

01-Commands For Basic Switch Configuration

Content
目录

1 Commands for Basic Configuration	7
authentication line	7
banner	7
boot img	8
boot startup-config	8
clock set	9
config	10
disable	10
enable	10
enable password	11
end	12
exec-timeout	12
exit	13
help	13
hostname	14
ip host	14
ipv6 host	15
ip http server	15
login	16
password	16
privilege	17
reload	17
service password-encryption	18
service terminal-length	18
sysContact	19
sysLocation	19
set default	20
set boot password	20
setup	21
show clock	21
show cpu usage	22
show cpu utilization	22
show memory usage	23
show privilege	23
show privilege mode LINE	24
show tech-support	24
show version	25
username	25
web-auth privilege <1-15>	26
write	26
write running-config	27
2 Commands for Telnet	28
aaa authorization config-commands	28
accounting exec	28
accounting command	29
authentication enable	30
authentication ip access-class	30
authentication ipv6 access-class	31
authentication line login	31
authentication securityip	32
authentication securityipv6	33
authorization	34
authorization line vty command	34
clear line vty <0-31>	35
crypto key clear rsa	36
terminal length	36
telnet	37
telnet server enable	38
telnet-server max-connection	38
ssh-server authentication-retries	38
ssh-server enable	39
ssh-server host-key create rsa	39
ssh-server max-connection	40
ssh-server timeout	41

show crypto key	41
show ssh-server	41
show telnet login	42
show users	42
who	43
3 Commands for Configuring Switch IP	43
interface vlan	43
ip address	44
ipv6 address	45
ip bootp-client enable	45
ip dhcp-client enable	46
4 Commands for SNMP	48
rmon enable	48
rmon history	48
rmon event	49
rmon alarm	49
show rmon history	51
show rmon event	51
show rmon event log	52
show rmon alarm	52
clear rmon statistics	52
show private-mib oid	53
show snmp	53
show snmp engineid	54
show snmp group	54
show snmp mib	55
show snmp status	55
show snmp user	56
show snmp view	56
snmp-server community	57
snmp-server enable	58
snmp-server enable traps	58
snmp-server engineid	59
snmp-server group	59
snmp-server host	60
snmp-server securityip	61
snmp-server securityip enable	61
snmp-server trap-source	62
snmp-server user	62
snmp-server view	63
switchport updown notification enable	64
5 Commands for Switch Upgrade	66
copy (FTP)	66
copy (TFTP)	67
ftp-dir	68
ftp-server enable	68
ftp-server timeout	69
ip ftp	69
show ftp	70
show tftp	70
tftp-server enable	71
tftp-server retransmission-number	71
tftp-server transmission-timeout	72
6 Commands for File System	73
cd	73
copy	73
delete	74
dir	74
pwd	75
rename	75
7.Commands for Onvif Configuration	76
onvif server enable	76
onvif detect enable	76
clear onvif detect database	76
8. Commands for Alarm	77

alarm env-humidity	77
alarm env-temp	77
alarm power-consumption	77
alarm sys-temp	78
alarm-input detect-mode	78
alarm-log input	79
alarm-log output	79
alarm-output	79
alarm-output mode	79
alarm-output monitor-mode	80
alarm-input action	81
alarm-output monitor	81
show alarm-info	82

authentication line login.....	25
authentication securityip	26
authentication securityipv6	27
authorization	28
authorization line vty command.....	28
clear line vty <0-31>.....	29
crypto key clear rsa	30
terminal length	30
telnet.....	31
telnet server enable.....	32
telnet-server max-connection	32
ssh-server authentication-retries	32
ssh-server enable	33
ssh-server host-key create rsa.....	33
ssh-server max-connection.....	34
ssh-server timeout	35
show crypto key	35
show ssh-server	35
show telnet login	36
show users.....	36
who.....	37
3 Commands for Configuring Switch IP.....	37
interface vlan.....	37
ip address	38
ipv6 address	39
ip bootp-client enable.....	39
ip dhcp-client enable	40
4 Commands for SNMP	42
rmon enable.....	42
rmon history.....	42
rmon event.....	43
rmon alarm.....	43
show rmon history	45
show rmon event	45
show rmon event log	46
show rmon alarm	46
clear rmon statistics	46
show private-mib oid	47
show snmp	47
show snmp engineid.....	48
show snmp group	48
show snmp mib	49
show snmp status	49
show snmp user.....	50
show snmp view.....	50
snmp-server community.....	51
snmp-server enable	52
snmp-server enable traps.....	52
snmp-server engineid	53

snmp-server group.....	53
snmp-server host	54
snmp-server securityip	55
snmp-server securityip enable.....	55
snmp-server trap-source.....	56
snmp-server user	56
snmp-server view	57
switchport updown notification enable	58
5 Commands for Switch Upgrade	60
copy (FTP)	60
copy (TFTP)	61
ftp-dir	62
ftp-server enable.....	62
ftp-server timeout.....	63
ip ftp	63
show ftp.....	64
show tftp.....	64
tftp-server enable.....	65
tftp-server retransmission-number	65
tftp-server transmission-timeout	66
6 Commands for File System.....	67
cd.....	67
copy.....	67
delete	68
dir	68
pwd.....	69
rename.....	69
7.Commands for Onvif Configuration	70
onvif server enable.....	70
onvif detect enable	70
clear onvif detect database.....	70

1 Commands for Basic Configuration

authentication line

Command	authentication line {console vty web} login {local radius tacacs} no authentication line {console vty web} login	
Parameter	console	Log on the switch through the console serial port
	vty	Log on the switch through the vty(SSH or Telnet)
	web	Log on the switch through the web
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.	
Mode	Global Mode	
Usage Guide	<p>This command can configure the authentication methods for Console, VTY, and Web login separately.</p> <p>The authentication method can be any one or combination of Local, RADIUS and TACACS. Preferences from left to right when the login method is combined configuration.</p> <p>If the user has passed the authentication method, the authentication method of the lower preference is ignored.</p> <p>As long as pass an authentication method, the user can log in.</p> <p>AAA function and RADIUS server should be configured before the RADIUS authentication can be used.</p> <p>If local authentication is configured without configuring a local user, the user will be able to log on to the switch through the console method.</p> <p>They all support the following authentication methods.</p> <p>Local: Use the local user account database for authentication.</p> <p>Tacacs: Authentication using remote Tacas server.</p> <p>Radius: Authentication using remote Radius server.</p> <p>no command restores default authentication.</p>	
Example	<p>Configure Telnet and ssh login methods to Local and RADIUS authentication methods.</p> <p>Switch(config)# authentication line vty login local radius lists</p>	

banner

Command	banner motd<LINE> no banner motd
----------------	---

Parameter	<LINE>	The information displayed when the authentication is successful, length limit from 1 to 512 characters
Default	Do not show the information when the authentication is successful.	
Mode	Global Mode	
Usage Guide	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.	
Example	<p>Display “Welcome” after authentication is successful.</p> <p>Switch(config)# banner motd Welcome</p>	

boot img

Command	boot img <img-file-url> {primary backup}	
Parameter	<img-file-url>	Full path to the img file
	primary	First entry to the img document
	backup	Second entry to the img document
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.	
Mode	admin Mode	
Usage Guide	<p>This command is used to configure the first and second img files used by the switch next boot. The first and second img files can only use .img files stored in switch.</p> <ol style="list-style-type: none"> 1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, 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. 	
Example	<p>Set flash:/nos.img as the second booting IMG file used in the next booting of the switch.</p> <p>Switch#boot img flash:/nos.img backup</p>	

boot startup-config

Command	boot startup-config {NULL <file-url> }	
Parameter	NULL	Use the factory primitive configuration as the next reboot boot configuration
	<file-url>	Is the full path of CFG file used in the next booting.
Default	None.	
Mode	admin Mode	
Usage Guide	<p>This command is used configure the CFG file used in the next booting of the switch.</p> <p>Configure the CFG file used in the next booting can only use .cfg files stored in the switch.</p> <ol style="list-style-type: none"> 1. The file path comprises of three parts: device prefix used as the root directory (flash:/), sub-directory, 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. 	
Example	<p>Set flash:/ startup.cfg as the CFG file used in the next booting of the switch.</p> <p>Switch# boot startup-config flash:/ startup.cfg</p>	

clock set

Command	clock set <HH:MM:SS> <YYYY.MM.DD>	
Parameter	<HH:MM:SS>	Time, HH effective range 0 to 23, MM and SS 0 to 59
	<YYYY.MM.DD>	Year, month and date, and YYYY valid range is 1970 to 2038, MON is month 1 to 12, DD is date 1 to 31
Default	By default, upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.	
Mode	admin Mode	
Usage Guide	<p>This command is used to configure switch system time and date.</p> <p>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.</p>	
Example	<p>To set the switch current date and time to 2002.8.1 23: 0: 0.</p> <p>Switch#clock set 23:0:0 2002.8.1</p>	

config

Command	config [terminal]	
Parameter	[terminal]	indicates terminal configuration
Default	None.	
Mode	admin Mode.	
Usage Guide	This command is used to switch from admin management mode to config global configuration mode.	
Example	Enter config global configuration mode from admin management mode. Switch#config	

disable

Command	disable	
Parameter	none	none
Default	None.	
Mode	admin Mode.	
Usage Guide	This command is used for switch exit admin mode back to general user mode.	
Example	Exit admin mode back to general user mode. Switch#disable Switch>	

enable

Command	enable [<1-15>]	
Parameter	[<1-15>]	User Permission Level

Default	None.
Mode	User mode/ admin mode
Usage Guide	<p>Use enable command to enter Admin Mode from User Mode, or change the privilege level of the users.</p> <p>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.</p> <p>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.</p> <p>Set the Admin user password under Global Mode with "enable password" command.</p>
Example	<p>Enter management mode from user mode.</p> <p>Switch>enable Switch#</p>

