

## Content

### CHAPTER 1 COMMANDS FOR BASIC SWITCH CONFIGURATION ..... 1-1

1.1 COMMANDS FOR BASIC CONFIGURATION .....	1-1
1.1.1 authentication line login.....	1-1
1.1.2 banner .....	1-2
1.1.3 boot img .....	1-2
1.1.4 boot startup-config .....	1-3
1.1.5 clock set .....	1-3
1.1.6 config.....	1-4
1.1.7 debug ssh-server .....	1-4
1.1.8 disable .....	1-4
1.1.9 enable .....	1-4
1.1.10 enable password .....	1-5
1.1.11 end .....	1-5
1.1.12 exec-timeout .....	1-5
1.1.13 exit .....	1-6
1.1.14 help .....	1-6
1.1.15 hostname .....	1-7
1.1.16 ip host.....	1-7
1.1.17 ipv6 host.....	1-8
1.1.18 ip http server .....	1-8
1.1.19 language.....	1-8
1.1.20 login.....	1-9
1.1.21 password.....	1-9
1.1.22 privilege.....	1-9
1.1.23 reload.....	1-10
1.1.24 service password-encryption .....	1-10
1.1.25 service terminal-length.....	1-11
1.1.26 sysContact .....	1-11
1.1.27 sysLocation .....	1-11
1.1.28 set default .....	1-12
1.1.29 setup.....	1-12

1.1.30 show clock.....	1-12
1.1.31 show cpu usage .....	1-13
1.1.32 show cpu utilization.....	1-13
1.1.33 show memory usage .....	1-13
1.1.34 show privilege .....	1-14
1.1.35 show privilege mode LINE .....	1-14
1.1.36 show tcam usage .....	1-14
1.1.37 show temperature .....	1-15
1.1.38 show tech-support .....	1-15
1.1.39 show version .....	1-15
1.1.40 username .....	1-15
1.1.41 web-auth privilege <1-15> .....	1-16
1.1.42 web language .....	1-17
1.1.43 write .....	1-17
1.1.44 write running-config .....	1-17
<b>1.2 COMMANDS FOR TELNET .....</b>	<b>1-18</b>
1.2.1 aaa authorization config-commands .....	1-18
1.2.2 accounting exec.....	1-18
1.2.3 accounting command.....	1-19
1.2.4 authentication enable .....	1-19
1.2.5 authentication ip access-class .....	1-20
1.2.6 authentication ipv6 access-class .....	1-20
1.2.7 authentication line login.....	1-21
1.2.8 authentication securityip .....	1-22
1.2.9 authentication securityipv6 .....	1-22
1.2.10 authorization.....	1-22
1.2.11 authorization line vty command .....	1-23
1.2.12 clear line vty <0-31> .....	1-24
1.2.13 crypto key clear rsa .....	1-24
1.2.14 terminal length .....	1-24
1.2.15 terminal monitor.....	1-25
1.2.16 telnet.....	1-25
1.2.17 telnet server enable .....	1-26
1.2.18 telnet-server max-connection.....	1-26
1.2.19 ssh-server authentication-retries.....	1-26
1.2.20 ssh-server enable.....	1-27
1.2.21 ssh-server host-key create rsa.....	1-27
1.2.22 ssh-server max-connection .....	1-28

Commands for Basic Switch Configuration	Content
1.2.23 ssh-server timeout .....	1-28
1.2.24 show crypto key .....	1-28
1.2.25 show ssh-server .....	1-28
1.2.26 show telnet login .....	1-29
1.2.27 show users .....	1-29
1.2.28 who .....	1-30
<b>1.3 COMMANDS FOR CONFIGURING SWITCH IP .....</b>	<b>1-30</b>
1.3.1 interface vlan .....	1-30
1.3.2 interface ethernet 0 .....	1-30
1.3.3 ip address .....	1-30
1.3.4 ipv6 address .....	1-31
1.3.5 ip bootp-client enable .....	1-31
1.3.6 ip dhcp-client enable .....	1-32
<b>1.4 COMMANDS FOR SNMP .....</b>	<b>1-32</b>
1.4.1 debug snmp mib .....	1-32
1.4.2 debug snmp kernel .....	1-33
1.4.3 rmon enable .....	1-33
1.4.4 show private-mib oid .....	1-33
1.4.5 show snmp .....	1-34
1.4.6 show snmp engineid .....	1-35
1.4.7 show snmp group .....	1-35
1.4.8 show snmp mib .....	1-36
1.4.9 show snmp status .....	1-36
1.4.10 show snmp user .....	1-37
1.4.11 show snmp view .....	1-37
1.4.12 snmp-server community .....	1-37
1.4.13 snmp-server enable .....	1-39
1.4.14 snmp-server enable traps .....	1-39
1.4.15 snmp-server engineid .....	1-39
1.4.16 snmp-server group .....	1-40
1.4.17 snmp-server host .....	1-41
1.4.18 snmp-server securityip .....	1-42
1.4.19 snmp-server securityip .....	1-42
1.4.20 snmp-server trap-source .....	1-42
1.4.21 snmp-server user .....	1-43
1.4.22 snmp-server view .....	1-44
1.4.23 switchport updown notification enable .....	1-44
<b>1.5 COMMANDS FOR SWITCH UPGRADE .....</b>	<b>1-45</b>

1.5.1 copy (FTP) .....	1-45
1.5.2 copy (TFTP) .....	1-46
1.5.3 ftp-dir .....	1-48
1.5.4 ftp-server enable .....	1-48
1.5.5 ftp-server timeout.....	1-48
1.5.6 ip ftp.....	1-49
1.5.7 show ftp.....	1-49
1.5.8 show tftp.....	1-49
1.5.9 tftp-server enable .....	1-50
1.5.10 tftp-server retransmission-number .....	1-50
1.5.11 tftp-server transmission-timeout.....	1-50
<b>CHAPTER 2 FILE SYSTEM COMMANDS .....</b>	<b>2-1</b>
2.1 CD.....	2-1
2.2 COPY .....	2-1
2.3 DELETE.....	2-2
2.4 DIR .....	2-2
2.5 FORMAT .....	2-3
2.6 MKDIR .....	2-3
2.7 MOUNT .....	2-4
2.8 PWD .....	2-4
2.9 RENAME .....	2-4
2.10 RMDIR .....	2-4
2.11 UNMOUNT .....	2-5
<b>CHAPTER 3 COMMANDS FOR CLUSTER .....</b>	<b>3-1</b>
3.1 CLEAR CLUSTER NODES .....	3-1
3.2 CLUSTER AUTO-ADD .....	3-1
3.3 CLUSTER COMMANDER.....	3-2
3.4 CLUSTER IP-POOL.....	3-2
3.5 CLUSTER KEEPALIVE INTERVAL .....	3-3
3.6 CLUSTER KEEPALIVE LOSS-COUNT .....	3-3
3.7 CLUSTER MEMBER .....	3-4
3.8 CLUSTER MEMBER AUTO-TO-USER .....	3-5
3.9 CLUSTER RESET MEMBER.....	3-5
3.10 CLUSTER RUN .....	3-6
3.11 CLUSTER UPDATE MEMBER .....	3-6

---

<b>3.12</b>	<b>DEBUG CLUSTER .....</b>	<b>3-7</b>
<b>3.13</b>	<b>DEBUG CLUSTER PACKETS .....</b>	<b>3-7</b>
<b>3.14</b>	<b>SHOW CLUSTER .....</b>	<b>3-8</b>
<b>3.15</b>	<b>SHOW CLUSTER MEMBERS.....</b>	<b>3-9</b>
<b>3.16</b>	<b>SHOW CLUSTER CANDIDATES.....</b>	<b>3-10</b>
<b>3.17</b>	<b>SHOW CLUSTER TOPOLOGY .....</b>	<b>3-10</b>
<b>3.18</b>	<b>RCOMMAND COMMANDER .....</b>	<b>3-12</b>
<b>3.19</b>	<b>RCOMMAND MEMBER .....</b>	<b>3-13</b>

# Chapter 1 Commands for Basic Switch Configuration

## Explanation:

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

## 1.1 Commands for Basic Configuration

### 1.1.1 authentication line login

**Command:** `authentication line {console | vty | web} login {local | radius | tacacs}`  
`no authentication line {console | vty | web} login`

**Function:** Configure VTY (login with Telnet and SSH), Web and Console, so as to select the priority of the authentication mode for the login user. The no form command restores the default authentication mode.

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

**Command Mode:** Global Mode.

**Usage Guide:** The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configured in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or accept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. AAA function and RADIUS server should be configured before the RADIUS authentication can be used. And TACACS server should be configured before the TACACS configuration method can be used.

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

If local authentication is configured while no local users are configured, users will be

able to login the switch via the Console method.

**Example:** Configure the Telnet and ssh login method to RADIUS authentication method.

Switch(config)# authentication line vty login radius

**Relative Command:** **aaa enable, radius-server authentication host, tacacs-server authentication host, tacacs-server key**

## 1.1.2 banner

**Command:** **banner *motd* <LINE>**

**no banner motd**

**Function:** This command is used to configure the information displayed when the login authentication of a telnet or console user is successful, the no command configures that the information is not displayed when the authentication is successful.

**Parameters:** **<LINE>**: The information displayed when the authentication is successful, length limit from 1 to 100 characters.

**Default:** Do not show the information when the authentication is successful.

**Command mode:** Global mode.

**Example:**

Switch(config)#banner motd Welcome

## 1.1.3 boot img

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

**Function:** Configure the first and second img files used in the next boot of master board.

**Parameters:** primary means to configure the first IMG file, backup means to configure the second IMG file, <img-file-url> is the full path of the booting IMG file, the format of which is as follows:

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

**Command Mode:** Admin Mode.

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

**Example:**

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

Switch#boot img flash:/nos.img backup

2. Set flash:/5.4.128.0\_nos.img as the first booting IMG file used in the next booting of the system.

```
Switch#boot img flash:/5.4.128.0_nos.img primary
```

## 1.1.4 boot startup-config

**Command:** boot startup-config {NULL | <file-url> }

**Function:** Configure the CFG file used in the next booting of the master board.

**Parameters:** The NULL keyword means to use the factory original configuration as the next booting configuration. Setting the CFG file used in the next booting as NULL equals to implementing set default and write commands. <file-url> is the full path of CFG file used in the next booting.

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

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Example:**

1. Set flash:/ startup.cfg as the booting CFG file used in the next booting of the system.

```
Switch# boot startup-config flash:/ startup.cfg
```

2. Set flash:/ test-trunk.cfg as the booting CFG file used in the next booting of the system.

```
Switch#boot startup-config flash:/ test-trunk.cfg
```

## 1.1.5 clock set

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

**Function:** Set system date and time.

**Parameter:** <HH:MM:SS> is the current time, and the valid scope for **HH** is 0 to 23, **MM** and **SS** 0 to 59; <YYYY.MM.DD> is the current year, month and date, and the valid scope for **YYYY** is 1970~2038, **MON** meaning month, and **DD** between 1 to 31.

**Command mode:** Admin Mode.

**Default:** upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.

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

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

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

**Relative Command:** show clock



## 1.1.6 config

**Command:** config [terminal]

**Function:** Enter Global Mode from Admin Mode.

**Parameter:** [terminal] indicates terminal configuration.

**Command mode:** Admin Mode

**Example:**

Switch#config

## 1.1.7 debug ssh-server

**Command:** debug ssh-server

no debug ssh-server

**Function:** Display SSH server debugging information; the “no debug ssh-server” command stops displaying SSH server debugging information.

