QUANTUM® NETWORKS

QASA CLI GUIDE

Basic Switch Configuration

Contents

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	This command can configure the authentication methods for Console, VTY, and Web login separately. The authentication method can be any one or combination of Local, RADIUS and TACACS. Preferences from left to right when the login method is in combined configuration. If the user has passed the authentication method, the authentication method of the lower preference is ignored. As long as user pass an authentication method, the user can log in. AAA function and RADIUS server should be configured before the RADIUS authentication can be used. 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. They all support the following authentication methods. **Local:** Use the local user account database for authentication. **Tacacs:** Authentication using remote Tacacs server. **Radius:** Authentication using remote Radius server. No command restores default authentication.
Example	Configure Telnet and ssh login methods to Local and RADIUS authentication methods. **Switch(config)#**

banner

Command	**banner motd<LINE>** **no banner motd**
Parameter	**<LINE>:** The information is displayed when the authentication is successful, length limit is from 1 to 100 characters.
Default	By 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	Display "Welcome" after authentication is successful. **Switch(config)# banner motd Welcome**

boot img

Command	**boot img<img-file-url> {primary | backup}**
Parameter	**<img-file-url>:** Full path to the img file
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	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. 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 cannot be longer than 80 characters.
Example	Set flash:/nos.img as the second booting IMG file used in the next booting of the switch.

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	This command is used to configure the CFG file used in the next booting of the switch. Configure the CFG file used in the next booting can only use .cfg files stored in the switch. 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 cannot be longer than 80 characters.
Example	Set flash:/ startup.cfg as the CFG file used in the next booting of the switch.

clock set

Command	**clock set <HH:MM:SS><YYYY.MM.DD>**
Parameter	**<HH:MM:SS>:** Shows time. For HH, effective range is 0 to 23, For MM and SS, it is 0 to 59. **<YYYY.MM.DD>:** Year, month and date. For YYYY, valid range is 1970 to 2038, For month 1 to 12 and for 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	This command is used to configure switch system's time and date. The switch cannot continue timing with power off, hence the current date and time must be first set at environments where exact time is required.
Example	To set the switch's current date and time to 2002.8.1 23: 0: 0. **Switch#clock set 23:0:0 2002.8.1**

config

Command	**config [terminal]**
Parameter	**[terminal]:** indicates terminal configuration.
Default	None.
Mode	Admin Mode.
Usage Guide	This command is used in 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.
Default	None.
Mode	Admin Mode.
Usage Guide	This command is used in switch to 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	Use enable command to enter Admin Mode from User Mode, or change the privilege level of the users. To prevent unauthorized access of non-admin user, user authentication is required (i.e. Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted; if 3 consecutive entry of Admin user password are all wrong, it remains in the User Mode. When the user's privilege is changed from the low level to the high level, it needs to authenticate the password of the corresponding level, or else it will not authenticate the password. Set the Admin user password under Global Mode with "enable password" command.
Example	Enter management mode from user mode. **Switch>enable** **Switch#**

enable password

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

end

Command	**end**
Parameter	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 to configure the timeout of exiting admin mode. Timeout exit admin management mode, need to enter management mode and password to enter admin management mode again. When the timeout is set to 0, the timeout timer is disabled. "no exec-timeout "command is used 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.
Default	None.
Mode	All Modes.
Usage Guide	This command is used to quit current mode and return to its previous mode.
Example	Quit global mode to its 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, press '?'. If nothing matches, the help list will be empty and you must backup until entering a '?', which 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 to 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 "delhi" to 200.121.1.1. **Switch(config)#ip host delhi 200.121.1.1**

ipv6 host

Command	**ipv6 host <hostname><ipv6_addr>** **no ipv6 host { <hostname> | all}**
Parameter	**<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	By using this command, you can set the mapping relationship between the host and the IPv6 address. Set the association between host and IPv6 address, which can be used in commands like "traceroute6 <host>". The "no ip host" parameter of this command will delete the mapping.
Example	Set the IPv6 address of the host named Delhi to 2001:1:2:3::1. **Switch(config)#ipv6 host Delhi 2001:1:2:3::1**