enable password

Command	enable password [level <1-15>] [0 7] <password> no enable password [level <1-15>]						
Parameter	<table> <tr> <td>[level <1-15>]</td><td>used to specify the privilege level, the default level is 15</td></tr> <tr> <td>[0 7]</td><td>If enter option 0 on password settings, the password is not encrypted; If enter option 7 on password settings, the password is encrypted</td></tr> <tr> <td><password></td><td>the password for the user</td></tr> </table>	[level <1-15>]	used to specify the privilege level, the default level is 15	[0 7]	If enter option 0 on password settings, the password is not encrypted; If enter option 7 on password settings, the password is encrypted	<password>	the password for the user
[level <1-15>]	used to specify the privilege level, the default level is 15						
[0 7]	If enter option 0 on password settings, the password is not encrypted; If enter option 7 on password settings, the password is encrypted						
<password>	the password for the user						
Default	This password is empty by system default.						
Mode	Global Mode						
Usage Guide	<p>Configure the password used for enter Admin Mode from the User Mode.</p> <p>Configure this password to prevent unauthorized entering Admin Mode.</p> <p>It is recommended to set the password at the initial switch configuration.</p> <p>Also, it is recommended to exit Admin Mode with "exit" command when the administrator needs to leave the terminal for a long time.</p> <p>The "no enable password" command deletes this password.</p>						
Example	<p>Configure the command for general users to enter the admin mode by rule as test.</p> <p>Switch(config)#enable password 0 test</p>						

end

Command	end
Parameter	none none
Default	None.
Mode	Except user mode / admin mode
Usage Guide	This command is used to configure the command for general users to enter the admin mode by rule as test.
Example	Quit VLAN mode and return to Admin mode. Switch(config-vlan1)#end Switch#

exec-timeout

Command	exec-timeout <minutes> [<seconds>] no exec-timeout
Parameter	<minutes> the time value shown in minute and ranges between 0~35791 [<seconds>] the time value shown in seconds and ranges between 0~59
Default	Default timeout is 10 minutes.
Mode	Global mode
Usage Guide	This command is used Configure the timeout of exiting admin mode. Timeout exit admin management mode, need to enter management code and password to enter admin management mode again. When the timeout is set to 0, the timeout timer is disabled. “no exec-timeout”command to restore default values.
Example	Set the admin mode timeout value to 5 minutes, 30 seconds. Switch(config)#exec-timeout 5 30

exit

Command	exit
Parameter	none none
Default	None.
Mode	All Modes
Usage Guide	This command is used quit current mode and return to it's previous mode.
Example	Quit global mode to it's previous mode Switch(config)#exit Switch#

help

Command	help
Parameter	none none
Default	None.
Mode	All 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	Get help in global mode. 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.

hostname

Command	hostname <hostname> no hostname
Parameter	<hostname> the string for the prompt, up to 64 characters are allowed
Default	The default prompt is relative with the switch.
Mode	Global Mode
Usage Guide	Use this command , set the prompt in the switch command line interface. The no operation cancels the configuration.
Example	Set the prompt to “Test”. Switch(config)#hostname Test Test(config)#

ip host

Command	ip host <hostname> <ip_addr> no ip host {<hostname> all}
Parameter	<hostname> the string for the prompt, up to 64 characters are allowed <ip_addr> the corresponding IP address for the host name, takes a dot decimal format all all of the host name
Default	None.
Mode	Global Mode
Usage Guide	By using this command, you can set the mapping relationship between the host and the IP address. Set the association between host and IP address, which can be used in commands like “ping <host>”. The “no ip host” parameter of this command will delete the mapping.
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

<hr/>							
<hr/>							
ipv6 host							
<hr/>							
Command	ipv6 host <hostname> <ipv6_addr> no ipv6 host { <hostname> all}						
Parameter	<table><tr><td><hostname></td><td>the string for the prompt, up to 64 characters are allowed</td></tr><tr><td><ipv6_addr></td><td>the corresponding IPv6 address for the host name, takes a dot decimal format</td></tr><tr><td>all</td><td>all of the host name</td></tr></table>	<hostname>	the string for the prompt, up to 64 characters are allowed	<ipv6_addr>	the corresponding IPv6 address for the host name, takes a dot decimal format	all	all of the host name
<hostname>	the string for the prompt, up to 64 characters are allowed						
<ipv6_addr>	the corresponding IPv6 address for the host name, takes a dot decimal format						
all	all of the host name						
Default	None.						
Mode	Global Mode						
Usage Guide	<p>By using this command, you can set the mapping relationship between the host and the IPv6 address.</p> <p>Set the association between host and IPv6 address, which can be used in commands like “traceroute6 <host>”.</p> <p>The “no ip host” parameter of this command will delete the mapping.</p>						
Example	<p>Set the IPv6 address of the host named beijing to 2001:1:2:3::1.</p> <p>Switch(config)#ipv6 host beijing 2001:1:2:3::1</p>						

<hr/>			
ip http server			
<hr/>			
Command	ip http server no ip http server		
<hr/>			
Parameter	<table><tr><td>none</td><td>none</td></tr></table>	none	none
none	none		
<hr/>			
Default	Enable.		
<hr/>			
Mode	Global Mode		
<hr/>			
Usage Guide	Use this command to enable Web configuration.		
	The “no ip http server” command disables Web configuration.		
<hr/>			
Example	Enable Web Server function and enable Web configurations.		

Switch(config)#ip http server

login

Command	login no login
Parameter	none none
Default	No login by default.
Mode	Global Mode
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

password

Command	password [0 7] <password> no password
Parameter	[0 7] if input option 0 on password setting, the password is not encrypted; if input option 7, the password is encrypted <password> password for the user
Default	This password is empty by system default.
Mode	Global Mode
Usage Guide	With this command, configure the password used for enter normal user mode on the console. The “no password” command deletes this password.
Example	Configure the password used to enter normal user mode as test, password is not encrypted.

Switch(config)#password 0 test

privilege

Command

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

Parameter

mode	register mode of the command, 'Tab, or '?', is able to show all register modes
<1-15>	level, its range between 1 and 15
LINE	the command needs to be configured, it supports the command abbreviation

Default

None.

Mode

Global Mode

Usage Guide

Use this command to configure the permission level for the specified command. This function cannot change the command itself.

LINE must be the whole command format, the command with the abbreviation format must be analyzed successfully.

Can choose to set the level of the NO command, but it does not affect the result.

When using a no command, the LINE must be a configured command line.

If the command line with the parameter, the parameter must be matched with the configured command.

The no command restores the original level of the command.

Example

Change the level of show ip route command to level 5.
Restore the original level of the show ip route command.

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

reload

Command

reload

Parameter

none	none
-------------	------

Default

None.

Mode	Admin Mode
Usage Guide	The user can use this command to restart the switch continuously.
Example	Hot restart switch. Switch(config)#reload

service password-encryption

Command	service password-encryption no service password-encryption
Parameter	none none
Default	No service password-encryption by system default.
Mode	Global Mode
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

service terminal-length

Command	service terminal-length <0-512> no service terminal-length
Parameter	<0-512> Columns of characters displayed on each screen of vty, ranging between 0-512
Default	None.
Mode	Global Mode
Usage Guide	Use this command , configure the columns of characters displayed on each screen of the terminal.

	<p>The columns of characters displayed on each screen on the telnet.ssh client and the Console will be following this configuration.</p> <p>The “no service terminal-length” command cancels the screen shifting operation.</p>
Example	<p>Set the number of vty threads to 20.</p> <p>Switch(config)#service terminal-length 20</p>

sysContact

Command	<p>sysContact <LINE> no sysContact</p>
Parameter	<p><LINE> the prompt character string, range from 0 to 255 characters</p>
Default	<p>The default is factory setting.</p>
Mode	<p>Global Mode</p>
Usage Guide	<p>With this command,the user can set the factory contact mode bases the fact instance.</p> <p>The “no sysContact” command reset the switch to factory settings.</p>
Example	<p>Set the factory contact mode to test.</p> <p>Switch(config)#sysContact test</p>

sysLocation

Command	<p>sysLocation<LINE> no sysLocation</p>
Parameter	<p><LINE> the prompt character string, range from 0 to 255 characters</p>
Default	<p>The default is factory setting.</p>
Mode	<p>Global Mode</p>
Usage Guide	<p>With this command,the user can set the factory address bases the fact instance.</p> <p>The “no sysLocation” command reset the switch to factory settings.</p>

Example	Set the factory address to test.
	Switch(config)#sysLocation test

set default

Command	set default
Parameter	none none
Default	None.
Mode	Admin Mode
Usage Guide	<p>Reset the switch to factory settings.</p> <p>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.</p> <p>Note: After the command, “write” command must be executed to save the operation. The switch will reset to factory settings after restart.</p>
Example	<p>Restore factory settings and restart.</p> <p>Switch#set default Are you sure? [Y/N] = y</p> <p>Switch#write</p> <p>Switch#reload</p>

set boot password

Command	set boot password no set boot password
Parameter	none none
Default	None.
Mode	Global Mode
Usage Guide	<p>Under the img mode, configure the password of entering the bootrom mode next time; under the global mode, input this command and the password according to the prompt and confirm it, then successfully to configure.</p>

Notice: the characters length of the password is from 3 to 32.

The no command cancels the password.

Example

Sets the password when entering boot mode.

Switch(config)#set boot password

New password :*****

Confirm password :*****

Set password success!

setup

Command

setup

Parameter

none	none
-------------	------

Default

None.

Mode

Admin Mode

Usage Guide

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

Example

Enter setup mode.

Switch#setup

show clock

Command

show clock

Parameter

none	none
-------------	------

Default

None.

Mode

Admin Mode.

Usage Guide

Displays the current system clock.

Example

Displays the current system clock.

Switch#show clock

show cpu usage

Command	show cpu usage [<slotno>]	
Parameter	[<slotno>]	Specify slots
Default	None.	
Mode	Admin and configuration mode	
Usage Guide	Display current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage by this 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%	

show cpu utilization

Command	show cpu utilization	
Parameter	none	none
Default	None.	
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	Displays CPU utilization. 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%

show memory usage

Command	show memory usage [<slotno>]	
Parameter	[<slotno>]	Specify slots
Default	None.	
Mode	Admin Mode	
Usage Guide	Show memory usage rate. 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%	

show privilege

Command	show privilege	
Parameter	none	none
Default	None.	
Mode	Global Mode	
Usage Guide	Show privilege of the current user.	
Example	Show privilege of the current user. Switch(config)#show privilege Current privilege level is 15	

show privilege mode LINE

Command	show privilege mode LINE	
Parameter	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
Default	None.	
Mode	Admin mode/Global mode	
Usage Guide	<p>Show the level of the specified command.</p> <p>LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully.</p> <p>For half-baked command, false</p> <p>command about writing and command that abbreviation cannot be analyzed successfully, the level of them cannot be shown.</p>	
Example	<p>Show the level of privilege command.</p> <p>Switch(config)#show privilege exec show ip route</p> <p>The command : show ip route</p> <p>Privilege is : 15</p>	

show tech-support

Command	show tech-support [no-more]	
Parameter	[no-more]	Display the operational information and the task status of the switch directly, do not connect the user by "more".
Default	None.	
Mode	Admin mode/Global mode	
Usage Guide	<p>This command is used to collect the relative information when the switch operation is malfunctioned.</p> <p>Display the operational information and the task status of the switch.</p> <p>The technique specialist use this command to diagnose whether the switch operate normally.</p>	
Example	Displays the operational information and the task status of the switch.	