**Default:** This function is disabled by default.

**Command mode:** Admin Mode.

## 1.1.8 disable

**Command:** disable

**Function:** Disable admin mode.

**Parameter:** None.

**Default:** None.

**Command mode:** Admin Mode.

**Usage Guide:** None.

**Example:**

Switch#disable

Switch>

## 1.1.9 enable

**Command:** enable [<1-15>]

**Function:** Use **enable** command to enter Admin Mode from User Mode, or change the privilege level of the users.

**Command mode:** User Mode/ Admin Mode.

**Default:** None.

**Usage Guide:** To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3

consecutive entry of Admin user password are all wrong, it remains in the User Mode. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password. Set the Admin user password under Global Mode with “**enable password**” command.

**Example:**

```
Switch>enable
```

```
Switch#
```

## 1.1.10 enable password

**Command:** **enable password** [level <1-15>] [0 | 7] <password>  
**no enable password** [level <1-15>]

**Function:** Configure the password used for enter Admin Mode from the User Mode, The “**no enable password**” command deletes this password.

**Parameter:** **level <1-15>** is used to specify the privilege level, the default level is 15. **<password>** is the password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

**Command mode:** Global Mode

**Default:** This password is empty by system default

**Usage Guide:** Configure this password to prevent unauthorized entering Admin Mode. It is recommended to set the password at the initial switch configuration. Also, it is recommended to exit Admin Mode with “**exit**” command when the administrator needs to leave the terminal for a long time.

## 1.1.11 end

**Command:** **end**

**Function:** Quit current mode and return to Admin mode when not at User Mode/ Admin Mode.

**Command mode:** Except User Mode/ Admin Mode

**Example:** Quit VLAN mode and return to Admin mode.

```
Switch(config-vlan1)#end
```

```
Switch#
```

## 1.1.12 exec-timeout

**Command:** **exec-timeout** <minutes> [<seconds>]  
**no exec-timeout**

**Function:** Configure the timeout of exiting admin mode. The “no exec-timeout” command restores the default value.

**Parameters:** **<minute>** is the time value shown in minute and ranges between 0~35791. **<seconds>** is the time value shown in seconds and ranges between 0~59.

**Command mode:** Global mode

**Default:** Default timeout is 10 minutes.

**Usage guide:** To secure the switch, as well to prevent malicious actions from unauthorized user, the time will be count from the last configuration the admin had made, and the system will exit the admin mode at due time. It is required to enter admin code and password to enter the admin mode again. The timeout timer will be disabled when the timeout is set to 0.

**Example:** Set the admin mode timeout value to 6 minutes.

```
Switch(config)#exec-timeout 6
```

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

```
Switch(config)#exec-timeout 5 30
```

## 1.1.13 exit

**Command:** exit

**Function:** Quit current mode and return to it's previous mode.

**Command mode:** All Modes

**Usage Guide:** This command is to quit current mode and return to it's previous mode.

**Example:** Quit global mode to it's previous mode

```
Switch#exit
```

```
Switch#
```

## 1.1.14 help

**Command:** help

**Function:** Output brief description of the command interpreter help system.

**Command mode:** All configuration modes.

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

**Example:**

```
switch(config)#help
```

CLI provides advanced help feature. When you need help, anytime at the command line please press '?'.

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

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show ve?'.)

## 1.1.15 hostname

**Command:** `hostname <hostname>`

`no hostname`

**Function:** Set the prompt in the switch command line interface. The no operation cancels the configuration.

**Parameter:** `<hostname>` is the string for the prompt, up to 64 characters are allowed.

**Command mode:** Global Mode

**Default:** The default prompt is relative with the switch.

**Usage Guide:** With this command, the user can set the CLI prompt of the switch according to their own requirements.

**Example:** Set the prompt to "Test".

```
Switch(config)#hostname Test
```

```
Test(config)#
```

## 1.1.16 ip host

**Command:** `ip host <hostname> <ip_addr>`

`no ip host {<hostname>|all}`

**Function:** Set the mapping relationship between the host and IP address; the "no ip host" parameter of this command will delete the mapping.

**Parameter:** `<hostname>` is the host name, up to 64 characters are allowed; `<ip_addr>` is the corresponding IP address for the host name, takes a dot decimal format; **all** is all of the host name.

**Command mode:** Global Mode

**Usage Guide:** Set the association between host and IP address, which can be used in commands like "ping `<host>`".

**Example:** Set IP address of a host with the hostname of "beijing" to 200.121.1.1.

```
Switch(config)#ip host beijing 200.121.1.1
```

Command related: telnet, ping, traceroute

## 1.1.17 ipv6 host

**Command:** `ipv6 host <hostname> <ipv6_addr>`

`no ipv6 host { <hostname> /all}`

**Function:** Configure the mapping relationship between the IPv6 address and the host; the `no` command deletes this mapping relationship.

**Parameter:** `<hostname>` is the name of the host, containing max 64 characters; `<ipv6_addr>` is the IPv6 address corresponding to the host name. **all** is all the host address.

**Command Mode:** Global Mode

**Usage Guide:** Configure a fixed corresponding relationship between the host and the IPv6 address, applicable in commands such as `traceroute6 <host>`, etc.

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

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

**Command related:** ping6, traceroute6

## 1.1.18 ip http server

**Command:** `ip http server`

`no ip http server`

**Function:** Enable Web configuration; the “`no ip http server`” command disables Web configuration

**Command mode:** Global mode

**Default:** Enable.

**Usage guide:** Web configuration is for supplying an interface configured with HTTP for the user, which is straight and visual, easy to understand.

**Example:** Enable Web Server function and enable Web configurations.

Switch(config)#ip http server

## 1.1.19 language

**Command:** `language {chinese | english}`

**Function:** Set the language for displaying the help information.

**Parameter:** **chinese** for Chinese display; **english** for English display.

**Command mode:** Admin and Config Mode.

**Default:** The default setting is English display.

**Usage Guide:** Switch provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information

display will revert to English.

## 1.1.20 login

**Command:** login

**no login**

**Function:** login enable password authentication, no login command cancels the login configuration.

**Command mode:** Global mode

**Default:** No login by default

**Usage guide:** By using this command, users have to enter the password set by password command to enter normal user mode with console; no login cancels this restriction.

**Example:** Enable password

Switch(config)#login

## 1.1.21 password

**Command:** password [0 | 7] <password>

**no password**

**Function:** Configure the password used for enter normal user mode on the console. The “no password” command deletes this password.

**Parameter:** password is the password for the user. If input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

**Command mode:** Global mode

**Default:** This password is empty by system default

**Usage guide:** When both this password and login command are configured, users have to enter the password set by password command to enter normal user mode on console.

**Example:**

Switch(config)#password 0 test

Switch(config)#login

## 1.1.22 privilege

**Command:** privilege mode level <1-15> LINE

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

**Function:** Configure the level for the specified command, the no command restores the original level of the command.

**Parameters:** mode: register mode of the command, ‘Tab’ or ‘?’ is able to show all register modes

<1-15> is the level, its range between 1 and 15

LINE: the command needs to be configured, it supports the command abbreviation

**Command Mode:** Global mode

**Usage Guide:** This function cannot change the command itself. LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the configuration is failure. For changing the command line with the parameter, it should fill in the parameter which is able to be selected discretionarily according to the required format. However, level of the no command is able to be set optionally and it does not affect the result. When using no command, LINE must be the configured command line. If the command line with the parameter, the parameter must be matched with the configured command. (After configure the privilege of enable command, please add command **authentication line console login local** and configure corresponding privilege username password to ensure users can enter privilege mode again. If console link in usual user mode after complete configuration through other login way, please input exit or quit again, it will prompt user to input user name password to enter privilege mode.)

**Example:** Change the level of **show ip route** command to level 5.

Switch(config)#privilege exec level 5 show ip route

Change the level of **peer A.B.C.D** command to level 6.

Switch(config)#privilege router-msdp level 6 peer 1.2.3.4

Restore the original level for **show ip route** command.

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

Restore the original level for **peer A.B.C.D** command.

Switch(config)#no privilege router-msdp level 6 peer 1.2.3.4

## 1.1.23 reload

**Command:** reload

**Function:** Warm reset the switch.

**Command mode:** Admin Mode.

**Usage Guide:** The user can use this command to restart the switch without power off.

## 1.1.24 service password-encryption

**Command:** service password-encryption

**no service password-encryption**

**Function:** Encrypt system password. The “**no service password-encryption**” command cancels the encryption.

**Command mode:** Global Mode

**Default:** No service password-encryption by system default

**Usage guide:** The current unencrypted passwords as well as the coming passwords configured by password, enable password, ip ftp and username command will be encrypted by executed this command. no service password-encryption cancels this function however encrypted passwords remain unchanged.

**Example:** Encrypt system passwords

Switch(config)#service password-encryption

## 1.1.25 service terminal-length

**Command:** service terminal-length <0-512>

**no service terminal-length**

**Function:** Configure the columns of characters displayed in each screen on terminal (vty). The “**no service terminal-length**” command cancels the screen shifting operation.

**Parameter:** Columns of characters displayed on each screen of vty, ranging between 0-512.

**Command mode:** Global Mode

**Usage guide:** Configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telnet ssh client and the Console will be following this configuration.

**Example:** Set the number of vty threads to 20.

Switch(config)#service terminal-length 20

## 1.1.26 sysContact

**Command:** sysContact <LINE>

**no sysContact**

**Function:** Set the factory contact mode, the “**no sysContact**” command reset the switch to factory settings.

**Parameter:** <LINE> is the prompt character string, range from 0 to 255 characters.

**Command mode:** Global Mode

**Default:** The factory settings.

**Usage guide:** The user can set the factory contact mode bases the fact instance.

**Example:** Set the factory contact mode to test.

Switch(config)#sysContact test

## 1.1.27 sysLocation

**Command:** sysLocation <LINE>



**no sysLocation**

**Function:** Set the factory address, the “**no sysLocation**” command reset the switch to factory settings.

**Parameter:** <LINE> is the prompt character string, range from 0 to 255 characters.

**Command mode:** Global Mode

**Default:** The factory settings.

**Usage guide:** The user can set the factory address bases the fact instance.

**Example:** Set the factory address to test.

Switch(config)#sysLocation test

## 1.1.28 set default

**Command:** set default

**Function:** Reset the switch to factory settings.

**Command mode:** Admin Mode.

**Usage Guide:** Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.

**Note:** After the command, “**write**” command must be executed to save the operation. The switch will reset to factory settings after restart.

**Example:**

Switch#set default

Are you sure? [Y/N] = y

Switch#write

Switch#reload

## 1.1.29 setup

**Command:** setup

**Function:** Enter the Setup Mode of the switch.

**Command mode:** Admin Mode.

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

## 1.1.30 show clock

**Command:** show clock

**Function:** Display the current system clock.

**Command mode:** Admin and Configuration Mode.

**Usage Guide:** If the system clock is inaccurate, user can adjust the time by examining the

system date and clock.

**Example:**

```
Switch#show clock
```

```
Current time is TUE AUG 22 11: 00: 01 2002
```

**Command related:** clock set

## 1.1.31 show cpu usage

**Command:** show cpu usage [<slotno>]

**Function:** Show CPU usage rate.

**Command mode:** Admin and configuration mode.

**Usage Guide:** Check the current usage of CPU resource by **show cpu usage** command.

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

**Example:** Show the current usage rate of CPU.

```
Switch#show cpu usage
```

```
Last 5 second CPU IDLE: 87%
```

```
Last 30 second CPU IDLE: 89%
```

```
Last 5 minute CPU IDLE: 89%
```

```
From running CPU IDLE: 89%
```

## 1.1.32 show cpu utilization

**Command:** show cpu utilization

**Function:** Show the current CPU utilization rate.

**Parameter:** None.

**Default:** None.

**Command mode:** Admin mode.

**Usage Guide:** This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.

**Example:** Show CPU utilization rate.

```
Switch#show cpu utilization
```

```
Last 5 second CPU USAGE: 9%
```

```
Last 30 second CPU USAGE: 11%
```

```
Last 5 minute CPU USAGE: 11%
```

```
From running CPU USAGE: 11%
```

## 1.1.33 show memory usage

**Command:** show memory usage [<slotno>]

**Function:** Show memory usage rate.

**Command mode:** Admin and configuration mode.

**Usage Guide:** Check the current usage of memory resource by **show memory usage** command. Only the **chassis switch** uses **slotno** parameter which is used to show the memory usage rate of card on the specified slot, if there is no parameter, the default is current card.