ip http server

Command	**ip http server** **no ip http server**
Parameter	None.
Default	Enable.
Mode	Global Mode.
Usage Guide	Use this command to enable Web configuration. The "no ip http server" command disables Web configuration.
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 the input option is 0 on password setting, the password is not encrypted; if the input option is 7, the password is encrypted. **<password>:** password for the user.
Default	This password is empty by default by system.
Mode	Global Mode.
Usage Guide	With this command, configure the password used to enter normal user mode on the console. The "no password" command deletes this password.
Example	To 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#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 executing this command. No service password-encryption cancels this function, however, encrypted passwords remain unchanged.
Example	To 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 to configure the columns of characters displayed on each screen of the terminal. The columns of characters displayed on each screen on the telent.ssh client and the Console will be following this configuration. The "no service terminal-length" command cancels the screen shifting operation.
Example	Set the number of vty threads to 20. **Switch(config)#service terminal-length 20**

sysContact

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

sysLocation

Command	**sysLocation<LINE>** **no sysLocation**
Parameter	**<LINE>:** the prompt character string, range from 0 to 255 characters.
Default	The default is factory setting.
Mode	Global Mode
Usage Guide	With this command, The user can set the factory address bases the fact instance. The "no sysLocation" command reset the switch to factory settings.
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	Reset the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time. **Note**: After the command, "write" command must be executed to save the operation. The switch will reset to factory settings after restart.
Example	Restore factory settings and restart. **Switch#set default** Are you sure? [Y/N] = y **Switch#write** **Switch#reload**

set boot password

Command	**set boot password** **no set boot password**
Parameter	**none: none**
Default	None.
Mode	Global Mode.
Usage Guide	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 configure it. ***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** Current time is TUE AUG 22 11：00：01 2002

show cpu usage

Command	**show cpu usage [<slotno>]**
Parameter	**[<slotno>]:** Specify slots
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage. Only the chassis switch uses slot no 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#showcpu 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	To display CPU utilization. **Switch#showcpu 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 slot no 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	Shows 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	Shows the level of the specified command. LINE must be the whole command format, the abbreviation format is used to the command which can be analyzed successfully. For half-baked command, false command about writing and command whose abbreviation cannot be analyzed successfully, the level of them cannot be shown.
Example	Show the level of privilege command. **Switch(config)#show privilege exec show ip route** The command : show ip route Privilege is : 15

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	This command is used to collect the relative information when the switch operation is malfunctioned. Displays the operational information and the task status of the switch. The technique specialist use this command to diagnose whether the switch operate normally or not.
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 information of hardware version and the software version.
Example	Displays the version information of the switch. **Switch#show version**

username

Command	**username <username> [privilege <privilege>] [password [0 | 7]<password>]** **no username <username>**
Parameter	**<username>:** The username, its range should not exceed to 32 characters. **<privilege>:** The maximum privilege level of the command that the user is able to execute, its value is limited between 1 to 15, and 1 is by default. **[0 | 7]:** If input option is 0 on password setting, the password is not encrypted; if input option is 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, make sure that one user has to 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 configuring 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/Global Mode.
Usage Guide	Save the current configured parameters to the Flash memory. 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.
Example	Save the current configuration. **Switch#write**

write running-config

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

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	Admin Mode.
Usage Guide	Enables 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 **Vty:** 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	Configures 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 **vty:** 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	Configures 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 command audit methods through telnet login, command level 15.

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	Configures the list of the enable authentication method. The enable authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configured in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. To be mentioned, if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method); it will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method is used. And TACACS server should be configured before the TACACS configuration method is used. The no command restores the default authentication method.
Example	Configure the enable authentication method to be tacacs and local. **Switch(config)#authentication enable tacacs local**

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 32.
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	**<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 32.
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	**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	Configures VTY (login with Telnet and SSH), Web and Console, to select the list of the authentication method for the login user. Authentication method can be any one or combination of Local, RADIUS and TACACS. When login method is configured in combination, the preference goes from left to right. If the users have passed the authentication method, authentication method of lower preferences will be ignored. if the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authentication method (Exception: if the local authentication method failed, it will attempt the next authentication method)； It will attempt the next authentication method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method can be used. And TACACS server should be configured before the TACACS configuration method can be used. The authentication line console login command is exclusive with the "login" command. The authentication line console login command configures the switch to use the Console login method. And the login command makes the Console login to use the passwords configuration by the password command for authentication. If local authentication is configured while no local users are configured, users will be able to login the switch via the Console method.