Switch#show tech-support

show version

Command	show version
Parameter	none none
Default	None.
Mode	Admin mode/Global 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	Display the version information of the switch. Switch#show version

username

Command	username <username> [privilege <privilege>] [password [0 7]<password>] no username <username>								
Parameter	<table><tr><td><username></td><td>the username, its range should not exceed 32 characters</td></tr><tr><td><privilege></td><td>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</td></tr><tr><td>[0 7]</td><td>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)</td></tr><tr><td><password></td><td>password for the user</td></tr></table>	<username>	the username, its range should not exceed 32 characters	<privilege>	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	[0 7]	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)	<password>	password for the user
<username>	the username, its range should not exceed 32 characters								
<privilege>	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								
[0 7]	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)								
<password>	password for the user								
Default	None.								
Mode	Global Mode								
Usage Guide	Configure local login username and password along with its privilege level. 16 local users at most can be configured through this command, and the maximum length of the password should be no less than 32. 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.

The no command delete user.

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.

```
Switch(config)#username admin privilege 15 password 0 admin
Switch(config)# username user1 privilege 1 password 7
4a7d1ed414474e4033ac29ccb8653d9b
Switch(config)# username user2 password 0 user2
Switch(config)# authentication line console login local
```

web-auth privilege <1-15>

Command

web-auth privilege <1-15>
no web-auth privilege

Parameter

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

Default

The default level is 15.