**Example:** Show the current usage rate of the memory.

```
Switch#show memory usage
```

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

## 1.1.34 show privilege

**Command:** show privilege

**Function:** Show privilege of the current users.

**Parameter:** None.

**Command Mode:** All configuration modes

**Example:** Show privilege of the current user.

```
Switch(Config)#show privilege
```

```
Current privilege level is 15
```

## 1.1.35 show privilege mode LINE

**Command:** show privilege mode LINE

**Function:** Show the level of the specified command.

**Parameters:** mode: register mode of the command, 'Tab' or '?' is able to show all register modes

LINE: the command needs to be configured, it supports the command abbreviation

**Command Mode:** Admin and configuration mode

**Usage Guide:** LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.

**Example:** Show the level of **privilege** command.

```
Switch(config)#show privilege exec show ip route
```

```
The command : show ip route
```

```
Privilege is : 15
```

## 1.1.36 show tcam usage

This command is not supported by the switch.

## 1.1.37 show temperature

**Command:** show temperature

**Function:** Display the current temperature of the switch CPU.

**Command mode:** All mode.

**Usage Guide:** This command is used to monitor the temperature of the switch CPU.

**Example:** Display the current temperature of the switch CPU.

Switch(Config)#show temperature

Temperature: 47.0625 °C

## 1.1.38 show tech-support

**Command:** show tech-support [no-more]

**Function:** Display the operational information and the task status of the switch. The technique specialist use this command to diagnose whether the switch operate normally.

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

**Command mode:** Admin and Configuration Mode.

**Usage Guide:** This command is used to collect the relative information when the switch operation is malfunctioned.

**Example:**

Switch#show tech-support

## 1.1.39 show version

**Command:** show version

**Function:** Display the version information of the switch.

**Command mode:** Admin and Configuration Mode.

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

**Example:**

Switch#show version.

## 1.1.40 username

**Command:** username <username> [privilege <privilege>] [password [0 | 7] <password>]

no username <username>

**Function:** Configure local login username and password along with its privilege level.

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

**Command Mode:** Global Mode.

**Usage Guide:** There are two available choices for the preferences of the registered commands in the switch. They are 1 and 15. Preference of 1 is for the commands of the normal user configuration mode. Preference of 15 is for the commands registered in modes other than the normal user configuration modes. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32.

**Notice:** The user can log in user and priority after the command configures, before issuing the command authentication line console login local, it should be made sure that at one user has be configured as preference level of 15, in order to login the switch and make configuration changes in privileged mode and global mode. If there are no configured local users with preference level of 15, while only Local authentication is configured for the Console login method, the switch can be login without any authentication. When using the HTTP method to login the switch, only users with preference level of 15 can login the switch, users with preference level other than 15 will be denied.

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

Above all the configurations, only the admin user is able to login the switch in privileged mode through Telnet or Console login method, user1 and user2 can only login the switch in normal user mode through the telnet and console login method. For HTTP login method, only the admin user can pass the authentication configuration, user1 and user2 will be denied.

```
Switch(config)#username admin privilege 15 password 0 admin
```

```
Switch(config)# username user1 privilege 1 password 7
```

```
4a7d1ed414474e4033ac29ccb8653d9b (The password is 32 bits password encrypted by MD5)
```

```
Switch(config)# username user2 password 0 user2
```

```
Switch(config)# authentication line console login local
```

## 1.1.41 web-auth privilege <1-15>

**Command:** web-auth privilege <1-15>

no web-auth privilege

**Function:** Configure the level of logging in the switch by web.

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

**Command Mode:** Global Mode.

**Default:** 15.

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

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

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

## 1.1.42 web language

**Command:** web language {chinese | english}

**Function:** Set the language for displaying the HTTP Server information.

**Parameter:** **chinese** for Chinese display; **english** for English display.

**Command mode:** Admin Mode

**Default:** The default setting is English display.

**Usage Guide:** The user can select the language according to their preference.

## 1.1.43 write

**Command:** write

**Function:** Save the currently configured parameters to the Flash memory.

**Command mode:** Admin Mode.

**Usage Guide:** After a set of configuration with desired functions, the setting should be saved to the specified configuration file, so that the system can revert to the saved configuration automatically in the case of accidentally powered off or power failure. This is the equivalent to the **copy running-config startup-config** command.

## 1.1.44 write running-config

**Command:** write running-config [<startup-config-file-name>]

**Function:** Save the current running config as .cfg file to Flash Memory.

**Parameters:** <startup-config-file-name> is the full path of the cfg file. The format of which is as follows:

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

**Command Mode:** Admin Mode.

**Usage Guide:** Config file saved by Flash Memory can be used for startup file.

**Example:** Save the current running config as .cfg file with name of 123.

Switch#write running-config 123.cfg

## 1.2 Commands for Telnet

### 1.2.1 aaa authorization config-commands

**Command:** aaa authorization config-commands

**no aaa authorization config-commands**

**Function:** Enable command authorization function for the login user with VTY (login with Telnet and SSH). The no command disables this function. Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command.

**Default:** Disable.

**Command Mode:** Global Mode.

**Usage Guide:** Only after configuring this command and configuring command authorization manner and authorization selection priority of login user with VTY, it can be authorized when configuring command with corresponding command level for login user with VTY.

**Example:** Enable VTY command authorization function.

Switch(config)# aaa authorization config-commands

### 1.2.2 accounting exec

**Command:** accounting line {console | vty} exec {start-stop | stop-only | none}  
method1 [method2...]

**no accounting line {console | vty} exec**

**Function:** Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.

**Parameters:** **line** selects the accounting line, including **console**, **vty** (telnet and ssh); **start-stop** sends the accounting start or the accounting stop when the user is logging or exit the login; **stop-only** sends the accounting stop when the user exits the login only; **none** does not send the accounting start or the accounting stop; **method** is the list of the accounting method, it only supports **tacacs** keyword; **tacacs** uses the remote TACACS+

server to count.

**Default:** There is no accounting.

**Command Mode:** Global Mode.

**Usage Guide:** **console** and **vty** login method are able to set the corresponding accounting method respectively, the accounting method only supports TACACS+ method currently.

**Example:** Configure the login accounting with the telnet method.

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

### 1.2.3 accounting command

**Command:** **accounting line {console | vty} command <1-15> {start-stop | stop-only | none} method1 [method2...]**

**no accounting line {console | vty} command <1-15>**

**Function:** Configure the list of the command accounting method with VTY (login with Telnet and SSH) and Console. The no command restores the default accounting method.

**Parameters:** **line** selects the accounting line, including **console**, **vty** (telnet and ssh); **command <1-15>** is the level of the accounting command; **start-stop** sends the accounting start or the accounting stop when the user is logging or exit the login; **stop-only** sends the accounting stop when the user exits the login only; **none** does not send the accounting start or the accounting stop; **method** is the list of the accounting method, it only supports **tacacs** keyword; **tacacs** uses the remote TACACS+ server to count.

**Default:** There is no accounting method.

**Command Mode:** Global Mode.

**Usage Guide:** **console** and **vty** login method are able to set the corresponding command accounting method respectively, the accounting method only supports TACACS+ method currently. Only the stop information of the accounting is recorded, whether command accounting configures start-stop method or stop-only method.

**Example:** Configure the command accounting with the telnet method.

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

### 1.2.4 authentication enable

**Command:** **authentication enable method1 [method2...]**

**no authentication enable**

**Function:** Configure the list of the enable authentication method. The no command restores the default authentication method.

**Parameters:** **method** is the list of the authentication method, it must be among **local**,



**tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

**Default:** The local authentication is enable command by default.

**Command Mode:** Global Mode.

**Usage Guide:** The enable authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

**Example:** Configure the enable authentication method to be tacacs and local.

Switch(config)#authentication enable tacacs local

## 1.2.5 authentication ip access-class

**Command:** authentication ip access-class {<num-std>|<name>}

**no authentication ip access-class**

**Function:** Binding standard IP ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

**Parameters:** <num-std> is the access-class number for standard numeric ACL, ranging between 1-99; <name> is the access-class name for standard ACL, the character string length is ranging between 1 and 32.

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

**Command Mode:** Global Mode.

**Example:** Binding standard IP ACL protocol to access-class 1.

Switch(config)#authentication ip access-class 1 in

## 1.2.6 authentication ipv6 access-class

**Command:** authentication ipv6 access-class {<num-std>|<name>} in

**no authentication ipv6 access-class**

**Function:** Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web; the no form command will cancel the binding ACL.

**Parameters:** <num-std> is the access-class number for standard numeric ACL, ranging

between 500-599; <name> is the access-class name for standard ACL, the character string length is ranging between 1 and 32.

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

**Command Mode:** Global Mode.

**Example:** Binding standard IP ACL protocol to access-class 500.

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

## 1.2.7 authentication line login

**Command:** authentication line {console | vty | web} login method1 [method2...]

**no authentication line {console | vty | web} login**

**Function:** Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user. The no form command restores the default authentication method.

**Parameters:** **line** selects the login line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authentication method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authenticate; **tacacs** uses the remote TACACS+ authentication server to authenticate; **radius** uses the remote RADIUS authentication server to authenticate.

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

**Command Mode:** Global Mode.

**Usage Guide:** The authentication method for Console, VTY and Web login can be configured respectively. And authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

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

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

**Example:** Configure the telnet and ssh login with the remote RADIUS authentication.

Switch(config)#authentication line vty login radius

**Relative Command:** `aaa enable`, `radius-server authentication host`, `tacacs-server authentication host`, `tacacs-server key`

## 1.2.8 authentication securityip

**Command:** `authentication securityip <ip-addr>`

`no authentication securityip <ip-addr>`

**Function:** To configure the trusted IP address for Telnet and HTTP login method. The no form of this command will remove the trusted IP address configuration.

**Parameters:** `<ip-addr>` is the trusted IP address of the client in dotted decimal format which can login the switch.

**Default:** No trusted IP address is configured by default.

**Command Mode:** Global Mode.

**Usage Guide:** IP address of the client which can login the switch is not restricted before the trusted IP address is not configured. After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch. Up to 32 trusted IP addresses can be configured in the switch.

**Example:** To configure 192.168.1.21 as the trusted IP address.

Switch(config)# authentication securityip 192.168.1.21

## 1.2.9 authentication securityipv6

**Command:** `authentication securityipv6 <ipv6-addr>`

`no authentication securityipv6 <ipv6-addr>`

**Function:** To configure the security IPv6 address for Telnet and HTTP login method. The no form of this command will remove the specified configuration.

**Parameters:** `<ipv6-addr>` is the security IPv6 address which can login the switch.

**Default:** No security IPv6 addresses are configured by default.

**Command Mode:** Global Mode.

**Usage Guide:** IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured. After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch. Up to 32 security IPv6 addresses can be configured in the switch.

**Example:** Configure the security IPv6 address is 2001:da8:123:1::1.

Switch(config)# authentication securityipv6 2001:da8:123:1::1

## 1.2.10 authorization

**Command:** `authorization line {console | vty | web} exec method [method...]`

**no authorization line {console | vty | web} exec**

**Function:** Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console. The no command restores the default authorization method.

