins, 42 secs
!
!
!
!
username "" privilege user secret "dnXencJRwflV6"
username "admin" secret "FzjrGO6vfbERY"
voice-vlan vpt 0
voice-vlan dscp 0
.....................................................
```

3.27.7 show flash

Command:

```
show flash
```

Mode:

Privileged EXEC

Usage Guide:

Use "**show flash**" command to show all files' status which stored in flash.

Example:

This example shows how to show all files status stored in flash.

```
Switch# show flash
File Name File Size Modified
------------------------ ---------------- ------------------------
startup-config 1191 2000-01-01 00:00:23
image0 (active) 4372401 2012-09-24 01:57:29
image1 (backup) 0
```


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

3.28 Time

3.28.1 clock set

Command:

```
clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31>
<2000-2035>
```

Parameter:

HH:MM:SS	Specify static time of year, month, day, hour, minute, second
(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2035>	

Mode:

Global Configuration

Usage Guide:

Use the **clock set** command to set static time. The static time won't save to configuration file.

Example:

The example shows how to set static time of switch. You can verify settings by the following show **show clock** command.

```
switch# clock set 11:03:00 sep 21 2012
11:03:00 DFL(UTC+8) Sep 21 2012
switch# show clock
11:03:21 DFL(UTC+8) Sep 21 2012
No time source
```

3.28.2 clock timezone

Command:

```
clock timezone ACRONYM HOUR-OFFSET [minutes <0-59>]

no clock timezone
```

Parameter:

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

ACRONYM	Specify acronym name of time zone
HOUR-OFFSET	Specify hour offset of time zone
minutes <0-59>	Specify minute offset of time zone

Default:

Default time zone is UTC+8.

Mode:

Global Configuration

Usage Guide:

Use the **clock timezone** command to set timezone setting. Use the no form of this command to default setting.

Example:

The example shows how to set time zone of switch and then restore to default time zone. You can verify settings by the following show show clock command.

```
switch(config)# clock timezone test +5
switch(config)# show clock detail
10:13:27 test(UTC+5) Sep 21 2012
No time source
Time zone:
Acronym is test
Offset is UTC+5
switch(config)# no clock timezone
switch(config)# show clock detail
13:14:50 DFL(UTC+8) Sep 21 2012
No time source
Time zone:
Acronym is DFL
Offset is UTC+8
```

3.28.3 clock source

Command:

```
clock source (local|sntp)
```

Parameter:

local	Specify to use static time
sntp	Specify to use sntp time

Default:

Default is using local time.

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

Mode:

Global Configuration

Usage Guide:

Use the **clock source** command to set the source of time. The "**local**" means that use static setting by user manual set. The "**sntp**" means that use remote SNTP server. Use the no form of this command to default setting.

Example:

The example shows how to set clock source of switch. You can verify settings by the following show show clock command.

```
switch(config)# clock source sntp
switch(config)# show clock detail
08:32:12 test(UTC+5) Sep 21 2012
No time source
Time zone:
Acronym is DFL
Offset is UTC+8
```

3.28.4 clock summer-time

Command:

```
clock summer-time ACRONYM date
(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM
(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM [<1-
1440>]

clock summer-time ACRONYM recurring (usa|eu) [<1-1440>]

clock summer-time ACRONYM recurring (<1-5>|first|last)
(sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec)
HH:MM (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat)
(jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM [<1-1440>]

no clock summer-time
```

Parameter:

(jan|feb|mar|apr|ma	Specify acronym name of time zone

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

y|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM	
[<1-1440>]	Specify adjust offset of daylight saving time
usa	Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November
eu	Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October
(<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM	Specify ecurring daylight saving time duration.

Mode:

Global Configuration

Usage Guide:

Use the **clock summer-time** command to set daylight saving time for system time. The "**usa**" or "**eu**" means that use the global daylight saving policy which defined by international organization. In both the "**date**"and "**recurring**", the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The "**recurring**" means that adjust time every year within the month . Use the no form of this command to default setting.

Example:

The example shows how to set clock source of switch. You can verify settings by the following show show clock command.