Mode

Global Mode

Usage Guide

Configure the level of logging in the switch by web.
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
```

write

Command

write

Parameter

none	none
-------------	------

Default	None.
Mode	Admin Mode
Usage Guide	<p>Save the currently configured parameters to the Flash memory.</p> <p>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.</p>
Example	<p>Save the current configuration.</p> <p>Switch#write</p>

write running-config

Command	write running-config [<startup-config-file-name>]
Parameter	[<startup-config-file-name>] the full path of the cfg file
Default	None.
Mode	Admin Mode
Usage Guide	<p>Save the current running config as .cfg file to Flash Memory.</p> <p>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.</p> <p>The suffix of all file names should be .cfg.</p> <p>The length of the full file path should not be longer than 128 characters, while the file name cannot be longer than 80 characters.</p>
Example	<p>Save the current running config as .cfg file with name of 123.</p> <p>Switch#write running-config 123.cfg</p>

2 Commands for Telnet

aaa authorization config-commands

Command	aaa authorization config-commands no aaa authorization config-commands	
Parameter	none	none
Default	By default,disable.	
Mode	Global Mode	
Usage Guide	Enable command authorization function for the login user with VTY (login with Telnet and SSH). Only enabling this command and configuring command authorization manner, it will request to authorize when executing some command. The no command disables this function.	
Example	Enable VTY command authorization function. Switch(config)#aaa authorization config-commands	

accounting exec

Command	accounting line {console vty} exec {start-stop stop-only none} method1 [method2...] no accounting line {console vty} exec	
Parameter	console	log in through serial port
	vtty	log in through telnet or 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	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
Default	By default there is no accounting.	
Mode	Global Mode	
Usage Guide	Configure the list of the accounting method for the login user with VTY (login with Telnet and SSH) and Console.	

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

The no command restores the default accounting method.

Example Configure the login accounting with the telnet method.

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

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>

Parameter	console	log in through serial port
	vtty	log in through telnet or ssh
	command <1-15>	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	the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count

Default By default there is no accounting method.

Mode Global Mode

Usage Guide 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.

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.

The no command restores the default accounting method.

Example Configure command audit methods through telnet login, command level 15.

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

authentication enable

Command	authentication enable method1 [method2...] no authentication enable	
Parameter	method	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.	
Mode	Global Mode	
Usage Guide	<p>Configure the list of the enable authentication method.</p> <p>The enable authentication method can be any one or combination of Local,RADIUS and TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right.</p> <p>If the users have passed the authentication method, authentication method of lower preferences will be ignored.</p> <p>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.</p> <p>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.</p> <p>The no command restores the default authentication method.</p>	
Example	<p>Configure the enable authentication method to be tacacs and local.</p> <p>Switch(config)#authentication enable tacacs local</p>	

authentication ip access-class

Command	authentication ip access-class {<num-std> <name>} no authentication ip access-class	
Parameter	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string

	length is ranging between 1 and 64
Default	The binding ACL to Telnet/SSH/Web function is closed by default.
Mode	Global Mode
Usage Guide	Binding standard IP ACL protocol to login with Telnet/SSH/Web. The no form command will cancel the binding ACL.
Example	Binding standard IP ACL protocol to access-class 1. Switch(config)#authentication ip access-class 1 in

authentication ipv6 access-class

Command	authentication ipv6 access-class {<num-std> <name>} no authentication ipv6 access-class				
Parameter	<table> <tr> <td><num-std></td><td>the access-class number for standard numeric ACL, ranging between 500-599</td></tr> <tr> <td><name></td><td>the access-class name for standard ACL, the character string length is ranging between 1 and 64</td></tr> </table>	<num-std>	the access-class number for standard numeric ACL, ranging between 500-599	<name>	the access-class name for standard ACL, the character string length is ranging between 1 and 64
<num-std>	the access-class number for standard numeric ACL, ranging between 500-599				
<name>	the access-class name for standard ACL, the character string length is ranging between 1 and 64				
Default	The binding ACL to Telnet/SSH/Web function is closed by default.				
Mode	Global Mode				
Usage Guide	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web. The no form command will cancel the binding ACL.				
Example	Binding standard IP ACL protocol to access-class 500. Switch(config)#authentication ipv6 access-class 500 in				

authentication line login

Command	authentication line {console vty web} login method1 [method2...] no authentication line {console vty web} login		
Parameter	<table> <tr> <td>console</td><td>log in through serial port</td></tr> </table>	console	log in through serial port
console	log in through serial port		

vty	log in through telnet or ssh
web	log in through web
method	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.
Mode	Global Mode
Usage Guide	<p>Configure VTY (login with Telnet and SSH), Web and Console, so as to select the list of the authentication method for the login user.</p> <p>Authentication method can be any one or combination of Local, RADIUS and TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right.</p> <p>If the users have passed the authentication method, authentication method of lower preferences will be ignored.</p> <p>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);</p> <p>it will attempt the next authentication method if it receives nothing.</p> <p>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.</p> <p>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.</p> <p>If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.</p> <p>The no form command restores the default authentication method.</p>
Example	<p>Configure the telnet and ssh login with the remote RADIUS authentication.</p> <p>Switch(config)#authentication line vty login radius</p>

authentication securityip

Command	authentication securityip <ip-addr> no authentication securityip <ip-addr>
----------------	---

Parameter	<ip-addr> 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.
Mode	Global Mode
Usage Guide	<p>To configure the trusted IP address for Telnet and HTTP login method.</p> <p>IP address of the client which can login the switch is not restricted before the trusted IP address is not configured.</p> <p>After the trusted IP address is configured, only clients with trusted IP addresses are able to login the switch.</p> <p>Up to 32 trusted IP addresses can be configured in the switch.</p> <p>The no form of this command will remove the trusted IP address configuration.</p>
Example	<p>To configure 192.168.1.21 as the trusted IP address.</p> <p>Switch(config)#authentication securityip 192.168.1.21</p>

authentication securityipv6

Command	authentication securityipv6 <ipv6-addr> no authentication securityipv6 <ipv6-addr>
Parameter	<ip-addr> the security IPv6 address which can login the switch
Default	No security IPv6 addresses are configured by default.
Mode	Global Mode
Usage Guide	<p>To configure the security IPv6 address for Telnet and HTTP login method.</p> <p>IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured.</p> <p>After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login the switch.</p> <p>Up to 32 security IPv6 addresses can be configured in the switch.</p> <p>The no form of this command will remove the specified configuration.</p>
Example	<p>Configure the security IPv6 address is 2001:da8:123:1::1.</p> <p>Switch(config)#authentication securityipv6 2001:da8:123:1::1</p>

authorization

Command	authorization line {console vty web} exec method [method...] no authorization line {console vty web} exec	
Parameter	console	log in through serial port
	vty	log in through telnet or ssh
	web	log in through web
	method	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	There is no authorization method by default.	
Mode	Global Mode	
Usage Guide	<p>Configure the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console.</p> <p>And authorization method can be any one or combination of Local,RADIUS or TACACS.</p> <p>When login method is configuration in combination, the preference goes from left to right.</p> <p>If the users have passed the authorization method, authorization method of lower preferences will be ignored.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The no command restores the default authorization method.</p>	
Example	<p>Configure the telnet authorization method to RADIUS.</p> <p>Switch(config)#authorization line vty exec radius</p>	

authorization line vty command

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

no authorization line vty command <1-15>

Parameter	command <1-15>	Level scope of authorization orders 1~15
	local	Authorization is granted locally
	radius	Authorization for remote radius
	tacacs	Authorization for remote tacacs
	none	Authorization mode is empty
<hr/>		
Default	The authorization manner is not configured as default.	
<hr/>		
Mode	Global Mode	
<hr/>		
Usage Guide	<p>Configure command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH).</p> <p>The enabling authorization method can be any one or combination of Local. RADIUS and TACACS.</p> <p>When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order.</p> <p>If the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored.</p> <p>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.</p> <p>When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. when using TACACS authorization, TACACS server must be configured.</p> <p>None is the manner of escaping and it only can be the last manner.</p> <p>This manner returns to passed authorization directly and it is successful to configure the command.</p> <p>The no command recovers to be default manner.</p>	
<hr/>		
Example	Configure level 1 command authorization manner of telnet login user as TACACS.	
<hr/>		
Switch(config)#authorization line vty command 1 tacacs		

clear line vty <0-31>

Command	clear line vty <0-31>	
Parameter	<0-31>	appointed line
Default	None.	
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.
Example	Admin users who are forced to log in through VTY (using Telnet or SSH login) are offline. Switch#clear line vty 0 Confirm[Y/N]:y [OK]

crypto key clear rsa

Command	crypto key clear rsa	
Parameter	none	none
Default	None.	
Mode	Admin Mode	
Usage Guide	This command is used to clear the secret key ofthe ssh and close the ssh service.	
Example	Clear the secret key ofthe ssh and close the ssh service. Switch#crypto key clear rsa ssh host key is cleared successfully. ssh is closed successfully.	

terminal length

Command	terminal length <0-512> terminal no length	
Parameter	<0-512>	Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display)
Default	Default Length is 25.	
Mode	Admin Mode	
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	

	<p>any key to show information in next screen.</p> <p>The “terminal no length” cancels the screen switching operation and display content once in all.</p>										
Example	<p>Configure length of characters in each display to 20.</p> <p>Switch#terminal length 20</p>										
telnet											
Command	telnet [vrf<vrf-name>] [<ip-addr> <ipv6-addr> host <hostname>][<port>]										
Parameter	<table> <tr> <td><vrf-name></td><td>the specific VRF name</td></tr> <tr> <td><ip-addr></td><td>the IP address of the remote host, shown in dotted decimal notation</td></tr> <tr> <td><ipv6-addr></td><td>the IPv6 address of the remote host</td></tr> <tr> <td><hostname></td><td>the name of the remote host, containing max 64 characters</td></tr> <tr> <td><port></td><td>the port number, ranging between 0 and 65535</td></tr> </table>	<vrf-name>	the specific VRF name	<ip-addr>	the IP address of the remote host, shown in dotted decimal notation	<ipv6-addr>	the IPv6 address of the remote host	<hostname>	the name of the remote host, containing max 64 characters	<port>	the port number, ranging between 0 and 65535
<vrf-name>	the specific VRF name										
<ip-addr>	the IP address of the remote host, shown in dotted decimal notation										
<ipv6-addr>	the IPv6 address of the remote host										
<hostname>	the name of the remote host, containing max 64 characters										
<port>	the port number, ranging between 0 and 65535										
Default	None.										
Mode	Admin Mode										
Usage Guide	<p>This command is used when the switch is applied as Telnet client, for logging on remote host to configure.</p> <p>When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host.</p> <p>To connect to another remote host, the current TCP connection must be disconnected with a hotkey “CTRL+ \”.</p> <p>To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured.</p> <p>For required commands please refer to ip host and ipv6 host.</p> <p>In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telnetting this host name.</p>										