**Parameters:** **line** selects the authorization line, including **console**, **vty** (telnet and ssh) and **web**; **method** is the list of the authorization method, it must be among **local**, **tacacs** and **radius** keywords; **local** uses the local database to authorize; **tacacs** uses the remote TACACS+ server to authorize; **radius** uses the remote RADIUS server to authorize.

**Default:** There is no authorization mode.

**Command Mode:** Global Mode.

**Usage Guide:** The authorization method for Console, VTY and Web login can be configured respectively. And authorization method can be any one or combination of Local, RADIUS or TACACS. When login method is configuration in combination, the preference goes from left to right. If the users have passed the authorization method, authorization method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used.

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

**Example:** Configure the telnet authorization method to RADIUS.

Switch(config)#authorization line vty exec radius

## 1.2.11 authorization line vty command

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

**no authorization line vty command <1-15>**

**Function:** Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH). The no command recovers to be default manner.

**Default:** The authorization manner is not configured as default.

**Command Mode:** Global Mode.

**Usage Guide:** Configure the authorization manner when VTY login user configures command, the manners include any combination of Local, RADIUS and TACACS, the manner of none is just as the last manner. When using combination authorization

manners, the priority of the front authorization manner is the highest and the others are in descending order; if the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored. Notice: as long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner. When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured. None is the manner of escaping and it only can be the last manner. This manner returns to passed authorization directly and it is successful to configure the command.

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

Switch(config)#authorization line vty command 1 tacacs

## 1.2.12 clear line vty <0-31>

**Command:** clear line vty <0-31>

**Function:** Delete the logged user information on the appointed line, force user to get down the line who logs in through telnet or ssh.

**Command mode:** Admin Mode.

**Usage guide:** After inputting this command, there is need to judge for this command, "Confirm[Y/N]: ", when inputting "Y" or "y", run to delete; when inputting "? ", do not run to delete, print the notice information only. When inputting other characters, do not run to delete.

## 1.2.13 crypto key clear rsa

**Command:** crypto key clear rsa

**Function:** Clear the secret key of ssh.

**Command mode:** Admin Mode.

## 1.2.14 terminal length

**Command:** terminal length <0-512>

**terminal no length**

**Function:** Set length of characters displayed in each screen on terminal; the "terminal no length" cancels the screen switching operation and display content once in all.

**Parameter:** Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display).

**Command mode:** Admin Mode.

**Default:** Default Length is 25.

**Usage guide:** Set length of characters displayed in each screen on terminal, so that the-More-message will be shown when displayed information exceeds the screen. Press any key to show information in next screen. Default length is 25.

**Example:** Configure length of characters in each display to 20.

Switch#terminal length 20

## 1.2.15 terminal monitor

**Command:** terminal monitor

terminal no monitor

**Function:** Copy debugging messages to current display terminal; the “terminal no monitor” command restores to the default value.

**Command mode:** Admin Mode.

**Usage guide:** Configures whether the current debugging messages is displayed on this terminal. If this command is configured on telnet or SSH clients, debug messages will be sent to that client. The debug message is displayed on console by default.

**Example:**

Switch#terminal monitor

## 1.2.16 telnet

**Command:** telnet [vrf <vrf-name>] [<ip-addr> | <ipv6-addr> | host <hostname>] [<port>]

**Function:** Login on the remote host by Telnet

**Parameter:** <vrf-name> is the specific VRF name; <ip-addr> is the IP address of the remote host, shown in dotted decimal notation; <ipv6-addr> is the IPv6 address of the remote host; <hostname> is the name of the remote host, containing max 64 characters; <port> is the port number, ranging between 0 and 65535.

**Command Mode:** Admin Mode.

**Usage Guide:** This command is used when the switch is applied as Telnet client, for logging on remote host to configure. When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey “CTRL+ \”. To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.

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

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

## 1.2.17 telnet server enable

**Command:** telnet server enable

**no telnet server enable**

**Function:** Enable the Telnet server function in the switch: the “no telnet server enable” command disables the Telnet function in the switch.

**Default:** Telnet server function is enabled by default.

**Command mode:** Global Mode

**Usage Guide:** This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch.

**Example:** Disable the Telnet server function in the switch.

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

## 1.2.18 telnet-server max-connection

**Command:** telnet-server max-connection {<max-connection-number> | default}

**Function:** Configure the max connection number supported by the Telnet service of the switch.

**Parameters:** <max-connection-number>: the max connection number supported by the Telnet service, ranging from 5 to 16. The default option will restore the default configuration.

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

**Command Mode:** Global Mode

**Usage Guide:** None.

**Example:** Set the max connection number supported by the Telnet service as 10.

```
Switch(config)#telnet-server max-connection 10
```

## 1.2.19 ssh-server authentication-retries

**Command:** ssh-server authentication-retries <authentication-retries>

**no ssh-server authentication-retries**

**Function:** Configure the number of times for retrying SSH authentication; the “no

**ssh-server authentication-retries** command restores the default number of times for retrying SSH authentication.

**Parameter:** **< authentication-retries >** is the number of times for retrying authentication; valid range is 1 to 10.

**Command mode:** Global Mode

**Usage Guide:** None.

**Default:** The number of times for retrying SSH authentication is 3 by default.

**Example:** Set the time for retrying SSH authentication to 5.

Switch(config)#ssh-server authentication-retries 5

## 1.2.20 ssh-server enable

**Command:** **ssh-server enable**

**no ssh-server enable**

**Function:** Enable SSH function on the switch; the **"no ssh-server enable"** command disables SSH function.

**Command mode:** Global Mode

**Default:** SSH function is disabled by default.

**Usage Guide:** In order that the SSH client can log on the switch, the users need to configure the SSH user and enable SSH function on the switch.

**Example:** Enable SSH function on the switch.

Switch(config)#ssh-server enable

## 1.2.21 ssh-server host-key create rsa

**Command:** **ssh-server host-key create rsa [modulus < modulus >]**

**Function:** Generate new RSA host key.

**Parameter:** **modulus** is the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024.

**Command mode:** Global Mode

**Default:** The system uses the key generated when the ssh-server is started at the first time.

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

**Example:** Generate new host key.



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

## 1.2.22 ssh-server max-connection

**Command:** `ssh-server max-connection {<max-connection-number>|default}`

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

**Parameters:** <max-connection-number>: the max connection number supported by the SSH service, ranging from 5 to 16. The default option will restore the default configuration.

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

**Command Mode:** Global Mode

**Usage Guide:** None.

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

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

## 1.2.23 ssh-server timeout

**Command:** `ssh-server timeout <timeout>`

`no ssh-server timeout`

**Function:** Configure timeout value for SSH authentication; the “**no ssh-server timeout**” command restores the default timeout value for SSH authentication.

**Parameter:** <timeout> is timeout value; valid range is 10 to 600 seconds.

**Command mode:** Global Mode

**Default:** SSH authentication timeout is 180 seconds by default.

**Usage Guide:** This command is used to set SSH authentication timeout, the default timeout is 180 seconds.

**Example:** Set SSH authentication timeout to 240 seconds.

Switch(config)#ssh-server timeout 240

## 1.2.24 show crypto key

**Command:** `show crypto key`

**Function:** Show the secret key of ssh.

**Command mode:** Admin Mode.

## 1.2.25 show ssh-server

**Command:** `show ssh-server`

**Function:** Display SSH state and users which log on currently.

**Command mode:** Admin Mode.

**Example:**

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

## 1.2.26 show telnet login

**Command:** show telnet login

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

**Command Mode:** Admin and Configuration Mode.

**Usage Guide:** Check the Telnet client messages connected through Telnet with the switch.

**Example:**

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

## 1.2.27 show users

**Command:** show users

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

**Command mode:** Admin Mode.

**Usage Guide:** When inputting this command, show the user information who logs in through telnet or ssh. It includes line number, user name and user IP. Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.

**Example:**

```
Switch#show users
```

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

## 1.2.28 who

**Command:** who

**Function:** Show the current login users with vty.

**Parameter:** None.

**Command Mode:** All configuration modes

**Example:** Show the current login users with vty.

Switch#who

Telnet user a login from 192.168.1.20

## 1.3 Commands for Configuring Switch IP

### 1.3.1 interface vlan

**Command:** interface vlan <vlan-id>

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

**Function:** Enter the VLAN interface configuration mode; the no operation of this command will delete the existing VLAN interface.

**Parameters:** <vlan-id> is the VLAN ID of an existing VLAN, ranging from 1 to 4094.

**Command Mode:** Global Configuration Mode.

**Usage Guide:** Users should first make sure the existence of a VLAN before configuring it. User “exit” command to quit the VLAN interface configuration mode back to the global configuration mode.

**Example:** Enter the VLAN interface configuration mode of VLAN1.

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#

### 1.3.2 interface ethernet 0

This command is not supported by the switch.

### 1.3.3 ip address

**Command:** ip address <ip-address> <mask> [secondary]

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

**Function:** Set the IP address and mask for the specified VLAN interface; the “no ip address <ip address> <mask> [secondary]” command deletes the specified IP address setting.

**Parameter:** <ip-address> is the IP address in dot decimal format; <mask> is the subnet

mask in dot decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

**Default:** No IP address is configured upon switch shipment.

**Command mode:** VLAN Interface Mode

**Usage Guide:** A VLAN interface must be created first before the user can assign an IP address to the switch.

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

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0
```

```
Switch(Config-if-Vlan1)#exit
```

```
Switch(config)#
```

**Relative Command:** **ip bootp-client enable**, **ip dhcp-client enable**

### 1.3.4 ipv6 address

**Command:** **ipv6 address <ipv6address / prefix-length> [eui-64]**

**no ipv6 address <ipv6address / prefix-length> [eui-64]**

**Function:** Configure aggregatable global unicast address, site-local address and link-local address for the interface.

**Parameters:** **<ipv6address>** is the prefix of an IPV6 address; **<prefix-length>** is the length of the prefix of an IPV6 address, ranging from 3 to 128; **eui-64** means that the eui64 interface id of the interface will automatically create an IPV6 address.

**Command Mode:** Interface Configuration Mode.

**Default:** None.

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

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

```
Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64
```

### 1.3.5 ip bootp-client enable

**Command:** **ip bootp-client enable**

**no ip bootp-client enable**

**Function:** Enable the switch to be a BootP Client and obtain IP address and gateway

address through BootP negotiation; the “**no ip bootp-client enable**” command disables the BootP Client function and releases the IP address obtained in BootP.

**Default:** BootP client function is disabled by default.

**Command mode:** VLAN Interface Mode

**Usage Guide:** Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed.

**Note:** To obtain IP address via BootP, a DHCP server or a BootP server is required in the network.

**Example:** Get IP address through BootP.

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

**Relative command:** ip address, ip dhcp-client enable

## 1.3.6 ip dhcp-client enable

**Command:** ip dhcp-client enable

**no ip dhcp-client enable**

**Function:** Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the “**no ip dhcp-client enable**” command disables the DHCP client function and releases the IP address obtained in DHCP. **Note:** To obtain IP address via DHCP, a DHCP server is required in the network.

**Default:** the DHCP client function is disabled by default.

**Command mode:** VLAN Interface Mode

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

**Example:** Getting an IP address through DHCP.

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

## 1.4 Commands for SNMP

### 1.4.1 debug snmp mib

**Command:** `debug snmp mib`

**no debug snmp mib**

**Function:** Enable the SNMP mib debugging; the "**no debug snmp mib**" command disables the debugging.

**Command Mode:** Admin Mode.

**Usage Guide:** When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

**Example:**

Switch#debug snmp mib

## 1.4.2 debug snmp kernel

**Command:** `debug snmp kernel`

**no debug snmp kernel**

**Function:** Enable the SNMP kernel debugging; the "**no debug snmp kernel**" command disables the debugging function.

**Command Mode:** Admin Mode.

**Usage Guide:** When user encounters problems in applying SNMP, the SNMP debugging is available to locate the problem causes.

**Example:**

Switch#debug snmp kernel

## 1.4.3 rmon enable

**Command:** `rmon enable`

**no rmon enable**

**Function:** Enable RMON; the "**no rmon enable**" command disables RMON.

**Command mode:** Global Mode

**Default:** RMON is enabled by default.

**Example:**

Enable RMON.

Switch(config)#rmon enable

Disable RMON.

Switch(config)#no rmon enable

## 1.4.4 show private-mib oid

**Command:** `show private-mib oid`

**Function:** Show the original oid of the private mib.

**Command mode:** Admin and configuration mode.

**Usage Guide:** Check the beginning oid of the private mib by **show private-mib oid** command.

**Example:** Show the original oid of the private mib.