```
switch(config)# clock source sntp
switch(config)# show clock detail
08:32:12 test(UTC+5) Sep 21 2012
No time source
Time zone:
Acronym is DFL
Offset is UTC+8
```


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

3.28.5 show clock

Command:

```
show clock [detail]
```

Parameter:

detail	Show more detail information of clock

Mode:

Global Configuration

Usage Guide:

Use the **show clock** command to show clock of switch. The "**detail**" means that show more information of clock such as time zone and daylight saving time.

Example:

The example shows how to show clock of switch and detail information.

```
Switch(config)# clock source sntp
Switch(config)# clock summer-time DLS recurring usa
Switch(config)# sntp host 192.168.1.100
Switch(config)# show clock
14:34:43 DLS(UTC+9) Sep 25 2012
Time source is sntp
Switch(config)# show clock detail
14:35:39 DLS(UTC+9) Sep 25 2012
Time source is sntp
Time zone:
Acronym is DFL
Offset is UTC+8
Summertime:
Acronym is DLS
Recurring every year.
Begins at 2 0 3 2:0
Ends at 1 0 11 2:0
Offset is 60 minutes.
```

3.28.6 sntp

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

Command:

```
sntp host HOSTNAME [port <1-65535>]

no sntp
```

Parameter:

HOSTNAME	Specify ip address or hostname of sntp server
port <1-65535>	Specify server port of sntp server

Mode:

Global Configuration

Usage Guide:

Use the sntp command to set remote SNTP server. Default server port is 123. Use the no form of this command to default setting.

Example:

The example shows how to set remote SNTP server of switch. You can verify settings by the following show show sntp command.

```
switch(config)# clock source sntp
switch(config)# sntp host 192.168.1.100
switch(config)# show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123
```

3.28.7 show sntp

Command:

```
show sntp
```

Mode:

Global Configuration

Usage Guide:

Use the **show sntp** command to remote SNTP server information.

Example:

The example shows how to show remote SNTP server.

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

```
Switch(config)# show sntp
SNTP is Enabled
SNTP Server address: 192.168.1.100
SNTP Server port: 123
```


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

3.29 VLAN

3.29.1 vlan

Command:

```
vlan

no vlan
```

Mode:

Global Configuration

Usage Guide:

Create or remove a VLAN entry. Using `vlan` command to entry the VLAN configuration mode.

Example:

The following example creates and removes a VLAN entry (100).

```
Switch# configure
Switch (config)# vlan 100
Switch (config-vlan)# exit
Switch (config)# no vlan 100
Switch (config)# exit
Switch#
```

3.29.2 vlan name

Command:

```
vlan name NAME
```

Parameter:

NAME	Specify the name of the VLAN (Max. 32 chars).

Mode:

VLAN Configuration

Usage Guide:

Configure the name of a VLAN entry.

Example:

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

This example sets the VLAN name of VLAN 100 to be `VLAN-one-hundred`.

```
Switch# configure
Switch(config)# vlan 100
Switch(config-vlan)# name VLAN-one-hundred
Switch(config-vlan)# exit
Switch(config)#
```

3.29.3 switchport mode

Command:

```
switchport mode ( access | hybrid | trunk [uplink] | tunnel )
```

Parameter:

access	Specify the VLAN mode to Access port.
hybrid	Specify the VLAN mode to Hybrid port.
trunk	Specify the VLAN mode to Trunk port.
uplink	Specify the Uplink property on this Trunk port.
tunnel	Specify the VLAN mode to Dot1Q Tunnel port.

Default:

Switchport mode trunk

Mode:

Port Configuration

Usage Guide:

The VLAN mode is used to configure the port for different port role.

Access port: Accepts only untagged frames and join an untagged VLAN.

Hybrid port: Support all functions as defined in IEEE 802.1Q specification.

Trunk port: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. If it is an uplink port, it can recognize double tagging on this port.

Tunnel port: Port-based Q-in-Q mode.

The configuration could be shown by “show interface switchport” command.

Example:

This example sets VLAN mode to Access port.