	The no form of command restores the default authentication method.
Example	Configure the telnet and ssh login with the remote RADIUS authentication. **Switch(config)#authentication line vty login radius**

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

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	To configure the security IPv6 address for Telnet and HTTP login method. IPv6 address of the client which can login the switch is not restricted before the security IPv6 address is not configured.

	After the security IPv6 address is configured, only clients with security IPv6 addresses are able to login into switch. Up to 32 security IPv6 addresses can be configured in the switch. The no form of this command will remove the specified configuration.
Example	Configure the security IPv6 address is 2001:da8:123:1::1. **Switch(config)#authentication securityipv6 2001:da8:123:1::1**

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	Configures the list of the authorization method for the login user with VTY (login with Telnet and SSH), Web and Console. Authorization method can be any one or combination of Local, RADIUS or TACACS. When login method is configured in combination, the preference goes from left to right. If the users have passed the authorization method, authorization method of lower preferences will be ignored. If the user receives corresponding protocol's answer whether refuse or incept, it will not attempt the next authorization method; it will attempt the next authorization method if it receives nothing. And AAA function RADIUS server should be configured before the RADIUS configuration method is used. And TACACS server should be configured before the TACACS configuration method is used. The local users adopt username command permission while authorization command is not configured, the users login the switch via RADIUS/TACACS method and works under common mode. The no command restores the default authorization method.

Example	To configure the telnet authorization method to RADIUS. **Switch(config)#authorization line vty exec radius**

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
Default	The authorization manner is not configured as default.
Mode	Global Mode.
Usage Guide	Configures command authorization manner and authorization selection priority of login user with VTY (login with Telnet and SSH). The enabling authorization method can be any one or combination of Local, RADIUS and TACACS. When using combination authorization manners, the priority of the front authorization manner is the highest and the others are in descending order. If the authorization with high priority passed, it is successful to configure command and the back authorization manner will be ignored. As long as one authorization manner receives a clear response of the corresponding agreement. Whether it is received or refused, the next authorization manner will not be attempted. If the clear response is not received, try the next manner. When using RADIUS authorization, AAA function must be enabled and configure RADIUS server. When using TACACS authorization, TACACS server must be configured. None is the manner of escaping and it only can be the last manner. This method returns after being authorized directly, and the command is configured successfully. The no command recovers to be default manner.
Example	Configure level 1 command authorization manner of telnet login user as TACACS. **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 entering this command, you will be prompted with 'Confirm[Y/N]:' If 'Y' or 'y' is entered, the delete operation will proceed. If '？ ' is entered, the delete operation will not run, and only a notice will be displayed. For any other input, the delete operation will not be executed.
Example	Admin users who are forced to log in through VTY (using Telnet or SSH login) are off line. **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 of the ssh and close the ssh service.
Example	Clear the secret key of the 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 any key to show information in next screen. The "terminal no length" cancels the screen switching operation and display content once in all.
Example	Configure length of characters in each display to 20. **Switch#terminal length 20** ssh is closed successfully.

telnet

Command	**telnet [vrf<vrf-name>] {<ip-addr> | <ipv6-addr> | host <hostname>}[<port>]**
Parameter	**<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	This command is used when the switch is applied as Telnet client, for logging in remote host to configure. When a switch is applied as a Telnet client, it can only establish one TCP connection with the remote host. To connect to another remote host, the current TCP connection must be disconnected with a hotkey "CTRL+ \".

	To telnet a host name, mapping relationship between the host name and the IP/IPv6 address should be previously configured. For required commands please refer to ip host and ipv6 host. In case a host corresponds to both an IPv4 and an IPv6 addresses, the IPv6 should be preferred when telneting this host name.
Example	The switch telnets to a remote host whose IP address is 20.1.1.1. **Switch#telnet 20.1.1.1 23** Connecting Host 20.1.1.1 Port 23... Service port is 23 Connected to 20.1.1.1 login:123 password:*** router>

telnet server enable

Command	**telnet server enable** **no telnet server enable**
Parameter	**none: none**
Default	None.
Mode	Global Mode.
Usage Guide	Enables the Telnet server function in the switch. This command is available in Console only. The administrator can use this command to enable or disable the Telnet client to login to the switch. The “no telnet server enable “command disables the Telnet function in the switch.
Example	Disable the Telnet server function in the switch. **Switch(config)#no telnet server enable**