Example	<p>The switch telnets to a remote host whose IP address is 20.1.1.1.</p> <p>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></p>										

telnet server enable

Command	telnet server enable no telnet server enable
Parameter	none none
Default	Telnet server function is enabled by default.
Mode	Global Mode
Usage Guide	<p>Enable the Telnet server function in the switch</p> <p>This command is available in Console only.</p> <p>The administrator can use this command to enable or disable the Telnet client to login to the switch.</p> <p>The “no telnet server enable”command disables the Telnet function in the switch.</p>
Example	<p>Disable the Telnet server function in the switch.</p> <p>Switch(config)#no telnet server enable</p>

telnet-server max-connection

Command	telnet-server max-connection {<max-connection-number> default}
Parameter	<max-connection-number> the max connection number supported by the Telnet service, ranging from 1 to 16 default restore the default configuration
Default	The system default value of the max connection number is 5.
Mode	Global Mode
Usage Guide	Configure the max connection number supported by the Telnet service of the switch.
Example	<p>Set the max connection number supported by the Telnet service as 10.</p> <p>Switch(config)#telnet-server max-connection 10</p>

ssh-server authentication-retries

Command	ssh-server authentication-retries <authentication-retries> no ssh-server authentication-retries
Parameter	<authentication-retries> the number of times for retrying authentication, valid range is 1 to 10
Default	The number of times for retrying SSH authentication is 3 by default.
Mode	Global Mode
Usage Guide	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.
Example	Set the time for retrying SSH authentication to 5. Switch(config)#ssh-server authentication-retries 5

ssh-server enable

Command	ssh-server enable no ssh-server enable
Parameter	none none
Default	SSH function is disabled by default.
Mode	Global Mode
Usage Guide	Enable SSH function on the switch. 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. The “no ssh-server enable” command disables SSH function.
Example	Enable SSH function on the switch. Switch(config)#ssh-server enable

ssh-server host-key create rsa

Command	ssh-server host-key create rsa [modulus < modulus >]
Parameter	<div> <div>< modulus ></div> <div>the modulus which is used to compute the host key; valid range is 768 to 2048. The default value is 1024</div> </div>
Default	The system uses the key generated when the ssh-server is started at the first time.
Mode	Global Mode
Usage Guide	<p>This command is used to generate a new SSH service host rsa key.</p> <p>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.</p> <p>No command disables SSH service.</p>
Example	<p>Generate new host key.</p> <p>Switch(config)#ssh-server host-key create rsa</p>

ssh-server max-connection

Command	ssh-server max-connection {<max-connection-number> default}
Parameter	<div> <div><max-connection-number></div> <div>the max connection number supported by the SSH service, ranging from 1 to 16.</div> </div> <div> <div>default</div> <div>restore default</div> </div>
Default	The system default value of the max connection number is 5.
Mode	Global Mode
Usage Guide	Configure the max connection number supported by the SSH service of the switch.
Example	<p>Set the max connection number supported by the SSH service as 10.</p> <p>Switch(config)#ssh-server max-connection 10</p>

ssh-server timeout

Command	ssh-server timeout <timeout> no ssh-server timeout
Parameter	<timeout> timeout value; valid range is 10 to 600 seconds
Default	SSH authentication timeout is 180 seconds by default.
Mode	Global Mode
Usage Guide	Configure timeout value for SSH authentication. The “no ssh-server timeout” command restores the default timeout value for SSH authentication.
Example	Set SSH authentication timeout to 240 seconds. Switch(config)#ssh-server timeout 240

show crypto key

Command	show crypto key
Parameter	none none
Default	None.
Mode	Admin Mode
Usage Guide	Show the secret key of ssh.
Example	Show the secret key of ssh. Switch#show crypto key

show ssh-server

Command	show ssh-server
Parameter	none none

Default	None.
Mode	Admin Mode
Usage Guide	Display SSH state and users which log on currently.
Example	<p>Display SSH state and users which log on currently.</p> <pre> 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 </pre>

show telnet login

Command	show telnet login
Parameter	none none
Default	None.
Mode	Admin Mode
Usage Guide	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.
Example	<p>Display Telnet client information.</p> <pre> Switch#show telnet login Authenticate login by local Login user: aa </pre>

show users

Command	show users
Parameter	none none
Default	None.

Mode	Admin Mode															
Usage Guide	<p>Show the user information who logs in through telnet or ssh. It includes line number, user name and user IP.</p> <p>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.</p>															
Example	<p>Displays user information.</p> <p>Switch#show users</p> <table><tr><td>Line</td><td>User</td><td>Location</td></tr><tr><td>vty 16</td><td>a</td><td>192.168.1.1</td></tr><tr><td>vty 0</td><td>admin</td><td>192.168.1.2</td></tr><tr><td>vty 17</td><td>mab</td><td>192.168.1.13</td></tr><tr><td>vty 1</td><td>test</td><td>192.168.1.40</td></tr></table>	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
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														

who

Command	who
Parameter	none none
Default	None.
Mode	All configuration modes
Usage Guide	Show the current login users with vty.
Example	<p>Show the current login users with vty.</p> <pre>Switch#who</pre> <p>Telnet user a login from 192.168.1.20</p>

3 Commands for Configuring Switch IP

interface vlan

Command	interface vlan <vlan-id> no interface vlan <vlan-id>
Parameter	<vlan-id> the VLAN ID of an existing VLAN, ranging from 1 to 4094

Default	None.						
Mode	Global Mode						
Usage Guide	<p>This command is used enter the VLAN interface configuration mode</p> <p>Users should first make sure the existence of a VLAN before configuring it.</p> <p>User “exit” command to quit the VLAN interface configuration mode back to the global configuration mode.</p> <p>the no operation of this command will delete the existing VLAN interface.</p>						
Example	<p>Enter the VLAN interface configuration mode of VLAN1.</p> <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#</pre>						
ip address							
Command	<pre>ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>] [secondary]</pre>						
Parameter	<table> <tr> <td><ip-address></td><td>the IP address in dot decimal format</td></tr> <tr> <td><mask></td><td>the subnet mask in dot decimal format</td></tr> <tr> <td>[secondary]</td><td>indicates the IP configured is a secondary IP address</td></tr> </table>	<ip-address>	the IP address in dot decimal format	<mask>	the subnet mask in dot decimal format	[secondary]	indicates the IP configured is a secondary IP address
<ip-address>	the IP address in dot decimal format						
<mask>	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.						
Mode	VLAN Interface Mode						
Usage Guide	<p>Set the IP address and mask for the specified VLAN interface.</p> <p>A VLAN interface must be created first before the user can assign an IP address to the switch.</p> <p>The no command deletes the specified IP address setting.</p>						
Example	<p>Set 10.1.128.1/24 as the IP address of VLAN1 interface.</p> <pre>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)#</pre>						

ipv6 address

Command	ipv6 address <ipv6address prefix-length> [eui-64] no ipv6 address <ipv6address prefix-length> [eui-64]						
Parameter	<table><tr><td><ipv6address></td><td>the prefix of an IPV6 address</td></tr><tr><td><prefix-length></td><td>the length of the prefix of an IPV6 address, ranging from 3 to 128</td></tr><tr><td>[eui-64]</td><td>means that the eui64 interface id of the interface will automatically create an IPV6 address</td></tr></table>	<ipv6address>	the prefix of an IPV6 address	<prefix-length>	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
<ipv6address>	the prefix of an IPV6 address						
<prefix-length>	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						
Default	No IPv6 address is configured upon switch shipment.						
Mode	VLAN Interface Mode						
Usage Guide	<p>Configure aggregatable global unicast address, site-local address and link-local address for the interface.</p> <p>The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage.</p> <p>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.</p> <p>The no command deletes the specified IPv6 address setting.</p>						
Example	<p>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.</p> <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ipv6 address 2001:3f:ed8::99/64 Switch(Config-if-Vlan1)#exit Switch(config)#</pre>						

ip bootp-client enable

Command	ip bootp-client enable no ip bootp-client enable		
Parameter	<table><tr><td>none</td><td>none</td></tr></table>	none	none
none	none		
Default	BootP client function is disabled by default.		
Mode	VLAN Interface Mode		

Usage Guide	<p>Enable the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation.</p> <p>Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed.</p> <p>To obtain IP address via BootP, a DHCP server or a BootP server is required in the network.</p> <p>The no command disables the BootP Client function and releases the IP address obtained in BootP.</p>
Example	<p>Get IP address through BootP.</p> <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip bootp-client enable Switch(Config-if-Vlan1)#exit Switch(config)#</pre>

ip dhcp-client enable

Command	<p>ip dhcp-client enable</p> <p>no ip dhcp-client enable</p>
Parameter	<p>none none</p>
Default	By default, the dhcp service is disabled.
Mode	VLAN Interface Mode
Usage Guide	<p>Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation.</p> <p>To obtain IP address via DHCP, a DHCP server is required in the network.</p> <p>Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.</p> <p>The no command disables the DHCP client function and releases the IP address obtained in DHCP.</p>
Example	<p>Getting an IP address through DHCP.</p> <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)#ip dhcp-client enable Switch(Config-if-Vlan1)#exit Switch(config)#</pre>

4 Commands for SNMP

rmon enable

Command	rmon enable no rmon enable	
Parameter	none	none
Default	RMON is enabled by default.	
Mode	Global Mode	
Usage Guide	This command is used to enable RMON remote network monitoring protocol. The no command disables RMON.	
Example	Disable RMON. Switch(config)#no rmon enable	

rmon history

Command	rmon history history-id interface (ethernet IFNAME IFNAME) ((buckets <1-65535>) (interval <1-3600>) (owner WORD)) no rmon history history-id	
Parameter	history-id	Specify RMON History Control Entry ID, valid range is : <1-65535>
	ethernet IFNAME	IFNAME is the name of the interface, for example 1/0/1
	IFNAME	IFNAME is the name of the interface, for example ethernet1/0/1
	buckets	The maximum number of entries for storing sampling statistics results
	interval	Sampling interval time, unit:s/second
	owner	Specify the user requesting RMON information (optional parameter), valid range is: <1-31> character
Default	Buckets default 50 Interval default 1800	
Mode	Global Mode	
Usage Guide	This command can regularly collect data from the specified port and save the collected information in a history table for future reference. no rmon history <1-65535> Delete configured RMON history control	
Example	Add or modify RMON history control. Switch(config)#rmon history 1 interface ethernet 1/0/1 buckets 5 interval 50	

rmon event

Command	rmon event event-id ((log log trap WORD) (description WORD) (trap WORD) (owner WORD)) no rmon event event-id	
Parameter	event-id Specify RMON event control entry ID, valid range is: <1-65535> log Generate event logs trap Generate alarms for events log trap Simultaneously generating event logs and alarms WORD Specify the group name. valid range is: <1-127> character description Specify the description information of the event (optional parameter), valid range is: <1-127> character owner Specify the user requesting RMON information (optional parameter), valid range is: <1-31> character	
Default	Default, no event triggered.	
Mode	Global Mode	
Usage Guide	This command is used when an event exceeds the alarm threshold, and the device can record logs or generate alarms, or both.	
Example	no rmon event <1-65535> Delete configured RMON events Configure simultaneous logging and alarm generation. Switch(config)# rmon event 1 log trap rw	

rmon alarm

Command	rmon alarm alarm-id interface(ethernet IFNAME IFNAME) counter sample { absolute delta }rising rising-threshold rising-event falling falling-threshold falling-event startup {rising falling rising-falling} [owner owner] no rmon alarm alarm-id	
Parameter	alarm-id Specify RMON alarm entry ID, valid range is: <1-65535> ethernet IFNAME IFNAME is the name of the interface, for example 1/0/1 IFNAME IFNAME is the name of the interface, for example ethernet1/0/1 counter The specified counter type, include (broadcast-pkts、collisions、crc-align-errors、drop-events、fragments、jabbers、multicast-pkts、octets、oversize-pkts、pkts、pkts1024to1518octets、pkts128to255octets、pkts256to511octets、pkts512to1023octets、pkts64octets、	

	pkts65to127octets 、undersize-pkts)
Sample	Specify the alarm query time interval, valid range is: <1-2147483647>
{ absolute delta }	None
rising-threshold	Specify rise threshold , valid range is: <1-2147483647>
rising-event	Specify the ascending event entry number , valid range is: <1-65535>
falling-threshold	Specify descent threshold , valid range is: <1-2147483647>
falling-event	Specify the descent event entry number, valid range is: <1-65535>
{rising falling rising-falling}	Rising:rising trigger event, falling:descent trigger event , rising-falling: Both rising and falling will trigger events