```
Switch(config)# interface gi12
Switch(config-if)# switchport mode access
```

3.29.4 switchport hybrid pvid

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

Command:

```
switchport hybrid pvid <1-4094>
```

Parameter:

<1-4094>	Specify the port-based VLAN ID on the Hybrid port.

Default:

switchport hybrid pvid = 1

Mode:

Port Configuration

Usage Guide:

This command configures the hybrid port's PVID. The configuration could be shown by "show interface switchport" command.

Example:

This example sets PVID to 100.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 100
```

3.29.5 switchport hybrid ingress-filtering

Command:

```
switchport bybrid ingress-filtering

no switchport bybrid ingress-filtering
```

Mode:

Port Configuration

Usage Guide:

This command per port configures the ingress-filtering status. This filtering is used to filter the frames come from the non-member ingress port. The configuration could be shown by "show interface switchport" command.

Example:

This example sets ingress-filtering to disable.

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

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid ingress-filtering
```

3.29.6 switchport hybrid acceptable-frame-type

Command:

```
switchport hybrid acceptable-frame-type ( all | tagged-only | untagged-only )
```

Parameter:

all	Specify to accept all frames
tagged-only	Specify to only accept tagged frames
untagged-only	Specify to only accept untagged frames

Default:

switchport hybrid acceptable-frame-type = all

Mode:

Port Configuration

Usage Guide:

This command per port configures the acceptable-frame-type. The configuration could be shown by “show interface switchport” command.

Example:

This example sets acceptable-frame-type to tagged-only.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid acceptable-frame-type tagged-only
```

3.29.7 switchport hybrid allowed vlan add

Command:

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

```
switchport hybrid allowed vlan add VLAN-LIST [ ( tagged | untagged ) ]
```

Parameter:

VLAN-LIST	Specifies the VLAN list to be added
(tagged | untagged)	Specifies the member type to tagged or untagged.

Mode:

Port Configuration

Usage Guide:

This command per hybrid port configures to add the allowed VLAN list. The configuration could be shown by “show interface switchport” command.

Example:

This example sets port fa10 VLAN to join the VLAN 100 as tagged member.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport hybrid allowed vlan add 100
```

3.29.8 switchport hybrid allowed vlan remove

Command:

```
switchport hybrid allowed vlan remove VLAN-LIST
```

Parameter:

VLAN-LIST	Specifies the VLAN list to be removed.

Mode:

Port Configuration

Usage Guide:

This command per hybrid port configures to remove the allowed VLAN list. The configuration could be shown by “show interface switchport” command.

Example:

This example sets port fa10 VLAN to leave the VLAN 100.

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

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport hybrid allowed vlan remove 100
```

3.29.9 switchport access vlan

Command:

```
switchport access vlan <1-4094>
```

Parameter:

<1-4094>	Specifies the access VLAN ID.

Mode:

Port Configuration

Usage Guide:

This command per Access port configures the native VLAN ID. The configuration could be shown by “show interface switchport” command

Example:

This example sets Access port fa10 native VLAN ID to 100.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
```

3.29.10 switchport tunnel vlan

Command:

```
switchport tunnel vlan <1-4094>
```

Mode:

Port Configuration

Usage Guide:

The command per Tunnel port configures the native VLAN. The configuration could be shown by “show interface switchport” command

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

Example:

This example sets Tunnel port gi10 native VLAN to 100

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode tunnel
Switch(config-if)# switchport tunnel vlan 100
```

3.29.11 switchport trunk native vlan

Command:

```
switchport trunk native vlan <1-4094>
```

Mode:

Port Configuration

Usage Guide:

The command per Trunk port configures the native VLAN. The configuration could be shown by “show interface switchport” command.