```
Switch#show private-mib oid
```

```
Private MIB OID:1.3.6.1.4.1.6339
```

## 1.4.5 show snmp

**Command:** show snmp

**Function:** Display all SNMP counter information.

**Command mode:** Admin and Configuration Mode.

**Example:**

```
Switch#show snmp
```

```
0 SNMP packets input
```

```
    0 Bad SNMP version errors
```

```
    0 Unknown community name
```

```
    0 Illegal operation for community name supplied
```

```
    0 Encoding errors
```

```
    0 Number of requested variables
```

```
    0 Number of altered variables
```

```
    0 Get-request PDUs
```

```
    0 Get-next PDUs
```

```
    0 Set-request PDUs
```

```
0 SNMP packets output
```

```
    0 Too big errors (Max packet size 1500)
```

```
    0 No such name errors
```

```
    0 Bad values errors
```

```
    0 General errors
```

```
    0 Get-response PDUs
```

```
    0 SNMP trap PDUs
```

Displayed information	Explanation
snmp packets input	Total number of SNMP packet inputs.
bad snmp version errors	Number of version information error packets.
unknown community name	Number of community name error packets.
illegal operation for community name supplied	Number of permission for community name error packets.

encoding errors	Number of encoding error packets.
number of requested variable	Number of variables requested by NMS.
number of altered variables	Number of variables set by NMS.
get-request PDUs	Number of packets received by “get” requests.
get-next PDUs	Number of packets received by “getnext” requests.
set-request PDUs	Number of packets received by “set” requests.
snmp packets output	Total number of SNMP packet outputs.
too big errors	Number of “Too_ big” error SNMP packets.
maximum packet size	Maximum length of SNMP packets.
no such name errors	Number of packets requesting for non-existent MIB objects.
bad values errors	Number of “Bad_values” error SNMP packets.
general errors	Number of “General_errors” error SNMP packets.
response PDUs	Number of response packets sent.
trap PDUs	Number of Trap packets sent.

## 1.4.6 show snmp engineid

**Command:** show snmp engineid

**Function:** Display the engine ID commands.

**Command Mode:** Admin and Configuration Mode.

**Example:**

Switch#show snmp engineid

SNMP engineID:3138633303f1276c Engine Boots is:1

Displayed Information	Explanation
SNMP engineID	Engine number
Engine Boots	Engine boot counts

## 1.4.7 show snmp group

**Command:** show snmp group

**Function:** Display the group information commands.

**Command Mode:** Admin and Configuration Mode.



**Example:**

Switch#show snmp group

Group Name:initial                      Security Level:noAuthnoPriv

Read View:one

Write View:<no writeview specified>

Notify View:one

Displayed Information	Explanation
Group Name	Group name
Security level	Security level
Read View	Read view name
Write View	Write view name
Notify View	Notify view name
<no writeview specified>	No view name specified by the user

## 1.4.8 show snmp mib

**Command:** show snmp mib

**Function:** Display all MIB supported by the switch.

**Command Mode:** Admin and Configuration Mode.

## 1.4.9 show snmp status

**Command:** show snmp status

**Function:** Display SNMP configuration information.

**Command mode:** Admin and Configuration Mode.

**Example:**

Switch#show snmp status

Trap enable

RMON enable

Community Information:

V1/V2c Trap Host Information:

V3 Trap Host Information:

Security IP Information:

Displayed information	Description
Community string	Community string
Community access	Community access permission
Trap-rec-address	IP address which is used to receive Trap.
Trap enable	Enable or disable to send Trap.
SecurityIP	IP address of the NMS which is allowed

	to access Agent
--	-----------------

## 1.4.10 show snmp user

**Command:** show snmp user

**Function:** Display the user information commands.

**Command Mode:** Admin and Configuration Mode.

**Example:**

Switch#show snmp user

User name: initialsha

Engine ID: 1234567890

Auth Protocol:MD5      Priv Protocol:DES-CBC

Row status:active

Displayed Information	Explanation
User name	User name
Engine ID	Engine ID
Priv Protocol	Employed encryption algorithm
Auth Protocol	Employed identification algorithm
Row status	User state

## 1.4.11 show snmp view

**Command:** show snmp view

**Function:** Display the view information commands.

**Command Mode:** Admin and Configuration Mode.

**Example:**

Switch#show snmp view

View Name:readview      1.      -Included      active  
                                  1.3.      Excluded      active

Displayed Information	Explanation
View Name	View name
1.and1.3.	OID number
Included	The view includes sub trees rooted by this OID
Excluded	The view does not include sub trees rooted by this OID
active	State

## 1.4.12 snmp-server community

**Command:** `snmp-server community {ro | rw} {0 | 7} <string> [access {<num-std>|<name>}] [ipv6-access {<ipv6-num-std>|<ipv6-name>}] [read <read-view-name>] [write <write-view-name>]`

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

**Function:** Configure the community string for the switch; the no command deletes the configured community string.

**Parameter:** **<string>** is the configured community string. If key option is set as 0, the specified community string is not encrypted, if key option is set as 7, the specified community string is encrypted;

**ro | rw** is the specified access mode to MIB, **ro** for read-only and **rw** for read-write;

**<num-std>** is the access-class number for standard numeric ACL, ranging between 1-99;

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

**<ipv6-num-std>** is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

**<name>** is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32;

**<read-view-name>** is the name of readable view which includes 1-32 characters;

**<write-view-name>** is the name of writable view which includes 1-32 characters.

**Command mode:** Global Mode

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

**Example:**

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

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

Add a community string named "public" with read-only permission.

Switch(config)#snmp-server community ro 0 public

Modify the read-write community string named "private" to read-only.

Switch(config)# snmp-server community ro 0 private

Delete community string "private".

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

Bind the read-only community string "public" to readable view "pviewr".

Switch(config)#snmp-server community ro 0 public read pviewr

Bind the read-write community string "private" to readable view "pviewr" and writable view "pvieww".

```
Switch(config)#snmp-server community rw 0 private read pviewr write pvieww
```

### 1.4.13 snmp-server enable

**Command:** snmp-server enable

**no snmp-server enable**

**Function:** Enable the SNMP proxy server function on the switch. The "no snmp-server enable" command disables the SNMP proxy server function

**Command mode:** Global mode

**Default:** SNMP proxy server function is disabled by system default.

**Usage guide:** To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command.

**Example:** Enable the SNMP proxy server function on the switch.

```
Switch(config)#snmp-server enable
```

### 1.4.14 snmp-server enable traps

**Command:** snmp-server enable traps

**no snmp-server enable traps**

**Function:** Enable the switch to send Trap message; the "no snmp-server enable traps" command disables the switch to send Trap message.

**Command mode:** Global Mode

**Default:** Forbid to send Trap message.

**Usage Guide:** When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

**Example:**

Enable to send Trap messages.

```
Switch(config)#snmp-server enable traps
```

Disable to send Trap messages.

```
Switch(config)#no snmp-server enable traps
```

### 1.4.15 snmp-server engineid

**Command:** snmp-server engineid <engine-string>

**no snmp-server engineid**

**Function:** Configure the engine ID; the "no" form of this command restores to the default engine ID.

**Command Mode:** Global mode

**Parameter:** *<engine-string>* is the engine ID shown in 1-32 digit hex characters.

**Default:** Default value is the company ID plus local MAC address.

**Usage Guide:** None

**Example:** Set current engine ID to A66688999F

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

Restore the default engine ID

```
Switch(config)#no snmp-server engineid
```

## 1.4.16 snmp-server group

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

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

**Function:** This command is used to configure a new group; the “no” form of this command deletes this group.

**Command Mode:** Global Mode

**Parameter:** *<group-string>* group name which includes 1-32 characters

**NoauthNopriv** Applies the non recognizing and non encrypting safety level

**AuthNopriv** Applies the recognizing but non encrypting safety level

**AuthPriv** Applies the recognizing and encrypting safety level

**read-string** Name of readable view which includes 1-32 characters

**write-string** Name of writable view which includes 1-32 characters

**notify-string** Name of trappable view which includes 1-32 characters

**<num-std>** is the access-class number for standard numeric ACL, ranging between 1-99;

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

**<ipv6-num-std>** is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

**<name>** is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.

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

**Example:** Create a group CompanyGroup, with the safety level of recognizing and encrypting, the read viewname is readview, and the writing is disabled.

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

Delete group

Switch (config)#no snmp-server group CompanyGroup AuthPriv

### 1.4.17 snmp-server host

**Command:** snmp-server host { <host-ipv4-address> / <host-ipv6-address> } {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}} } <user-string>

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

**Function:** As for the v1/v2c versions this command configures the IPv4 or IPv6 address and Trap community character string of the network manage station receiving the SNMP Trap message. And for v3 version, this command is used for receiving the network manage station IPv4 or IPv6 address and the Trap user name and safety level; the “no” form of this command cancels this IPv4 or IPv6 address.

**Command Mode:** Global Mode.

**Parameter:** <host-ipv4-addr> is IP address of NMS management station which receives Trap message.

<host-ipv6-addr> is IPv6 address of NMS management station which receives Trap message.

v1 | v2c | v3 is the version number when sending the trap.

NoauthNopriv | AuthNopriv | AuthPriv is the safety level v3 trap is applied, which may be non encrypted and non authentication, non encrypted and authentication, encrypted and authentication.

<user-string> is the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3.

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

**Example:**

Configure an IP address to receive Trap

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

Delete an IPv6 address to receive Trap.

Switch(config)#no snmp-server host 2001::1 v1 usertrap

## 1.4.18 snmp-server securityip

**Command:** `snmp-server securityip {<ipv4-address> | <ipv6-address>}`

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

**Function:** Configure security IPv4 or IPv6 address allowed to access NMS management station; the no command deletes security IPv4 or IPv6 address configured.

**Command Mode:** Global Mode.

**Parameter:** <ipv4-address> is NMS security IPv4 address, dotted decimal notation.

<ipv6-address> is NMS security IPv6 address, colon hexadecimal.

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

**Example:**

Configure security IP address of NMS management station.

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

Delete security IPv6 address.