owner	Specify the user requesting RMON information (optional parameter), valid range is: <1-31> character

Default	None.
Mode	Global Mode

Usage Guide	<ol style="list-style-type: none"> 1. This command is used to configure RMON, which can monitor the specified alarm variables at a specified sampling interval. When the value of the monitored data exceeds the defined threshold, an alarm event will be generated. 2. absolute: Absolute value sampling refers to the device obtaining the values of alarm nodes at sampling intervals, and directly comparing the values of alarm nodes or calculated values with the upper and lower thresholds to trigger corresponding events. 3. delta: Change value sampling: The device samples alarm nodes according to the sampling interval and subtracts the value obtained from the previous sampling time point from the current sampling time point to obtain the change value of the alarm node within the sampling interval. The change value of the alarm node or the calculated value is directly compared with the upper and lower threshold to trigger the corresponding event. 4. The set up threshold must be greater than the down threshold. 5. Rising: Rising trigger event, when the value of the alarm variable is greater than or equal to the upper limit threshold, a upper limit alarm event is triggered; 6. Falling: Descent trigger event, When the value of the alarm variable is less than or equal to the lower limit threshold, a lower limit alarm event is triggered. When the value of the alarm variable is greater than or equal to the upper limit threshold, a upper limit alarm event is triggered; rising-falling: Both rising and falling events will trigger events, and the calculated values will be compared with the configured upper and lower thresholds to trigger the corresponding events. The rising and falling events will be triggered alternately. 7. This configuration requires first enabling snmp server and configuring RMON events 8. no rmon alarm <1-65535> Delete the configured RMON alarm entry.
--------------------	---

Example	<p>Configure rising trigger event alarms.</p> <pre> Switch(config)#snmp-server enable Switch(config)#rmon event 1 log Switch(config)# rmon alarm 1 interface ethernet 1/0/1 broadcast-pkts 10 absolute rising 2000 1 falling 200 1 startup rising </pre>
----------------	--

show rmon history

Command	show rmon history history-id statistic show rmon history history-id show rmon history all	
Parameter	statistic history-id all	Viewing RMON Statistical Table Information Specify RMON History Control Entry ID, valid range is: <1-65535> View configuration information for all historical control entries in RMON
Default	None.	
Mode	Global Mode	
Usage Guide	<ol style="list-style-type: none">1. when the RMON function is not working properly and needs to be viewed, debugged, or located, this operation can be used.2. show rmon history history-id statistic view statistical information for RMON history control entries3. show rmon history history-id view configuration information for RMON historical control entries	
Example	View statistical information for RMON history control entries. Switch(config)#show rmon history 1 statistic	

show rmon event

Command	show rmon event event -id show rmon event all	
Parameter	event -id all	Specify RMON event control entry ID, valid range is: <1-65535> View configuration information for all event control entries in RMON
Default	None.	
Mode	Global Mode	
Usage Guide	This command is used to view configuration information for event control entries.	
Example	View the configuration information of the RMON specified event control entry. Switch(config)#show rmon event 1	

show rmon event log

Command	show rmon event event -id log	
Parameter	event -id log	Specify RMON event control entry ID, valid range is: <1-65535> Generate event logs
Default	None.	
Mode	Global Mode	
Usage Guide	This command is used to view the log of events generated by the specified event entry.	
Example	View the log of events generated by the specified event entry. Switch(config)#show rmon event 1 log	

show rmon alarm

Command	show rmon alarm alarm-id show rmon alarm all	
Parameter	alarm-id all	Specify RMON alarm entry ID, valid range is: <1-65535> View the configuration information of all RMON alarm control entries
Default	None.	
Mode	Global Mode	
Usage Guide	This command is used to view the configuration information of the RMON alarm control entry.	
Example	View the configuration information of the specified RMON alarm control entry. Switch(config)#show rmon alarm 1	

clear rmon statistics

Command	clear rmon statistics interface (ethernet IFNAME IFNAME)	
Parameter	ethernet IFNAME IFNAME	IFNAME is the name of the interface, for example 1/0/1 IFNAME is the name of the interface, for example ethernet1/0/1
Default	None.	
Mode	Admin Mode	

Usage Guide	This command is used to clear interface RMON statistics table information.
Example	Clear RMON statistics table information for interface ethernet 1/0/1. Switch(config)#clear rmon statistics interface ethernet 1/0/24

show private-mib oid

Command	show private-mib oid
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Show the original oid of the private mib. 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

show snmp

Command	show snmp
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display all SNMP counter information.
Example	Display all SNMP counter information. 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

show snmp engineid

Command	show snmp engineid
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the engine ID commands.
Example	Display the engine ID commands. Switch#show snmp engineid SNMP engineID:3138633303f1276c

show snmp group

Command	show snmp group
Parameter	none none
Default	None.
Mode	Admin and configuration mode

Usage Guide	Display the group information .
Example	Display the group information . Switch#show snmp group Group Name:initial Security Level:noAuthnoPriv Read View:one Write View:<no writeview specified> Notify View:one

show snmp mib

Command	show snmp mib
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display all MIB supported by the switch.
Example	Display all MIB supported by the switch. Switch#show snmp mib

show snmp status

Command	show snmp status
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display SNMP configuration information.
Example	Display SNMP configuration information. Switch#show snmp status Trap enable

RMON enable
Community Information:
V1/V2c Trap Host Information:
V3 Trap Host Information:
Security IP Information:

show snmp user

Command	show snmp user
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the user information commands.
Example	Display the user information commands. Switch#show snmp user User name: initialsha Engine ID: 1234567890 Auth Protocol:MD5 Priv Protocol:DES-CBC Row status:active

show snmp view

Command	show snmp view
Parameter	none none
Default	None.
Mode	Admin and configuration mode
Usage Guide	Display the view information.
Example	Display the view information. Switch#show snmp view View Name :readview 1. -Included active

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 {ro rw} {0 7} <string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]	
Parameter	{ro rw}	the specified access mode to MIB, ro for read-only and rw for read-write
	{0 7}	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
	<string>	the configured community string
	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
	<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
	<read-view-name>	the name of readable view which includes 1-32 characters
	<write-view-name>	the name of writable view which includes 1-32 characters
Default	None.	
Mode	Global Mode	
Usage Guide	<p>Configure the community string for the switch.</p> <p>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.</p> <p>The no command deletes the configured community string.</p>	
Example	<p>Add a community string named “private” with read-write permission.</p> <p>Switch(config)#snmp-server community rw 0 private</p> <p>Delete the community string named “private”.</p> <p>Switch(config)#no snmp-server community 0 private</p>	

snmp-server enable

Command	snmp-server enable no snmp-server enable	
Parameter	none	none
Default	None.	
Mode	Global Mode	
Usage Guide	<p>Enable the SNMP proxy server function on the switch.</p> <p>To perform configuration management on the switch with network manage software, the SNMP proxy server function has to be enabled with this command.</p> <p>The “no snmp-server enable” command disables the SNMP proxy server function.</p>	
Example	<p>Enable the SNMP proxy server function on the switch.</p> <p>Switch(config)#snmp-server enable</p>	

snmp-server enable traps

Command	snmp-server enable traps no snmp-server enable traps	
Parameter	none	none
Default	By default forbid to send Trap message.	
Mode	Global Mode	
Usage Guide	<p>Enable the switch to send Trap message.</p> <p>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.</p> <p>The no command disables the switch to send Trap message.</p>	
Example	<p>Enable to send Trap messages.</p> <p>Switch(config)#snmp-server enable traps</p>	

snmp-server engineid

Command	snmp-server engineid <engine-string> no snmp-server engineid	
Parameter	<engine-string>	the engine ID shown in 1-32 digit hex characters
Default	Default value is the company ID plus local MAC address.	
Mode	Global Mode	
Usage Guide	Configure the engine ID. The “no” form of this command restores to the default engine ID.	
Example	Set current engine ID to A66688999F Switch(config)#snmp-server engineid A66688999F	

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>}]	
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>	the access-class number for standard numeric ACL, ranging between 1-99
	<name>	the access-class name for standard ACL, the character string length is ranging between 1-32
	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599
	<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
Default	None.	

Mode	Global Mode
Usage Guide	<p>This command is used to configure a new group.</p> <p>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.</p> <p>The “no” form of this command deletes this group.</p>
Example	<p>Create a group CompanyGroup, with the safety level of recognizing and encrypting, the read viewname is readview, and the writing is disabled.</p> <p>Switch (config)#snmp-server group CompanyGroup AuthPriv read readview</p>

snmp-server host

Command	<pre>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></pre>														
Parameter	<table> <tr> <td><host-ipv4-address></td><td>IP address of NMS management station which receives Trap message</td></tr> <tr> <td><host-ipv6-address></td><td>IPv6 address of NMS management station which receives Trap message</td></tr> <tr> <td>v1 v2c v3</td><td>the version number when sending the trap</td></tr> <tr> <td>NoauthNopriv</td><td>Applies the non recognizing and non encrypting safety level</td></tr> <tr> <td>AuthNopriv</td><td>Applies the recognizing but non encrypting safety level</td></tr> <tr> <td>AuthPriv</td><td>Applies the recognizing and encrypting safety level</td></tr> <tr> <td><user-string></td><td>the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3</td></tr> </table>	<host-ipv4-address>	IP address of NMS management station which receives Trap message	<host-ipv6-address>	IPv6 address of NMS management station which receives Trap message	v1 v2c v3	the version number when sending the trap	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	<user-string>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3
<host-ipv4-address>	IP address of NMS management station which receives Trap message														
<host-ipv6-address>	IPv6 address of NMS management station which receives Trap message														
v1 v2c v3	the version number when sending the trap														
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														
<user-string>	the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3														
Default	None.														
Mode	Global Mode														
Usage Guide	<p>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.</p> <p>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</p>														

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.

The “no” form of this command cancels this IPv4 or IPv6 address.

Example	Configure an IP address to receive Trap. Switch(config)#snmp-server host 1.1.1.5 v1 usertrap
----------------	--

snmp-server securityip

Command	snmp-server securityip {<ipv4-address> <ipv6-address>} no snmp-server securityip {<ipv4-address> <ipv6-address>}	
Parameter	<ipv4-address>	NMS security IPv4 address, dotted decimal notation
	<ipv6-address>	NMS security IPv6 address, colon hexadecimal
Default	None.	
Mode	Global Mode	
Usage Guide	Configure security IPv4 or IPv6 address allowed to access NMS management station 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. The no command deletes security IPv4 or IPv6 address configured.	
Example	Configure security IP address of NMS management station. Switch(config)#snmp-server securityip 1.1.1.5	

snmp-server securityip enable

Command	snmp-server securityip {enable disable}	
Parameter	enable disable	SNMP security ip configuration enabled or disabled
Default	Enable the security IP address authentication function.	

Mode	Global Mode
Usage Guide	Enable/disable the security IP address authentication on NMS management station.
Example	Disable the security IP address authentication function. Switch(config)#snmp-server securityip disable

snmp-server trap-source

Command	snmp-server trap-source {<ipv4-address> <ipv6-address>} no snmp-server trap-source {<ipv4-address> <ipv6-address>}	
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
Default	None.	
Mode	Global Mode	
Usage Guide	Set the source IPv4 or IPv6 address which is used to send trap packet. 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. The no command deletes the configuration.	