Example:

This example sets Trunk port gi10 native VLAN to 100.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 100
```

3.29.12 switchport trunk allowed vlan

Command:

```
switchport trunk allowed vlan ( add | remove ) ( VLAN-LIST | all )
```

Parameter:

(add | remove)	Specify the action to add or remove the allowed VLAN list.
(VLAN-LIST | all)	Specify the VLAN list or all VLANs to be added or removed.

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

Mode:

Port Configuration

Usage Guide:

The command per Trunk port configures the allowed VLAN list. The configuration could be shown by “show interface switchport” command.

Example:

This example sets Trunk port gi10 to add the allowed VLAN 100.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport trunk allowed vlan add 100
```

3.29.13 switchport default-vlan tagged

Command:

```
switchport default-vlan tagged

no switchport default-vlan tagged
```

Mode:

Port Configuration

Usage Guide:

The command per port configures the membership of the default VLAN to tagged. The configuration could be shown by “show interface switchport” command.

Example:

This example sets Trunk port gi10 membership with the default VLAN to tagged.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport default-vlan tagged
```

3.29.14 switchport forbidden default-vlan

Command:

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

```
switchport forbidden default-vlan

no switchport forbidden default-vlan
```

Mode:

Port Configuration

Usage Guide:

The command per port configures the membership of the default VLAN to forbidden. The configuration could be shown by “show interface switchport” command.

Example:

This example sets the membership of the default VLAN with port gi10 to forbidden.

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport forbidden default-vlan
```

3.29.15 switchport forbidden vlan

Command:

```
switchport forbidden vlan ( add | remove ) VLAN-LIST
```

Parameter:

(add | remove)	Add or remove forbidden membership.
VLAN-LIST	Specify the VLAN list.

Mode:

Port Configuration

Usage Guide:

The command per port configures the membership of the specfied VLANs to forbidden. The configuration could be shown by “show interface switchport” command.

Example:

This example sets the membership of the VLAN 100 with port fa10 to forbidden

```
Switch# configure
Switch(config)# interface gi10
Switch(config-if)# switchport forbidden vlan add 100
```


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

3.29.16 management-vlan

Command:

```
management-vlan vlan <1-4094>

no management-vlan
```

Parameter:

<1-4094>	Specify the VLAN ID of management-vlan.

Default:

management VLAN = VLAN 1

Mode:

Global Configuration

Usage Guide:

(1) Set <1-4094> as management VLAN id; suggest to create the VLAN and make the port to be member of it firstly.

(2) When use no command, restore management vlan to be default VLAN.

(3) If want to see management vlan created ,use “show management-vlan”

Example:

The following example specifies that management vlan 2 is created

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

3.29.17 show management-vlan

Command:

```
show management-vlan
```

Parameter:

login	Add/Edit login authentication list
enable	Add/Edit enable authentication list
default	Edit default authentication list

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

Mode:

Global Configuration

Usage Guide:

Display information about management vlan

Example:

The following example specifies that show management vlan

```
Switch(config)# show management-vlan
```

3.29.18 protocol-vlan group

Command:

```
vlan protocol-vlan group <1-8> frame-type (ethernet_ii|llc_other|snap_1042)
protocol-value VALUE
no vlan protocol-vlan group <1-8>
```

Parameter:

<1-8>	Specify protocol vlan group to configure
(ethernet_ii|llc_other|snap_1042)	Specify protocol based frame type
VALUE	Specify protocol value to configure

Mode:

Global Configuration

Usage Guide:

Use the **vlan protocol-vlan group** Global Configuration mode command to add protocol vlan group with spefied proto type and value.

Use the no form of this command to remove protocol vlan group setting.

You can verify your setting by entering the **show vlan proto-vlan Privileged EXEC** command

Example:

The following example show how to configure protocol vlan group:

```
Switch(config)# vlan protocol-vlan group 1 frame-type ethernet_ii protocol-value
0x806
Switch(config)# vlan protocol-vlan group 2 frame-type llc_other protocol-value 0x800
Switch# show vlan protocol-vlan
```


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

```
Group ID | Status | Type | value
---------------+-------------------+---------------------+------------------
1 | Enabled | Ethernet | 0x0806
2 | Enabled | LLC other | 0x0800
3 | Disabled | -- | --
4 | Disabled | -- | --
5 | Disabled | -- | --
6 | Disabled | -- | --
7 | Disabled | -- | --
8 | Disabled | -- | --
```

3.29.19 protocol vlan binding

Command:

```
vlan protocol-vlan group <1-8> vlan <1-4094>

no vlan protocol-vlan group <1-8>
```

Parameter:

<1-8>	Specify protocol vlan group to binding
<1-4094>	Specifies the Proto VLAN ID to configure.