```
Switch(config)#no snmp-server securityip 2001::1
```

## 1.4.19 snmp-server securityip

**Command:** `snmp-server securityip {enable | disable}`

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

**Command Mode:** Global Mode

**Default:** Enable the security IP address authentication function.

**Example:**

Disable the security IP address authentication function.

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

## 1.4.20 snmp-server trap-source

**Command:** `snmp-server trap-source {<ipv4-address> | <ipv6-address>}`

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

**Function:** Set the source IPv4 or IPv6 address which is used to send trap packet, the no command deletes the configuration.

**Parameter:** <ipv4-address>: IPv4 address is used to send trap packet in dotted decimal notation

<ipv6-address>: IPv6 address is used to send trap packet in colon

hexadecimal.

**Command Mode:** Global Mode.

**Usage Guide:** If there is no configuration, select the source address according to the interface address sent by actual trap packet, when configure the IP address, adopt the configured source address as the source address of trap packet.

**Example:**

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

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

Delete the configured source address which is used to send IPv6 trap packet.

Switch(config)#no snmp-server trap-source 2001::1

## 1.4.21 snmp-server user

**Command:** snmp-server user *<user-string>* *<group-string>* [{authPriv | authNoPriv} auth {md5 | sha} *<word>*] [access {*<num-std>*|*<name>*}] [ipv6-access {*<ipv6-num-std>*|*<ipv6-name>*}]

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

**Function:** Add a new user to an SNMP group; the "no" form of this command deletes this user.

**Command Mode:** Global Mode.

**Parameter:** *<user-string>* is the user name containing 1-32 characters.

*<group-string>* is the name of the group the user belongs to, containing 1-32 characters.

**authPriv** use DES for the packet encryption.

**authNoPriv** not use DES for the packet encryption.

**auth** perform packet authentication.

**md5** packet authentication using HMAC MD5 algorithm.

**sha** packet authentication using HMAC SHA algorithm.

*<word>* user password, containing 8-32 character.

*<num-std>* is the access-class number for standard numeric ACL, ranging between 1-99;

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

*<ipv6-num-std>* is the access-class number for standard numeric IPv6 ACL, ranging between 500-599;

*<name>* is the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.

**Usage Guide:** If the encryption and authentication is not selected, the default settings will



be no encryption and no authentication. If the encryption is selected, the authentication must be done. When deleting a user, if correct username and incorrect group name is inputted, the user can still be deleted.

**Example:**

Add a new user tester in the UserGroup with an encryption safety level and HMAC md5 for authentication, the password is hellohello

```
Switch (config)#snmp-server user tester UserGroup authPriv auth md5 hellohello
```

Delete an User

```
Switch (config)#no snmp-server user tester
```

## 1.4.22 snmp-server view

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

**Function:** This command is used to create or renew the view information; the "no" form of this command deletes the view information.

**Command Mode:** Global Mode.

**Parameter:** *<view-string>* view name, containing 1-32 characters.

*<oid-string>* is OID number or corresponding node name, containing 1-255 characters.

**include | exclude**, include/exclude this OID.

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

**Example:**

Create a view, the name is readview, including iso node but not including the iso.3 node

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

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

Delete the view

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

## 1.4.23 switchport updown notification enable

**Command:** `[no] switchport updown notification enable`

**Function:** Enable/disable the function of sending the trap message to the port of UP/DOWN event.

**Default:** Send the trap message to the port of IP/DOWN event as default.

**Command Mode:** Port Mode.

**Usage Guide:** This command can control to send the trap message when the port

happens the UP/DOWN event or not. As default, send the trap message to all the ports of UP/DOWN event after enabled snmp trap.

**Example:** Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event.

```
Switch(config)#in e 1/0/1
```

```
Switch(config-if-ethernet1/0/1)#no switchport updown notification enable
```

```
Switch(config-if-ethernet1/0/1)#show running-config current-mode
```

```
!
```

```
Interface Ethernet1/0/1
```

```
no switchport updown notification enable
```

## 1.5 Commands for Switch Upgrade

### 1.5.1 copy (FTP)

**Command:** `copy <source-url> <destination-url> [ascii | binary]`

**Function:** Download files to the FTP client.

**Parameter:** **<source-url>** is the location of the source files or directories to be copied; **<destination-url>** is the destination address to which the files or directories to be copied; forms of **<source-url>** and **<destination-url>** vary depending on different locations of the files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission (default transmission method). When URL represents an FTP address, its form should be: `ftp://<username>:<password>@{<ipaddress>|<ipv6address>|<hostname> }/<filename>`, amongst **<username>** is the FTP user name, **<password>** is the FTP user password, **<ipaddress>|<ipv6address>** is the IPv4 or IPv6 address of the FTP server/client, **<hostname>** is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, **<filename>** is the name of the FTP upload/download file.

Special keywords of the filename

Keywords	Source or destination addresses
<b>running-config</b>	Running configuration files
<b>startup-config</b>	It means the reboot configuration files when using copy running-config startup-config command
<b>nos.img</b>	System files
<b>boot.rom</b>	System startup files
<b>stacking/nos.img</b>	As destination address, execute system files upgrade for Slave in stacking mode

<b>stacking/nos.rom</b>	As destination address, execute system startup files upgrade for Slave in stacking mode
-------------------------	---

**Command Mode:** Admin Mode.

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

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

```
ftp username>
```

```
ftp password>
```

```
ftp filename>
```

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

**Notice:** The devices which support VSF do not support the command of copy running-config startup.cfg/vsf\_startup.cfg.

#### Examples:

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

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

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

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

(3) Save images in the FLASH to the FTP server of 2004:1:2:3::6

```
Switch#copy nos.img ftp://username:password@2004:1:2:3::6/ nos.img
```

(4) Obtain system file nos.img from the FTP server 2004:1:2:3::6

```
Switch#copy ftp:// username:password@2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration files

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

**Relevant Command:** write

## 1.5.2 copy (TFTP)

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

**Function:** Download files to the TFTP client.

**Parameter:** <source-url> is the location of the source files or directories to be copied; <destination-url> is the destination address to which the files or directories to be copied; forms of <source-url> and <destination-url> vary depending on different locations of the

files or directories. **ascii** indicates the ASCII standard will be adopted; **binary** indicates that the binary system will be adopted in the file transmission (default transmission method). When URL represents a TFTP address, its form should be: `tftp://{<ipaddress>|<ipv6address>|<hostname>}/<filename>`, amongst `<ipaddress>|<ipv6address>` is the IPv4 or IPv6 address of the TFTP server/client, `<hostname>` is the name of the host mapping with the IPv6 address, it does not support the file download and upload with hosts mapping with IPv4 addresses, `<filename>` is the name of the TFTP upload/download file.

Special keyword of the filename

Keywords	Source or destination addresses
<b>running-config</b>	Running configuration files
<b>startup-config</b>	It means the reboot configuration files when using copy running-config startup-config command
<b>nos.img</b>	System files
<b>bootrom</b>	System startup files

**Command Mode:** Admin Mode.

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

```
tftp server ip/ipv6 address[x.x.x.x]/[x::x::x]>
```

```
tftp filename>
```

Requesting for TFTP server address, file name

**Example:**

(1) Save images in the FLASH to the TFTP server of 10.1.1.1

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

(2) Obtain system file nos.img from the TFTP server 10.1.1.1

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

(3) Save images in the FLASH to the TFTP server of 2004:1:2:3::6

```
Switch#copy nos.img tftp:// 2004:1:2:3::6/ nos.img
```

(4) Obtain system file nos.img from the TFTP server 2004:1:2:3::6

```
Switch#copy tftp:// 2004:1:2:3::6/nos.img nos.img
```

(5) Save the running configuration files

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

**Relevant Command:** write

### 1.5.3 ftp-dir

**Command:** `ftp-dir <ftp-server-url>`

**Function:** Browse the file list on the FTP server.

**Parameter:** The form of `<ftp-server-url>` is :  
`ftp://<username>:<password>@{ <ipv4address> | <ipv6address> }`, amongst `<username>` is *the FTP* user name, `<password>` is the FTP user password, `{ <ipv4address> | <ipv6address> }` is the IPv4 or IPv6 address of the FTP server.

**Command Mode:** Admin Mode

**Example:** Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”.

```
Switch#ftp-dir ftp://Switch:superuser @10.1.1.1.
```

### 1.5.4 ftp-server enable

**Command:** `ftp-server enable`

`no ftp-server enable`

**Function:** Start FTP server, the “`no ftp-server enable`” command shuts down FTP server and prevents FTP user from logging in.

**Default:** FTP server is not started by default.

**Command mode:** Global Mode

**Usage Guide:** When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not started by default.

**Example:** Enable FTP server service.

```
Switch#config
```

```
Switch(config)# ftp-server enable
```

**Relative command:** `ip ftp`

### 1.5.5 ftp-server timeout

**Command:** `ftp-server timeout <seconds>`

**Function:** Set data connection idle time.

**Parameter:** `<seconds>` is the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600.

**Default:** The system default is 600 seconds.

**Command mode:** Global Mode

**Usage Guide:** When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.

**Example:** Modify the idle threshold to 100 seconds.

```
Switch#config
```

```
Switch(config)#ftp-server timeout 100
```

## 1.5.6 ip ftp

**Command:** `ip ftp username <username> password [0 | 7] <password>`  
`no ip ftp username <username>`

**Function:** Configure the username and password for logging in to the FTP; the no operation of this command will delete the configured username and password simultaneously.

**Parameters:** `<username>` is the username of the FTP link, its range should not exceed 32 characters; `<password>` is the password of the FTP link, if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted.

**Default Settings:** The system uses anonymous FTP links by default.

**Command Mode:** Global Configuration Mode.

**Examples:** Configure the username as Switch and the password as superuser.

```
Switch#
```

```
Switch#config
```

```
Switch(config)#ip ftp username Switch password 0 superuser
```

```
Switch(config)#
```

## 1.5.7 show ftp

**Command:** `show ftp`

**Function:** Display the parameter settings for the FTP server.

**Command mode:** Admin and Configuration Mode.

**Default:** Do not display.

**Example:**

```
Switch#show ftp
```

```
Timeout : 600
```

Displayed information	Description
Timeout	Timeout time.

## 1.5.8 show tftp

**Command:** `show tftp`

**Function:** Display the parameter settings for the TFTP server.

**Default:** Do not display.

**Command mode:** Admin and Configuration Mode.

**Example:**

```
Switch#show tftp
timeout      : 60
Retry Times  : 10
```

Displayed information	Explanation
Timeout	Timeout time.
Retry Times	Retransmission times.

## 1.5.9 tftp-server enable

**Command:** `tftp-server enable`

**no tftp-server enable**

**Function:** Start TFTP server, the “**no tftp-server enable**” command shuts down TFTP server and prevents TFTP user from logging in.

**Default:** Disable TFTP Server.

**Command mode:** Global Mode

**Usage Guide:** When TFTP server function is enabled, the switch can still perform TFTP client functions. TFTP server is not started by default.

**Example:** Enable TFTP server service.

```
Switch#config
```

```
Switch(config)#tftp-server enable
```

**Relative Command:** `tftp-server timeout`

## 1.5.10 tftp-server retransmission-number

**Command:** `tftp-server retransmission-number <number>`

**Function:** Set the retransmission time for TFTP server.

**Parameter:** **<number>** is the time to re-transfer, the valid range is 1 to 20.

**Default:** Retransmit 5 times.

**Command mode:** Global Mode

**Example:** Modify the retransmission to 10 times.

```
Switch#config
```

```
Switch(config)#tftp-server retransmission-number 10
```

## 1.5.11 tftp-server transmission-timeout

**Command:** `tftp-server transmission-timeout <seconds>`

**Function:** Set the transmission timeout value for TFTP server.

**Parameter:** **<seconds>** is the timeout value, the valid range is 5 to 3600s.

**Default:** The system default timeout setting is 600 seconds.

**Command mode:** Global Mode

**Example:** Modify the timeout value to 60 seconds.

Switch#config

Switch(config)#ftp-server transmission-timeout 60



# Chapter 2 File System Commands

## 2.1 cd

**Command:** `cd <directory>`

**Function:** Change the working directory for the storage device.

**Parameters:** `<directory>` is the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80.

**Command Mode:** Admin Mode.

**Default Settings:** The default working directory is Flash.

**Usage Guide:** After this command implemented, the current storage device will switch to the new working directory, which can be viewed by the “pwd” command.