Example	Set the IP address which is used to send trap packet. Switch(config)#snmp-server trap-source 1.1.1.5	

snmp-server user

Command	snmp-server user <use-string> <group-string> [{authPriv [auth {md5 sha} <word>]} {authNoPriv [{3des aes des} <word>]} [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>}]	
Parameter	<use-string>	the user name containing 1-32 characters

	<table> <tr> <td><group-string></td><td>the name of the group the user belongs to, containing 1-32 characters</td></tr> <tr> <td>authPriv</td><td>use DES for the packet encryption</td></tr> <tr> <td>authNoPriv</td><td>not use DES for the packet encryption</td></tr> <tr> <td>auth</td><td>perform packet authentication</td></tr> <tr> <td>md5</td><td>packet authentication using HMAC MD5 algorithm</td></tr> <tr> <td>sha</td><td>packet authentication using HMAC SHA algorithm</td></tr> <tr> <td>3des</td><td>packet authentication using 3DES to encrypt</td></tr> <tr> <td>aes</td><td>packet authentication using AES to encrypt</td></tr> <tr> <td>des</td><td>packet authentication using DES to encrypt</td></tr> <tr> <td><word></td><td>user password, containing 8-32 character</td></tr> <tr> <td><num-std></td><td>the access-class number for standard numeric ACL, ranging between 1-99</td></tr> <tr> <td><name></td><td>the access-class name for standard ACL, the character string length is ranging between 1-32</td></tr> <tr> <td><ipv6-num-std></td><td>the access-class number for standard numeric IPv6 ACL, ranging between 500-599</td></tr> <tr> <td><ipv6-name></td><td>the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32</td></tr> </table>	<group-string>	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	3des	packet authentication using 3DES to encrypt	aes	packet authentication using AES to encrypt	des	packet authentication using DES to encrypt	<word>	user password, containing 8-32 character	<num-std>	the access-class number for standard numeric ACL, ranging between 1-99	<name>	the access-class name for standard ACL, the character string length is ranging between 1-32	<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599	<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32
<group-string>	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																												
3des	packet authentication using 3DES to encrypt																												
aes	packet authentication using AES to encrypt																												
des	packet authentication using DES to encrypt																												
<word>	user password, containing 8-32 character																												
<num-std>	the access-class number for standard numeric ACL, ranging between 1-99																												
<name>	the access-class name for standard ACL, the character string length is ranging between 1-32																												
<ipv6-num-std>	the access-class number for standard numeric IPv6 ACL, ranging between 500-599																												
<ipv6-name>	the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32																												
Default	None.																												
Mode	Global Mode																												
Usage Guide	<p>Add a new user to an SNMP group.</p> <p>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.</p> <p>The "no" form of this command deletes this user.</p>																												
Example	<p>Add a new user tester in the UserGroup with HMAC md5 for authentication, the password is hellohello; Delete an User</p> <pre>Switch (config)#snmp-server user tester UserGroup authNoPriv auth md5 hellohello Switch (config)#no snmp-server user tester</pre>																												

snmp-server view

Command	<pre>snmp-server view <view-string> <oid-string> {include exclude} no snmp-server view <view-string> [<oid-string>]</pre>		
Parameter	<table> <tr> <td><view-string></td><td>view name, containing 1-32 characters</td></tr> </table>	<view-string>	view name, containing 1-32 characters
<view-string>	view name, containing 1-32 characters		

	<div> <div><oid-string></div> <div>OID number or corresponding node name, containing 1-255 characters</div> </div> <div> <div>include exclude</div> <div>include/exclude this OID</div> </div>
Default	None.
Mode	Global Mode
Usage Guide	<p>This command is used to create or renew the view information.</p> <p>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.</p> <p>the “no” form of this command deletes the view information.</p>
Example	<p>Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them.</p> <pre>Switch(config)#snmp-server view readview iso include Switch(config)#snmp-server view readview iso.3 exclude Switch(config)#no snmp-server view readview</pre>

switchport updown notification enable

Command	<div>switchport updown notification enable</div> <div>no switchport updown notification enable</div>
Parameter	<div>none</div> <div>none</div>
Default	Send the trap message to the port of IP/DOWN event as default.
Mode	Port Mode
Usage Guide	<p>Enable/disable the function of sending the trap message to the port of UP/DOWN event.</p> <p>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.</p> <p>The no command deletes the configuration.</p>
Example	<p>Disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event.</p> <pre>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</pre>

no switchport updown notification enable

5 Commands for Switch Upgrade

copy (FTP)

Command	copy <source-url> <destination-url> [ascii binary]														
Parameter	<table><tr><td><source-url></td><td>the location of the source files or directories to be copied</td></tr><tr><td><destination-url></td><td>the destination address to which the files or directories to be copied</td></tr><tr><td>ascii</td><td>ASCII standards will be adopted</td></tr><tr><td>binary</td><td>File transfer will be in binary mode (default transfer method)</td></tr></table>	<source-url>	the location of the source files or directories to be copied	<destination-url>	the destination address to which the files or directories to be copied	ascii	ASCII standards will be adopted	binary	File transfer will be in binary mode (default transfer method)						
<source-url>	the location of the source files or directories to be copied														
<destination-url>	the destination address to which the files or directories to be copied														
ascii	ASCII standards will be adopted														
binary	File transfer will be in binary mode (default transfer method)														
Default	None.														
Mode	Admin Mode														
Usage Guide	<p>This command is used to transfer files by TFTP.</p> <p>When URL represents an FTP address, its form should be:</p> <p>ftp://<username>:<password>@{<ipaddress> <ipv6address>}<hostname> }/<filename>,a mongst <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.</p> <p>Special keywords of the filename</p> <table><tr><th>keywords</th><th>explain</th></tr><tr><td>running-config</td><td>Running configuration files</td></tr><tr><td>startup-config</td><td>It means the reboot configuration files when using copy running-config startup-config command</td></tr><tr><td>nos.img</td><td>System files</td></tr><tr><td>bootrom</td><td>System startup files</td></tr><tr><td>stacking/nos.img</td><td>As destination address, execute system files upgrade for Slave in stacking mode</td></tr><tr><td>stacking/nos.rom</td><td>As destination address, execute system startup files upgrade for Slave in stacking mode</td></tr></table> <p>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:</p> <pre>ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] > ftp username> ftp password> ftp filename></pre> <p>Requesting for FTP server address, user name, password and file name</p>	keywords	explain	running-config	Running configuration files	startup-config	It means the reboot configuration files when using copy running-config startup-config command	nos.img	System files	bootrom	System startup files	stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode	stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode
keywords	explain														
running-config	Running configuration files														
startup-config	It means the reboot configuration files when using copy running-config startup-config command														
nos.img	System files														
bootrom	System startup files														
stacking/nos.img	As destination address, execute system files upgrade for Slave in stacking mode														
stacking/nos.rom	As destination address, execute system startup files upgrade for Slave in stacking mode														
Example	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

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

Save the running configuration files.

Switch#copy running-config startup-config

copy (TFTP)

Command

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

Parameter

<source-url>	the location of the source files or directories to be copied
<destination-url>	the destination address to which the files or directories to be copied
ascii	ASCII standards will be adopted
binary	File transfer will be in binary mode (default transfer method)

Default

None.

Mode

Admin Mode

Usage Guide

This command is used to transfer files by TFTP.

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	explain
running-config	Running configuration files
startup-config	It means the reboot configuration files when using copy running-config startup-config command
nos.img	System files
boot.rom	System startup files

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	<p>Save images in the FLASH to the TFTP server of 10.1.1.1</p> <pre>Switch#copy nos.img tftp://10.1.1.1/nos.img</pre> <p>Obtain system file nos.img from the TFTP server 10.1.1.1</p> <pre>Switch#copy tftp://10.1.1.1/nos.img nos.img</pre> <p>Save the running configuration files</p> <pre>Switch#copy running-config startup-config</pre>
----------------	---

ftp-dir

Command	ftp-dir <ftp-server-url>
Parameter	<ftp-server-url> ftp server address
Default	None.
Mode	Admin Mode
Usage Guide	<p>Browse the file list on the FTP server.</p> <p>The form of <ftp-server-url> is :</p> <p>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.</p>
Example	<p>Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”.</p> <pre>Switch#ftp-dir ftp://Switch:superuser @10.1.1.1</pre>

ftp-server enable

Command	ftp-server enable no ftp-server enable
Parameter	none none
Default	FTP server is not started by default.

Mode	Global Mode
Usage Guide	<p>This command is used to start the FTP server.</p> <p>When FTP server function is enabled, the switch can still perform ftp client functions.</p> <p>The “no ftp-server enable” command shuts down FTP server and prevents FTP user from logging in.</p>
Example	<p>Enable FTP server services.</p> <p>Switch(config)# ftp-server enable</p>

ftp-server timeout

Command	ftp-server timeout <seconds>
Parameter	<p><seconds> the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600</p>
Default	The system default is 600 seconds.
Mode	Global Mode
Usage Guide	<p>This command is used to configure FTP data connection idle time.</p> <p>When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.</p>
Example	<p>Modify the idle threshold to 100 seconds.</p> <p>Switch(config)#ftp-server timeout 100</p>

ip ftp

Command	<p>ip ftp username <username> password [0 7] <password></p> <p>no ip ftp username <username></p>
Parameter	<p><username> the username of the FTP link, its range should not exceed 32 characters</p> <p>[0 7] 0 means password is not encrypted ,7 means password is encrypted</p> <p><password> FTP link password</p>

Default	The system uses anonymous FTP links by default.
Mode	Global Mode
Usage Guide	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.
Example	Configure the username as Switch and the password as superuser. Switch(config)#ip ftp username Switch password 0 superuser

show ftp

Command	show ftp
Parameter	none none
Default	None.
Mode	Admin and Global Mode
Usage Guide	Display the parameter settings for the FTP server.
Example	Display the parameter settings for the FTP server. Switch#show ftp Timeout : 600

show tftp

Command	show tftp
Parameter	none none
Default	None.
Mode	Admin and Global Mode
Usage Guide	Display the parameter settings for the TFTP server.

Example	<p>Display the parameter settings for the TFTP server.</p> <pre>Switch#show tftp timeout : 60 Retry Times : 10</pre>
----------------	--

tftp-server enable

Command	<p>tftp-server enable no tftp-server enable</p>
Parameter	<p>none none</p>
Default	<p>Disable TFTP Server.</p>
Mode	<p>Global Mode</p>
Usage Guide	<p>This command is used to start the TFTP server.</p> <p>The “no ftp-server enable” command shuts down TFTP server and prevents TFTP user from logging in.</p>
Example	<p>Start the TFTP server.</p> <pre>Switch(config)#tftp-server enable</pre>

tftp-server retransmission-number

Command	<p>tftp-server retransmission-number <number></p>
Parameter	<p><number> the time to re-transfer, the valid range is 1 to 20</p>
Default	<p>Retransmit 5 times.</p>
Mode	<p>Global Mode</p>
Usage Guide	<p>Set the retransmission time for TFTP server.</p>
Example	<p>Modify the retransmission to 10 times.</p> <pre>Switch(config)#tftp-server retransmission-number 10</pre>

tftp-server transmission-timeout

Command	tftp-server transmission-timeout <seconds>
Parameter	<seconds> the timeout value, the valid range is 5 to 3600s
Default	The system default timeout setting is 600 seconds.
Mode	Global Mode
Usage Guide	Set the transmission timeout value for TFTP server.
Example	Modify the timeout value to 60 seconds. Switch(config)#tftp-server transmission-timeout 60

6 Commands for File System

cd

Command	cd <directory>	
Parameter	<directory>	the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80
Default	The default working directory is Flash.	
Mode	Admin Mode	
Usage Guide	Change the working directory for the storage device. 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:/	

copy