Mode:

Interface Configuration

Usage Guide:

Use the **vlan protocol-vlan binding** Interface Configuration mode command to binding protocol VLAN Group on specified interfaces,

Use the no form of this command to cancel protocol VLAN Group Binding.

You can verify your setting by entering the **show vlan protocol-vlan interfaces IF_PORTS Privileged EXEC** command

Example:

The following example how to configure Protocol VLAN function on specified interfaces.

```
Switch(config)# interface gi1
Switch(config-if)# vlan protocol-vlan group 1 vlan 2
Switch(config-if)# vlan protocol-vlan group 2 vlan 3
```

3.29.20 show protocol vlan group

Command:

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

```
show vlan protocol-vlan [group <1-8>]
```

Parameter:

<1-8>	Specify protocol vlan group to display

Mode:

Privileged EXEC

Usage Guide:

Use the **show vlan proto-vlan** command in EXEC mode to display Proto VLAN group configuration

Example:

The following example how to display Proto VLAN group configuration

```
Switch# show vlan protocol-vlan
Group ID | Status | Type | value
---------------+-------------------+--------------------+------------------
1 | Enabled | Ethernet | 0x0806
2 | Enabled | LLC other | 0x0800
3 | Disabled | -- | --
4 | Disabled | -- | --
5 | Disabled | -- | --
6 | Disabled | -- | --
7 | Disabled | -- | --
8 | Disabled | -- | --
```

3.29.21 show protocol vlan interfaces

Command:

```
show vlan protocol-vlan interfaces IF_PORTS
```

Parameter:

IF_PORTS	Specify interfaces protocol vlan to display

Mode:

Privileged EXEC

Usage Guide:

Use the **show vlan mac-vlan interface** command in EXEC mode to display the Protocol VLAN interfaces setting

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

Example:

The following example shows how to display the Protocol VLAN interfaces setting

```
Switch# show vlan protocol-vlan interfaces gi1
Port gi1 :
Group 1
Status : Enabled
VLAN ID : 2
Group 2
Status : Enabled
VLAN ID : 3
Group 3
Status : Disabled
Group 4
Status : Disabled
Group 5
Status : Disabled
Group 6
Status : Disabled
Group 7
Status : Disabled
Group 8
Status : Disabled
```


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

3.30 Voice VLAN

3.30.1 voice vlan

Command:

```
voice-vlan

no voice-vlan
```

Mode:

Global Configuration

Usage Guide:

Use the **voice vlan** global configuration command to enable the functional Voice VLAN on the device.

Use the no form of this command to disable voice vlan function.

You can verify your setting by entering the **show voice vlan Privileged EXEC** command.

Example:

The following example shows how to change voice vlan state from auto to oui mode.

```
Switch(config)# no voice-vlan
Switch(config)# voice-vlan cos 6
```

3.30.2 voice vlan id

Command:

```
voice-vlan vlan <1-4094>
```

Parameter:

<1-4094>	Specify the voice VLAN ID

Mode:

Global Configuration

Usage Guide:

Use the **voice vlan id** global configuration command to configure the VLAN identifier of the voice VLAN statically

You can verify your setting by entering the **show voice vlan Privileged EXEC** command

Example:

The following example shows how to set Voice VLAN ID, before make sure the VLAN EXIST.

```
Switch(config)# voice-vlan vlan 128
```


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

3.30.3 voice vlan oui-table

Command:

```
voice-vlan oui-table A:B:C DESCRIPTION

no voice-vlan oui-table A:B:C
```

Parameter:

A:B:C	Specify OUI Mac address to add or remove
DESCRIPTION	Specify description of the specified MAC address to the voice VLAN OUI table

Mode:

Global Configuration

Usage Guide:

Use the **voice vlan oui-table** global configuration command to add oui mac address to OUI Table

Use the **no** form of this command to remove all or specified oui mac address..