**Example:** Change the working directory of the current storage device to flash.

```
Switch#cd flash:
```

```
Switch#pwd
```

```
flash:/
```

```
Switch#
```

## 2.2 copy

**Command:** `copy <source-file-url> <dest-file-url>`

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

**Parameters:** `<source-file-url>` is the source file; `<dest-file-url>` is the destination file. When users operate on files stored in backup master board and line cards under IMG mode, URLs of the source file and the destination file should take such a form as described in the following requirements.

1. The prefix of the source file URL should be in one of the following forms:

- ☞ starting with “flash:/”
- ☞ “ftp://username:pass@server-ip/file-name”
- ☞ “tftp://server-ip/file-name”

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

- ☞ starting with “flash:/”
- ☞ “ftp://username:pass@server-ip/file-name”
- ☞ “tftp://server-ip/file-name”

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:**

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

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

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

URL Example: The URL of files in root directory of Flash devices on it should be flash:/nos.img.

**Example:** Copy the file “flash:/nos.img” and store it as “flash/ 6.1.11.0.img”.

```
Switch#copy flash:/nos.img flash:/nos-6.1.11.0.img
```

```
Copy flash:/nos.img to flash:/nos-6.1.11.0.img? [Y:N] y
```

```
Copied file flash:/nos.img to flash:/nos-6.1.11.0.img.
```

## 2.3 delete

**Command:** delete <file-url>

**Function:** Delete the designate file on the storage device.

**Parameters:** <file-url> is the full path of the file to be deleted.

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:** The designated file will be deleted after implementing this command.

**Example:** Delete file flash:/nos.img.

```
Switch#delete flash:/nos5.img
```

```
Delete file flash:/nos5.img?[Y:N]y
```

```
Deleted file flash:/nos.img.
```

## 2.4 dir

**Command:** dir [WORD]

**Function:** Display the information of the designated directory on the storage device.

**Parameters:** <WORD> is the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.

**Command Mode:** Admin Configuration Mode.

**Default Settings:** No <WORD> means to display information of the current working

directory.

**Usage Guide:** Implementing this command will display information of files and sub-directories in the designated directory.

**Note:** This command does not support a recursive display of all sub-directories.

**Example:** Display information of the directory “flash:/”.

Switch#dir flash:/

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

## 2.5 format

**Command:** `format <device>`

**Function:** Format the storage device.

**Parameters:** `<device>` is the name of the device to be formatted.

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:**

1. After formatting, all files on the storage device will be irrecoverably lost.
2. The only acceptable file system type of Format is FAT 32, without exception.
3. This command cannot be used to format flash.

## 2.6 mkdir

**Command:** `mkdir <directory>`

**Function:** Create a sub-directory in the designated directory on a certain storage device .

**Parameters:** `<directory>` is the sub-directory name, a sequence of consecutive characters, whose length ranges from 1 to 80.

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:** The new created directory should not be named the same as any other directory or file in the designated directory, or located on a flash device. If any error occurs, a prompt will be displayed.

## 2.7 mount

This command is not supported by the switch.

## 2.8 pwd

**Command:** pwd

**Function:** Display the current working directory.

**Parameters:** None.

**Command Mode:** Admin Mode.

**Default Settings:** The default directory is flash.

**Example:** Display the current working directory.

```
Switch#pwd
```

```
flash:/
```

```
Switch#
```

## 2.9 rename

**Command:** rename <source-file-url> <new-filename >

**Function:** Rename a designated file on the switch.

**Parameters:** <source-file-url> is the source file, in which whether specifying or not its path are both acceptable; <new-filename> is a filename without specifying its path.

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:** When using this command, if the new file name is not used as that of any existing directory or file, the rename operation can be done, or a prompt will indicate its failure.

**Example:** Change the name of file "nos.img" in the current working directory to "nos-6.1.11.0.img".

```
Switch# rename nos5.img nos-6.1.11.0.img
```

```
Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok !
```

## 2.10 rmdir

**Command:** rmdir <directory>

**Function:** Delete a sub-directory in the designated directory on a certain device .

**Parameters:** <directory> is the sub-directory name, a sequence of consecutive

characters whose length ranges from 1 to 80.

**Command Mode:** Admin Mode.

**Default Settings:** None.

**Usage Guide:** The directory to be deleted should exist and be empty, that is, all files in the directory should be deleted before deleting it, or an error prompt will be displayed.

## 2.11 unmount

This command is not supported by the switch.

## Chapter 3 Commands for Cluster

### 3.1 clear cluster nodes

**Command:** `clear cluster nodes [nodes-sn <candidate-sn-list> | mac-address <mac-addr>]`

**Function:** Clear the nodes in the candidate list found by the commander switch.

**Parameters:** candidate-sn-list: sn of candidate switches, ranging from 1 to 256. More than one candidate can be specified.

mac-address: mac address of the switches (including all candidates, members and other switches).

**Default:** No parameter means to clear information of all switches.

**Command Mode:** Admin Mode.

**Usage Guide:** After executing this command, the information of this node will be deleted from the chain list saved on commander switch. In 30 seconds, the commander will recreate a cluster topology and re-add this node. But after being read, the candidate id of the switch might change. The command can only be executed on commander switches

**Example:** Clear all candidate switch lists found by the commander switch.

Switch#clear cluster nodes

### 3.2 cluster auto-add

**Command:** `cluster auto-add`

`no cluster auto-add`

**Function:** When this command is executed in the commander switch, the newly discovered candidate switches will be added to the cluster as a member switch automatically; the “**no cluster auto-add**” command disables this function.

**Command mode:** Global Mode

**Default:** This function is disabled by default. That means that the candidate switches are not automatically added to the cluster.

**Usage Guide:** After enabling this command on a commander switch, candidate switches will be automatically added as members.

**Example:** Enable the auto adding function in the commander switch.

Switch(config)#cluster auto-add

### 3.3 cluster commander

**Command:** cluster commander [*<cluster-name>*]

no cluster commander

**Function:** Set the switch as a commander switch, and create a cluster.

**Parameter:** *<cluster-name>* is the cluster's name, no longer than 32 characters.

**Command mode:** Global Mode

**Default:** Default setting is no commander switch. cluster\_name is null by default.

**Usage Guide:** This command sets the role of a switch as commander switch and creates a cluster, which can only be executed on non commander switches. The cluster\_name cannot be changed after the switch becoming a commander, and "no cluster commander" should be executed first to do that. The no operation of this command will cancel the commander configuration of the switch.

**Example:** Set the current switch as the commander switch and name the cluster as switch.

```
Switch(config)#cluster commander switch
```

### 3.4 cluster ip-pool

**Command:** cluster ip-pool *<commander-ip>*

no cluster ip-pool

**Function:** Configure private IP address pool for member switches of the cluster.

**Parameters:** *commander-ip*: cluster IP address pool for allocating internal IP addresses of the cluster commander-ip is the head address of the address pool, of which the valid format is 10.x.x.x, in dotted-decimal notation; the address pool should be big enough to hold 128 members, which requires the last byte of addresses to be less than 126 (254 – 128 = 126) . IP address pool should never be changed with commander configured. The change can only be done after the "no cluster commander" command being executed.

**Command mode:** Global Mode

**Default:** The default address pool is 10.254.254.1.

**Usage Guide:** When candidate switches becomes cluster members, the commander switch allocates a private IP address to each member for the communication within the cluster, and thus to realized its management and maintenance of cluster members. This command can only be used on non-commander switches. Once the cluster established, users can not modify its IP address pool. The NO command of this command will restore the address pool back to default value, which is 10.254.254.1.

**Example:** Set the private IP address pool used by cluster member devices as

10.254.254.10

Switch(config)#cluster ip-pool 10.254.254.10

## 3.5 cluster keepalive interval

**Command:** cluster keepalive interval <second>

no cluster keepalive interval

**Function:** Configure the interval of keepalive messages within the cluster.

**Parameters:** <second>: keepalive interval, in seconds, ranging from 3 to 30.

**Default:** The default value is 30 seconds.

**Command Mode:** Global Configuration Mode.

**Usage Guide:** After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.

After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its keepalive interval is the one distributed by its commander.

Commander will send DP messages within the cluster once in every keepalive interval. Members will respond to the received DP messages with DR messages.

The no operation of this command will restore the keepalive interval in the cluster back to its default value.

**Example:** Set the keepalive interval in the cluster to 10 seconds.

Switch(config)#cluster keepalive interval 10

## 3.6 cluster keepalive loss-count

**Command:** cluster keepalive loss-count<loss-count>

no cluster keepalive loss-count

**Function:** Configure the max number of lost keepalive messages in a cluster that can be tolerated.

**Parameters:** loss-count: the tolerable max number of lost messages, ranging from 1 to 10.

**Default:** The default value is 3.

**Command Mode:** Global Configuration Mode

**Usage Guide:** After executing this command on a commander switch, the value of the parameter will be distributed to all member switches via the TCP connections between the commander and members.



After executing it on a non commander switch, the configuration value will be saved but not used until the switch becomes a commander. Before that, its loss-count value is the one distributed by its commander.

commander calculates the loss-count after sending each DP message by adding 1 to the loss-count of each switch and clearing that of a switch after receiving a DR message from the latter. When a loss-count reaches the configured value (3 by default) without receiving any DR message, the commander will delete the switch from its candidate chain list.

If the time that a member fails to receive DP messages from the commander reaches loss-count, it will change its status to candidate.

The no operation of this command will restore the tolerable max number of lost keepalive messages in the cluster back to its default value: 3.

**Example:** Set the tolerable max number of lost keepalive messages in the cluster to 5.

Switch(config)#cluster keepalive loss-count 5

## 3.7 cluster member

**Command:** cluster member {nodes-sn <candidate-sn-list> | mac-address <mac-addr> [id <member-id>]}

no cluster member {id <member-id> | mac-address <mac-addr>}

**Function:** On a commander switch, manually add candidate switches into the cluster created by it. The no command deletes the specified member switch to change it as candidate.

**Parameters:** nodes-sn: all cluster member switches as recorded in a chain list, each with a node sn which can be viewed by “show cluster candidates” command. One or more candidates can be added as member at one time. The valid range of candidate-sn-list is 1~256.

mac-address: the CPU Mac of candidate switches

member-id: A member id can be specified to a candidate as it becomes a member, ranging from 1 to 128, increasing from 1 by default.

nodes-sn is the automatically generated sn, which may change after the candidate becomes a member. Members added this way will be actually treated as those added in mac-addr mode with all config files in mac-addr mode.

If more than one switch is added as member simultaneously, no member-id is allowed; neither when using nodes-sn mode.

**Default:** None.

**Command Mode:** Global Mode

**Usage Guide:** After executing this command, the switch will add those identified in

**<nodes-sn>** or **<mac-address>** into the cluster it belongs to. One or more candidates are allowed at one time, linked with '-' or ';'. A switch can only be member or commander of one cluster, exclusively. Attempts to execute the command on a non commander switch will return error. The no operation of this command will delete the specified member switch, and turn it back to a candidate.

**Example:** In the commander switch, add the candidate switch which has the sequence number as 1. In the commander switch, add the switch whose the mac address is 11-22-33-44-55-66 to member, and the member-id is 5.

```
Switch(config)#cluster member nodes-sn 1
```

```
Switch(config)#cluster member mac-address 11-22-33-44-55-66 id 5
```

## 3.8 cluster member auto-to-user

**Command:** cluster member auto-to-user

**Function:** All members will be deleted when configuring no cluster auto-add. Users need to change automatically added members to manually added ones to keep them.

**Parameter:** None.

**Default:** None.

**Command Mode:** Global Mode.

**Usage Guide:** Execute this command on a switch to change automatically added members to manually added ones.

**Example:** change automatically added members to manually added ones.

```
Switch(config)#cluster member auto-to-user
```

## 3.9 cluster reset member

**Command:** cluster reset member [id <member-id> / mac-address <mac-addr>]

**Function:** In the commander switch, this command can be used to reset the member switch.

**Parameter:** member-id: ranging from 1 to 128. Use hyphen "-" or semicolon ";" to specify more than one member; if no value is provided, it means to reboot all member switches.