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 5 to 16. **default:** restore the default configuration
Default	The system default value of the max connection number is 5.
Mode	Global Mode.
Usage Guide	Configures the max connection number supported by the Telnet service of the switch.
Example	Set the max connection number supported by the Telnet service as 10. **Switch(config)#telnet-server max-connection 10**

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	Configures 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 authentication-retries <authentication-retries>** **no ssh-server authentication-retries**
Parameter	**none: none**
Default	SSH function is disabled by default.
Mode	Global Mode.
Usage Guide	Enables 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	**< modulus >:** the modulus is used to compute the host key; valid range is 768 to 2048. The default value is 1024.
Default	The system uses the key generated when the ssh-server started at the first time.
Mode	Global Mode.
Usage Guide	This command is used to generate a new SSH service host rsa key. When SSH client logs on the server, the new host key is used for authentication. After the new host key is generated and "write" command is used to save the configuration, the system uses this key for authentication all the time. Because it takes quite a long time to compute the new key and some clients are not compatible with the key generated by the modulus 2048, it is recommended to use the key which is generated by the default modulus 1024. No command disables SSH service.
Example	To generate new host key. **Switch(config)#ssh-server host-key create rsa**

ssh-server max-connection

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

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	Configures 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	Shows 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	Displays SSH state and users which log on currently.
Example	Display SSH state and users which log on currently. **Switch#showssh-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

show telnet login

Command	show telnet login
Parameter	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	To display SSH state and users which log on currently. **ssh-server login user number 2**

show users

Command	show users
Parameter	None.
Default	None.
Mode	Admin mode.
Usage Guide	Shows the user information who logs in through telnet or ssh. It includes line number, user name and user IP. Because 16 telnet users and 16 ssh users are supported at most currently, vty0-15 are used for telnet, and 16-31 are used for ssh.
Example	Displays user information. **Switch#show users** **Line User Location** vty 16 a 192.168.1.1 vty 0 admin 192.168.1.2 vty 17 mab 192.168.1.13 vty 1 test 192.168.1.40

who

Command	show telnet login
Parameter	**none:** none
Default	None.
Mode	All configuration mode.
Usage Guide	Shows the current login users with vty.
Example	Show the current login users with vty. **Switch#who** Telnet user a login from 192.168.1.20

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	This command is used to enter the VLAN interface configuration mode. Users should first make sure the existence of a VLAN before configuring it. Use "exit" command to quit the VLAN interface configuration mode back to the global configuration mode. The no operation of this command will delete the existing VLAN interface.
Example	Enter the VLAN interface configuration mode of VLAN1. **Switch(config)#interface vlan 1** **Switch(Config-if-Vlan1)#**

ip address

Command	**ip address <ip-address><mask> [secondary]** **no ip address [<ip-address><mask>] [secondary]**
Parameter	**<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	Set the IP address and mask for the specified VLAN interface. A VLAN interface must be created first before the user can assign an IP address to the switch. The no command deletes the specified IP address setting.
Example	Set 10.1.128.1/24 as the IP address of VLAN1 interface.

	Switch(config)#interface vlan 1 **Switch(Config-if-Vlan1)#ip address 10.1.128.1 255.255.255.0** **Switch(Config-if-Vlan1)#exit** **Switch(config)#**

ipv6 address

Command	**ipv6 address <ipv6address | prefix-length> [eui-64]** **no ipv6 address <ipv6address | prefix-length> [eui-64]**
Parameter	**<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	Configures aggregately global unicast address, site-local address and link-local address for the interface. The prefix of an IPV6 address should not be a multicast address, or other kinds of IPV6 addresses with specific usage. Different layer-three VLAN interfaces are forbidden to share a same address prefix. As for any global unicast address, the prefix should be limited in the range from 2001:: to 3fff ::, with a length no shorter than 3 and the prefix length of a site-local address or a link-local address should not be shorter than 10. The no command deletes the specified IPv6 address setting.
Example	To configure an IPV6 address at the layer-three interface of VLAN1: set the prefix as 2001:3f:ed8::99, the length of which is 64. **Switch(config)#interface vlan 1** **Switch(Config-if-Vlan1)#** **Switch(Config-if-Vlan1)#exit** **Switch(config)#**