Command	copy <source-file-url> <dest-file-url>	
Parameter	<source-file-url>	The source address of the file or directory to be copied
	<dest-file-url>	The destination address of the file or directory to be copied
Default	None.	
Mode	Admin Mode	
Usage Guide	Copy a designated file on the switch and store it as a new 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”

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

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.

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.

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
----------------	--

delete

Command	delete <file-url>
Parameter	<file-url> the full path of the file to be deleted
Default	None.
Mode	Admin Mode
Usage Guide	Delete the designate file on the storage device.
Example	Delete file flash:/nos.img. Switch#delete flash:/nos5.img Delete file flash:/nos5.img?[Y:N]y Deleted file flash:/nos5.img

dir

Command	dir [WORD]
Parameter	[WORD] the name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.

Default	No <WORD> means to display information of the current working directory.
Mode	Admin Mode
Usage Guide	Display the information of the designated directory on the storage device. This command does not support a recursive display of all sub-directories.
Example	Display information of the directory “flash:/”. <pre>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#</pre>

pwd

Command	pwd
Parameter	none none
Default	The default directory is flash.
Mode	Admin Mode
Usage Guide	Display the current working directory.
Example	Display the current working directory. <pre>Switch#pwd flash:/</pre>

rename

Command	rename <source-file-url> <new-filename >				
Parameter	<table> <tr> <td><source-file-url></td><td>the source file, in which whether specifying or not its path are both acceptable</td></tr> <tr> <td><new-filename ></td><td>filename without specifying its path</td></tr> </table>	<source-file-url>	the source file, in which whether specifying or not its path are both acceptable	<new-filename >	filename without specifying its path
<source-file-url>	the source file, in which whether specifying or not its path are both acceptable				
<new-filename >	filename without specifying its path				
Default	None.				
Mode	Admin Mode				

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 !
----------------	--

7.Commands for Onvif Configuration

onvif server enable

Command	onvif server enable no onvif server enable
Parameter	none
Default	none
Mode	Global Mode
Usage	This command is used to enable/disable the global Onvif server.
Example	Enable the Onvif server feature globally. Switch(config)#onvif server enable

onvif detect enable

Command	onvif detect enable
Parameter	none
Default	none
Mode	Global Mode
Usage	This command is used to enable global onvif detect.
Example	Enable onvif detect globally. Switch(config)#onvif detect enable

clear onvif detect database

Command	clear onvif detect database clear onvif detect mac <mac-address>
Parameter	<mac-address> Mac-address is the MAC address of the onvif device"xx-xx-xx-xx-xx-xx" format display;
Default	none
Mode	Admin Mode
Usage	This command is used to clear onvif detected data.
Example	Clears onvif detected data. Switch#clear onvif detect database

8. Commands for Alarm

alarm env-humidity

Command	alarm env-humidity < WORD>
Parameter	WORD Set the alarm threshold for environmental humidity , range<0-100>
Default	By default, the alarm threshold for environmental humidity is 80
Mode	Global Mode
Usage Guide	Monitoring range for configuring environmental humidity
Example	Set the alarm threshold for environmental humidity to 60 Switch(config)#alarm env-humidity 60

alarm env-temp

Command	alarm env-temp [max min] < WORD>
Parameter	max Set the maximum alarm threshold for environmental temperature, range<-60-100> min Set the minimum alarm threshold for environmental temperature, range<-60-100>
Default	By default, the maximum alarm threshold for ambient temperature is 65, and the minimum alarm threshold for ambient temperature is -20
Mode	Global Mode
Usage Guide	Used to configure the monitoring range of environmental temperature, set the maximum threshold for environmental temperature alarm to not be lower than the minimum value for environmental temperature alarm, and set the minimum value for environmental temperature alarm to not be higher than the maximum value for environmental temperature alarm
Example	Set the maximum alarm threshold for ambient temperature to 60 Switch(config)#alarm env-temp max 60

alarm power-consumption

Command	alarm power-consumption < WORD>
Parameter	WORD Set the alarm threshold for system power consumption , range <0-800>
Default	By default, the alarm threshold for system power consumption is 305
Mode	Global Mode

Usage Guide	Monitoring threshold for configuring system power consumption
Example	Set the monitoring threshold for system power consumption to 60
	Switch(config)#alarm power-consumption 60

alarm sys-temp

Command	alarm sys-temp [max min] < WORD>	
Parameter	max	Set the maximum alarm threshold for system temperature, range <-60-100>
	min	Set the minimum alarm threshold for system temperature, range <-60-100>
Default	By default, the maximum alarm threshold for system temperature is 65, and the minimum alarm threshold for system temperature is -20	
Mode	Global Mode	
Usage Guide	Used to configure the monitoring range of system temperature, set the maximum threshold for system temperature alarm to not be lower than the minimum value for system temperature alarm, and set the minimum value for system temperature alarm to not be higher than the maximum value for system temperature alarm	
Example	Set the maximum alarm threshold for system temperature to 60	
	Switch(config)#alarm sys-temp max 60	

alarm-input detect-mode

Command	alarm-input detect-mode [close high-level low-level]	
Parameter	close	Disable alarm input detection
	high-level	High level triggers alarm
	low-level	Low level triggers alarm
Default	By default, close alarm input detection	
Mode	Global Mode	
Usage Guide	<p>Used to configure the detection mode for alarm input,</p> <ol style="list-style-type: none"> 1. The switch can detect the voltage of the Alarm Input port. If the voltage is below 5V, it will be judged as Low Level, and if the voltage is between 5V and 57V, it will be judged as High Level. 2. When the Alarm Input Detection Method is configured as Close, Alarm Input will not trigger Port Alarm Action and Alarm Output. 3. When the Alarm Input Detection Method is configured as High Level(Low Level), the Port Alarm Action and Alarm Output will be triggered when the voltage detected by Alarm Input changes from Low Level to High Level(from High Level to Low Level). 	
Example	Set the detection mode of the alarm input to high-level alarm	
	Switch(config)#alarm-input detect-mode high-level	

alarm-log input

Command	alarm-log input [disable enable]	
Parameter	disable	Disable the alarm input log function
	enable	Enable alarm input log function
Default	By default, the alarm input log function is disabled	
Mode	Global Mode	
Usage Guide	Enable for configuring alarm input logs. Once enabled, when an alarm is triggered, commands can be used to view relevant alarm log information	
Example	Enable alarm input log function	
	Switch(config)#alarm-log input enable	

alarm-log output

Command	alarm-log output [disable enable]	
Parameter	disable	Disable the alarm output log function
	enable	Enable alarm output log function
Default	By default, the alarm output log function is disabled	
Mode	Global Mode	
Usage Guide	Enable for configuring alarm output logs. Once enabled, when an alarm is triggered, commands can be used to view relevant alarm log information	
Example	Enable alarm output log function	
	Switch(config)#alarm-log output enable	

alarm-output

Command	alarm-output [disable enable]	
Parameter	disable	Disable alarm output function
	enable	Enable alarm output function
Default	By default, the alarm output function is disabled	
Mode	Global Mode	
Usage Guide	Used to configure alarm output enablement, after which the configured alarm input fault type is monitored. If an abnormal fault type is detected, the alarm output action will be triggered	
Example	Enable alarm output function	
	Switch(config)#alarm-output enable	

alarm-output mode

Command	alarm-output mode [impulse often-close often-open]
---------	---

Parameter	impulse Impulse often-close Often close often-open Often open
Default	By default, the alarm output mode is often close
Mode	Global Mode
Usage Guide	<p>1. Alarm (often close)/Alarm(often open)/Alarm Impulse: When all items in the Failure Type are Normal, the Relay state is closed/open/closed.</p> <p>When an Alarm is detected in the Failure Type item, the Relay state is open/closed/impulse(Relay status switches between open and closed).</p> <p>2. When Alarm Output Enable is Disabled, the Relay state is only related to the configuration in the Output Method. For example, when the Output Method is Alarm(often open), the Relay state will remain open.</p> <p>When Alarm Output Enable is set to Enabled, the Relay status will be related to the configuration of the Output Method and whether there is an Alarm in the Failure Type. As described in section 1.</p>
Example	Configure the alarm output mode as impulse Switch(config)#alarm-output mode impulse

alarm-output monitor-mode

Command	alarm-output monitor-mode [alarm-input env-humidity env-temp sys-power sys-temp v1 v2] no alarm-output monitor-mode [alarm-input env-humidity env-temp sys-power sys-temp v1 v2]		
Parameter	alarm-input env- humidity Alarm In env-temp Environment Humidity sys-power Environment Temperature sys-temp System Power v1 System Temperature v2 DC1 Master V1 DC2 Slave V2		
Default	None.		
Mode	Global Mode		
Usage Guide	<p>1. To configure the fault type for detection, it is necessary to enable alarm output first before enabling monitoring of the fault type. If an abnormal fault type is detected, the alarm output action will be executed</p> <p>2. Support simultaneous detection of multiple types</p> <p>3. Alarm input: Low and high level alarms will trigger alarms</p> <p>4. Environmental humidity: Trigger an alarm based on the upper limit of the detected environmental humidity</p> <p>5. Environmental temperature: Detecting that the environmental temperature has reached the minimum or maximum value triggers an alarm</p> <p>6. System power consumption: Detecting that the system power consumption has reached the configured threshold triggers an alarm</p>		

	<p>7. System temperature: Detecting that the system temperature has reached the minimum or maximum value triggers an alarm</p> <p>8. v1: Detected v1 power failure or no input triggering alarm</p> <p>9. v2: Detected v2 power failure or no input triggering alarm</p> <p>10. The 'no' command will delete the set fault type</p>
--	---

Example	<p>Configure the fault detection type as alarm input</p> <p>Switch(config)#alarm-output monitor-mode alarm-input</p>
----------------	---

alarm-input action

Command	alarm-input action [close normal reboot]						
Parameter	<table> <tr> <td>close</td><td>Close Port</td></tr> <tr> <td>normal</td><td>the port does not take any action</td></tr> <tr> <td>reboot</td><td>Reboot Port</td></tr> </table>	close	Close Port	normal	the port does not take any action	reboot	Reboot Port
close	Close Port						
normal	the port does not take any action						
reboot	Reboot Port						
Default	None.						
Mode	Port Configuration Mode.						
Usage Guide	<p>1. When Alarm Input triggers an alarm, the port will perform the configured actions.</p> <p>2. Normal: When Alarm Input detects an alarm, the port does not take any action.</p> <p>Close Port: When Alarm Input detects an alarm, the port will be closed.</p> <p>Reboot Port: When Alarm Input detects an alarm, the port will reboot.</p>						
Example	<p>The port action when configuring low and high level alarms is to close the port</p> <p>Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#alarm-input action close</p>						

alarm-output monitor

Command	alarm-output monitor [poe port] no alarm-output monitor [poe port]				
Parameter	<table> <tr> <td>poe</td><td>PoE port</td></tr> <tr> <td>port</td><td>Port</td></tr> </table>	poe	PoE port	port	Port
poe	PoE port				
port	Port				
Default	None.				
Mode	Port Configuration Mode.				
Usage Guide	<p>When the status of the monitored port changes from Up to Down, an alarm output will be triggered</p> <p>When the status of the monitored POE port changes from On to Off, an alarm output will be triggered</p> <p>The 'no' command will delete the configured monitoring port/POE port configuration</p>				

Example	<p>When the status of the monitoring port changes from Up to Down, an alarm output is triggered</p> <pre> Switch#config Switch(config)#interface ethernet 1/0/1 Switch(config-if-ethernet1/0/1)#alarm-output monitor port </pre>	
show alarm-info		
Command	show alarm-info	
Parameter	none	无
Default	None.	
Mode	Admin and configuration mode.	
Usage Guide	Used to view the configuration and input information of the alarm function	
Example	<p>View the configuration and input information of the alarm function</p> <pre> Switch#show alarm-info *****Alarm input config***** Detect mode: Close Close port config: Reboot port config: *****Alarm output config***** Enable state: DISABLE Relay output mode: Alarm(often close) Failure type config: Port monitor config: Port poe monitor config: *****System info***** Power Type: PoE Relay State: Close System power(w): 5 System power upper(W): 305 Alarm log config: System temperature(°C): 15.1 System temperature range(°C): -20-65 Environment temperature(°C): No Sensor Environment temperature range(°C): -20-65 Environment humidity(%): No Sensor Environment humidity upper(%): 80 Power In (Master V1, Slave V2): V1 Master V1 Voltages (V): 55.2 Slave V2 Voltages (V): Power Failure Or No Input Detection Input (High Level:5~57V; Low Level:0~5V): Low Level </pre>	