**Default:** Boot all member switches.

**Command mode:** Admin Mode.

**Instructions:** In the commander switch, users can use this command to reset a member switch. If this command is executed in a non-commander switch, an error will be displayed.

**Example:** In the commander switch, reset the member switch 1.

Switch#cluster reset member 1

## 3.10 cluster run

**Command:** cluster run [key <WORD>] [vid <VID>]

**no cluster run**

**Function:** Enable cluster function; the “no cluster run” command disables cluster function.

**Parameter:** key: all keys in one cluster should be the same, no longer than 16 characters.

vid: vlan id of the cluster, whose range is 1-4094.

**Command mode:** Global Mode

**Default:** Cluster function is disabled by default, key: NULL(\0) vid: 1.

**Instructions:** This command enables cluster function. Cluster function has to be enabled before implementing any other cluster commands. The “no cluster run” disables cluster function. It is recommended that users allocate an exclusive vlan for cluster (such as vlan100)

**Note:** Routing protocols should be disabled on the layer-3 interface where cluster vlan locates to avoid broadcasting private route of the cluster.

**Example:** Disable cluster function in the local switch.

Switch (config)#no cluster run

## 3.11 cluster update member

**Command:** cluster update member <member-id> <src-url> <dst-filename> [ascii | binary]

**Function:** Remotely upgrade member switches from the commander switch.

**Parameters:** member-id: ranging from 1 to 128. Use hyphen “-” or semicolon “;” to specify more than one member;

src-url: the location of source files to be copied;

dst-filename: the specified filename for saving the file in the switch flash;

ascii means that the file transmission follows ASCII standard; binary means that the file transmission follows binary standard, which is the default mode.

when src-url is a FTP address, its form will be: ftp://<username>:<password>@<ipaddress>/<filename>, in which <username> is the FTP username <password> is the FTP password <ipaddress> is the IP address of the FTP server, <filename> is the name of the file to be downloaded via FTP.

when src-url is a TFTP address, its form will be: tftp://<ipaddress>/<filename>, in which

<ipaddress> is the IP address of the TFTP server <filename> is the name of the file to be downloaded via.

Special keywords used in filename:

Keywords	source or destination address
startup-config	start the configuration file
nos.img	system file

**Command mode:** Admin Mode

**Usage Guide:** The commander distributes the remote upgrade command to members via the TCP connections between them, causing the number to implement the remote upgrade and reboot. Trying to execute this command on a non-commander switch will return errors. If users want to upgrade more than one member, these switches should be the same type to avoid boot failure induced by mismatched IMG files.

**Example:** Remotely upgrade a member switch from the commander switch, with the member-id being 1, src-url being ftp:// switch: switch @192.168.1.1/nos.img, and dst-url being nos.img

```
Switch#cluster update member 1 ftp:// switch: switch @192.168.1.1/nos.img nos.img
```

## 3.12 debug cluster

**Command:** debug cluster {statemachine | application | tcp}

**no debug cluster {statemachine | application | tcp}**

**Function:** Enable the application debug of cluster; the no operation of this command will disable that.

**Parameters:** statemachine: print debugging when the switch status changes.

application: print debugging when there are users trying to configure the switch after logging onto it via SNMP, WEB.

tcp: the TCP connection between the commander and the member.

**Default:** None.

**Command Mode:** Admin Mode.

**Usage Guide:** None.

**Example:** Enable the debug status changed on the switch.

```
Switich#debug cluster statemachine
```

## 3.13 debug cluster packets

**Command:** debug cluster packets {DP | DR | CP} {receive | send}

**no debug cluster packets {DP | DR | CP} {receive | send}**

**Function:** Enable the debug; the no command disables the debug.

**Parameters:** DP: discovery messages.

DR: responsive messages.

CP: command messages.

receive: receive messages.

send: send messages.

**Default:** None.

**Command Mode:** Admin Mode.

**Usage Guide:** Enable the debug of cluster messages. After enabling classification, all DP, DR and CP messages sent or received in the cluster will be printed.

**Example:** Enable the debug of receiving DP messages.

Switch#debug cluster packets DP receive

## 3.14 show cluster

**Command:** show cluster

**Function:** Display cluster information of the switch.

**Parameter:** None.

**Command Mode:** Admin and Configuration Mode.

**Usage Guide:** None.

**Example:** Execute this command on different switches.

---in a commander-----

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: commander

IP pool: 10.254.254.1

Cluster name: MIS\_zebra

Keepalive interval: 30

Keepalive loss-count: 3

Auto add: Disabled

Number of Members: 0

Number of Candidates: 3

---in a member -----

Switch#show cluster

Status: Enabled

Cluster VLAN: 1

Role: Member

```

Commander Ip Address: 10.254.254.1
Internal Ip Address: 10.254.254.2
Commamder Mac Address: 00-12-cf-39-1d-90
---- a candidate -----
Switch#show cluster
Status: Enabled
Cluster VLAN: 1
Role: Candidate
---- disabled -----
Switch#show cluster
Status: Disabled

```

## 3.15 show cluster members

**Command:** `show cluster members [id <member-id> | mac-address <mac-addr>]`

**Function:** Display member information of a cluster. This command can only apply to commander switches.

**Parameters:** member-id: member id of the switch.

mac-addr: the CPU mac addresses of member switches.

**Default:** No parameters means to display information of all member switches.

**Command Mode:** Admin and Configuration Mode.

**Usage Guide:** Executing this command on a commander switch will display the configuration information of all cluster member switches.

**Example:** Execute this command on a commander switch to display the configuration information of all and specified cluster member switches.

```
Switch#show cluster members
```

Member From : User config(U); Auto member (A)

ID	From	Status	Mac	Hostname	Description	Internal IP
1	U	Inactive	00-01-02-03-04-05	MIS_zebra	DCRS-6804	10.254.254.2
2	A	Active	00-01-02-03-04-05	MIS_bison	DCRS-6804	10.254.254.3
3	U	Active	00-01-02-03-04-05	SRD_jaguar	DCRS-9808	10.254.254.4
4	A	Inactive	00-01-02-03-04-05	HRD_puma	DCRS-5950-28T	10.254.254.5

```
Switch#show cluster members id 1
```

Cluster Members:

```
ID: 1
```

Member status: Inactive member (user\_config)

IP Address: 10.254.254.2

MAC Address: 00-01-02-03-04-06

Description: DCRS-9808

Hostname: DSW102

## 3.16 show cluster candidates

**Command:** show cluster candidates [nodes-sn <candidate-sn-list> | mac-address <mac-addr>]

**Function:** Display the statistic information of the candidate member switches on the command switch

**Parameter:** candidate-sn-list: candidate switch sn, ranging from 1 to 256. More than one switch can be specified.

mac-address: mac address of the candidate switch

**Default:** No parameters means to display information of all member switches.

**Command Mode:** Admin and Configuration Mode.

**Usage Guide:** Executing this command on the switch will display the information of the candidate member switches.

**Example:** Display configuration information of all cluster candidate switches.

Switch#show cluster candidates

Cluster Candidates:

SN	Mac	Description	Hostname
-----			
xxx xx-xx-xx-xx-xx-xx	xxxxxxxxxxxxxxxxxxxxxxxxxx24	xxxxxxxxxxxxxxxxxxxxxxxxxx24	
1	00-01-02-03-04-06	ES3528M	
2	01-01-02-03-04-05	ES3528M	MIS_zebra

## 3.17 show cluster topology

**Command:** show cluster topology [root-sn <starting-node-sn> | nodes-sn <node-sn-list> | mac-address <mac-addr>]

**Function:** Display cluster topology information. This command only applies to commander switches.

**Parameters:** starting-node-sn: the starting node of the topology.

node-sn-list: the switch node sn.

mac-addr: the CPU mac address of the switch.

**Command Mode:** Admin and Configuration Mode.

**Example:** Execute this command on the commander switch to display the topology information under different conditions.

Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

local-port	remote-port	node
------------	-------------	------

x xxx xxxxxxxxxxxx12 xxxxxxxxxxxx12 xx xx-xx-xx-xx-xx-xx xxxxxxxxxxxx12 xxxxxxxxxxxx12 x

```
2 ES4626H      LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1      eth 1/0/2
```

```
3 ES4626H      LAB_SWITCH_3 CA 01-02-03-04-05-03 eth 1/0/1      eth 1/0/3
```

```
4 ES4626H      LAB SWITCH 4 CA 01-02-03-04-05-04 eth 1/0/1      eth 1/0/4
```

.....

```
5 ES3528M      LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/0/1      eth 1/0/2
```

6	ES3528M	LAB_SWITCH_1	OM	01-02-03-04-05-14	eth 1/0/1	eth 1/0/3
---	---------	--------------	----	-------------------	-----------	-----------

-----

Role: commander(CM);Member(M);Candidate(CA);Other commander(OC);Other member(OM)

local-port	remote-port	node
------------	-------------	------

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----



```
=====
* 2 ES4626H      LAB_SWITCH_2 M 01-02-03-04-05-02 eth 1/0/1  eth 1/0/2  -
    5 ES3528M      LAB_SWITCH_1 OC 01-02-03-04-05-13 eth 1/0/1  eth 1/0/2
Y
    6 ES3528M      LAB_SWITCH_1 OM 01-02-03-04-05-14 eth 1/0/1  eth 1/0/3
Y
```

```
Switch#show cluster topology nodes-sn 2
```

```
Topology role: Member
```

```
Member status: Active member (user-config)
```

```
SN: 2
```

```
MAC Address: 01-02-03-04-05-02
```

```
Description: ES4626H
```

```
Hostname : LAB_SWITCH_2
```

```
Upstream local-port: eth 1/0/1
```

```
Upstream node: 01-02-03-04-05-01
```

```
Upstream remote-port:eth 1/0/2
```

```
Upstream speed: 100full
```

```
Switch#
```

```
Switch#show cluster topology mac-address 01-02-03-04-05-02
```

```
Topology role: Member
```

```
Member status: Active member (user-config)
```

```
SN: 2
```

```
MAC Address: 01-02-03-04-05-02
```

```
Description: ES4626H
```

```
Hostname : LAB_SWITCH_2
```

```
Upstream local-port: eth 1/0/1
```

```
Upstream node: 01-02-03-04-05-01
```

```
Upstream remote-port: eth 1/0/2
```

```
Upstream speed: 100full
```

## 3.18 rcommand commander

**Command:** rcommand commander

**Function:** In the member switch, use this command to configure the commander switch.

**Parameter:** None.

**Default:** None.

**Command mode:** Admin Mode.

**Instructions:** This command is used to configure the commander switch remotely. Users have to telnet the commander switch by passing the authentication. The command “**exit**” is used to quit the configuration interface of the commander switch. This command can only be executed on member switches.

**Example:** In the member switch, enter the configuration interface of the commander switch.

```
Switch#rcommand commander
```

### 3.19 rcommand member

**Command:** `rcommand member <mem-id>`

**Function:** In the commander switch, this command is used to remotely manage the member switches in the cluster.

**Parameter:** `<mem-id>` commander the member id allocated by commander to each member, whose range is 1~128.

**Default:** None.

**Command mode:** Admin Mode.

**Usage Guide:** After executing this command, users will remotely login to a member switch and enter Admin Mode on the latter. Use exit to quit the configuration interface of the member. Because of the use of internal private IP, telnet authentication will be omitted on member switches. This command can only be executed on commander switches.

**Example:** In the commander switch, enter the configuration interface of the member switch with member-id 1.

```
Switch#rcommand member 1
```