ipbootp-client enable

Command	**ipbootp-client enable** **no ipbootp-client enable**
Parameter	**none: none**
Default	BootP client function is disabled by default.
Mode	VLAN Interface Mode.
Usage Guide	Enables the switch to be a BootP Client and obtain IP address and gateway address through BootP negotiation. Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any two methods for obtaining IP address is not allowed. To obtain IP address via BootP, a DHCP server or a BootP server is required in the network. The no command disables the BootP Client function and releases the IP address obtained in BootP.
Example	Get IP address through BootP. **Switch(config)#interface vlan 1** **Switch(Config-if-Vlan1)#ip bootp-client enable** **Switch(Config-if-Vlan1)#exit** **Switch(config)#**

ipdhcp-client enable

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

4. Commands for SNMP

rmon enable

Command	**rmon enable** **no rmon enable**
Parameter	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	To disable RMON. **Switch(config)#no rmon enable**

show private-mib oid

Command	**show private-mib oid**
Parameter	None.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Shows 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.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays all SNMP counter information.
Example	Display all SNMP counter information. **Switch#showsnmp** 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 snmpengineid

Command	show snmpengineid
Parameter	None.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays the engine ID commands.
Example	Display the engine ID commands. **Switch#showsnmpengineid** SNMP engineID:3138633303f1276c

show snmp group

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

show snmp status

Command	show snmp status
Parameter	None.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays SNMP configuration information.
Example	Display SNMP configuration information. **Switch#showsnmp 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.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays the user information commands.
Example	Display the user information commands. **Switch#showsnmp 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.
Default	None.
Mode	Admin and configuration mode.
Usage Guide	Displays the view information.
Example	Display the view information. **Switch#showsnmp view** View Name: readview 1. -Included active 1.3. Excluded 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	Configures the community string for the switch. 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. The no command deletes the configured community string.
Example	Add a community string named "private" with read-write permission. **Switch(config)#snmp-server community rw 0 private** Delete the community string named "private". **Switch(config)#no snmp-server community 0 private**

snmp-server enable

Command	**snmp-server enable** **no snmp-server enable**
Parameter	None.
Default	None.
Mode	Global Mode.
Usage Guide	Enables the SNMP proxy server function on the switch. To perform configuration management on the switch with network management software, the SNMP proxy server function has to be enabled with this command. The "no snmp-server enable" command disables the SNMP proxy server function.
Example	Enable the SNMP proxy server function on the switch. **Switch(config)#snmp-server enable**

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	Enables the switch to send Trap message. 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. The no command disables the switch to send Trap message.
Example	Enable to send Trap messages. **Switch(config)#snmp-server enable traps**

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	Configures 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	Configures the engine ID.
Example	Create a group Company Group, with the safety level of recognizing and encrypting, the read view name is read view, and the writing is disabled. **Switch (config)#snmp-server group CompanyGroupAuthPriv read readview**

snmp-server host

Command	**snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>** **no snmp-server host { <host-ipv4-address> | <host-ipv6-address> } {v1 | v2c | {v3 {NoauthNopriv | AuthNopriv | AuthPriv}}} <user-string>**
Parameter	**<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	For the v1/v2c versions of this command, configure the IPv4 or IPv6 address and the trap community string of the network management station receiving the SNMP Trap messages. For the v3 version, this command is used to configure the IPv4 or IPv6 address of the network management station, along with the trap username and security level. The Community character string configured in this command is the default community string of the RMON event group. If the RMON event group has no community character string configured, the community character string configured in this command will be applied when sending the Trap of RMON, and if the community character string is configured, its configuration will be applied when sending the RMON trap. This command allows to configure IPv4 or IPv6 addresses of SNMP management station that receive Trap message at the same time, but IPv4 and IPv6 addresses of v1 and v2c version are less than 8 in all. The “no”form of this command cancels this IPv4 or IPv6 address.
Example	Configure an IP address to receive Trap.