You can verify your setting by entering the **show voice vlan Privileged EXEC** command

Example:

This following example shows how to add OUI Mac.

```
Switch(config)#voice-vlan oui-table 00:01:02“Test”
```

3.30.4 voice vlan cos

Command:

```
voice-vlan cos <0-7> [remark]

no voice-vlan
```

Parameter:

<0-7>	Specify the voice VLAN Class of Service value in telephone oui mode
remark	Specify that the L2 user priority is remarked with the CoS value

Default:

The default cos value is 6, remark is disabled.

Mode:

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

Global Configuration

Usage Guide:

Use the **voice vlan cos** global configuration command to configure the voice VLAN cos value and 1p remark function

You can verify your setting by entering the **show voice vlan Privileged EXEC** command

Example:

The following example show how to set cos value and enable 1p remark function

```
Switch(config)# voice-vlan cos 7 remark
```

3.30.5 voice vlan aging-time

Command:

```
voice-vlan aing-time <30-65536>
```

Parameter:

<30-65536>	Specify the voice VLAN aging timeout interval in minutes

Default:

The default aging-timeout value is 1440 minutes

Mode:

Global Configuration

Usage Guide:

Use the **voice vlan aging-time** global configuration command to configure the voice VLAN aging timeout

You can verify your setting by entering the **show voice vlan Privileged EXEC** command

Example:

The following example show how to set aging time.

```
Switch(config)# voice-vlan aging-time 720
```


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

3.30.6 voice vlan cos mode

Command:

```
voice-vlan cos ( src | all )

no voice-vlan
```

Parameter:

src	Specify QoS attributes are applied to packets with OUIs in the source MAC address.
all	Specify QoS attributes are applied to packets that are classified to the Voice VLAN.

Default:

The defaultall port in Src mode.

Mode:

Interface Configuration

Usage Guide:

Use the **voice vlan cos mode** Interface configuration command to configure OUI voice VLAN cos mode configuration on an interface

You can verify your setting by entering the **show voice vlan interfaces Privileged EXEC** command

Example:

The following example how to configure voice packet QoS attributes on an interface

```
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan cos all
```

3.30.7 voice vlan enable

Command:

```
voice-vlan

no voice-vlan
```

Mode:

Interface Configuration

Usage Guide:

Use the **voice vlan** Interface configuration command to enable OUI voice VLAN configuration on an interface

Use the **no** form of this command to disable voice vlan on an interfaces

You can verify your setting by entering the **show voice vlan Privileged EXEC** command

Example:

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

The following example how to enable voice VLAN function in oui mode on an interface

```
Switch(config)#interface range gi1-3
Switch(config-if)#voice-vlan
```

3.30.8 show voice vlan

Command:

```
show voice-vlan

show voice-vlan interfaces IF_PORTS
```

Parameter:

IF_PORTS	Specifies intefaces to display voice VLAN settings in oui mode

Mode:

Privileged EXEC

Usage Guide:

Use the **show voice vlan** command in EXEC mode to display the voice VLAN status for all interfaces or for a specific interface if the voice VLAN type is OUI

Example:

The following example show how to display voice vlan auto mode and oui mode settings

```
Switch# show voice-vlan
Administrate Voice VLAN state : disabled
Voice VLAN ID : 1
Voice VLAN Aging : 720 minutes
Voice VLAN CoS : 5
Voice VLAN 1p Remark: enabled
Switch# show voice-vlan interfaces gi1
Voice VLAN Aging : 720 minutes
Voice VLAN CoS : 5
Voice VLAN 1p Remark: enabled
OUI table
OUI MAC | Description
```


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

```
--------------+-----------------
00:E0:BB | 3COM
00:03:6B | Cisco
00:E0:75 | Veritel
00:D0:1E | Pingtel
00:01:E3 | Siemens
00:60:B9 | NEC/Philips
00:0F:E2 | H3C
00:09:6E | Avaya
Port | State | Cos Mode
-------+----------+-----------
gi1 | Disabled | Src
```


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