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	Configures 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 sends SNMP packet which 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	To 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	Enables/disables 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	Sets 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	To 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 **<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	Adds a new user to an SNMP group. 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. The "no" form of this command deletes this user.
Example	Add a new user tester in the User Group with HMAC md5 for authentication, the password is hellohello; delete a User. **Switch (config)#** **Switch (config)#no snmp-server user tester**

snmp-server view

Command	**snmp-server view <view-string><oid-string> {include | exclude}** **no snmp-server view <view-string> [<oid-string>]**
Parameter	**<view-string>:** view name, containing 1-32 characters **<oid-string>:** OID number or corresponding node name, containing 1-255 characters **include | exclude:** include/exclude this OID
Default	None.
Mode	Global Mode.
Usage Guide	This command is used to create or renew the view information. 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.

	The “no" form of this command deletes the view information.
Example	Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them. **Switch(config)#snmp-server view readview iso include** **Switch(config)#snmp-server view readview iso.3 exclude** **Switch(config)#no snmp-server view readview**

switchport updown notification enable

Command	**switchport updown notification enable** **no switchport updown notification enable**
Parameter	**none: none**
Default	None.
Mode	Send the trap message to the port of IP/DOWN event as default.
Usage Guide	Enables/disables the function of sending the trap message to the port of UP/DOWN event. 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. The no command deletes the configuration.
Example	To disable the function of sending the trap message to the port 1/0/1 of the UP/DOWN event. **Switch(config)#in e 1/0/1** **Switch(config-if-ethernet1/0/1)#no switchport updown notification enable** **Switch(config-if-ethernet1/0/1)#show running-config current-mode**! **no switchport updown notification enable**

5. Commands for Switch Upgrade

copy（FTP）

<table>
<tr><td>Command</td><td>copy <source-url><destination-url> [ascii | binary]</td></tr>
<tr><td>Parameter</td><td><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)</td></tr>
<tr><td>Default</td><td>None.</td></tr>
<tr><td>Mode</td><td>Admin Mode.</td></tr>
<tr><td>Usage Guide</td><td>This command is used to transfer files by TFP.
When URL represents an FTP address, it should be: 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.

Special keywords of the filename
<table>
<tr><th>keywords</th><th>explaination</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>boot.rom</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>

This command supports command line hints, namely if the user can enter commands in following forms: copy <filename> ftp:// or copy ftp:// <filename> and press Enter, following hints will be provided by the system：
ftp server ip/ipv6 address [x.x.x.x]/[x:x::x:x] ></td></tr>
</table>

	ftp username>
ftp password>
ftp filename>
Requesting for FTP server address, user name, password and file name
Example	To 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** To 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 TTFP. When URL represents a TFTP address, it 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	explaination
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:x]>tftp filename> Requesting for TFTP server address, file name
Example	Save images in the FLASH to the TFTP server of 10.1.1.1 **Switch#copy nos.img tftp://10.1.1.1/nos.img** Obtain system file nos.img from the TFTP server 10.1.1.1 **Switch#copy tftp://10.1.1.1/nos.img nos.img** Save the running configuration files **Switch#copy running-config startup-config**

ftp-dir

Command	**ftp-dir<ftp-server-url>**
Parameter	**<ftp-server-url>:** ftp server address
Default	None.
Mode	Admin Mode.
Usage Guide	Browse the file list on the FTP server. The form of <ftp-server-url> is ： ftp://<username>:<password>@{<ipv4address> | <ipv6address>}, amongst <username>is the FTP user name, <password> is the FTP user password, {<ipv4address> | <ipv6address> } is the IPv4 or IPv6 address of the FTP server.
Example	Browse the list of the files on the server with the FTP client, the username is “Switch”, the password is “superuser”.

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	This command is used to start the FTP server. When FTP server function is enabled, the switch can still perform ftp client functions. The "no ftp-server enable" command shuts down FTP server and prevents FTP user from logging in.
Example	Enable FTP server services. **Switch(config)# ftp-server enable**

ftp-server timeout

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

ip ftp

Command	**ip ftp username <username> password [0 | 7] <password>** **no ip ftp username <username>**
Parameter	**<username>:** the username of the FTP link, its range should not be exceeded to 32 characters. **[0 | 7]:** 0 means password is not encrypted ,7 means password is encrypted. **<password>:** FTP link password
Default	The system uses anonymous FTP links by default.
Mode	Global Mode.
Usage Guide	Configures 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.
Default	None.
Mode	Admin and Global Mode.
Usage Guide	Displays 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.
Default	None.
Mode	Admin and Global Mode.
Usage Guide	Displays the parameter settings for the TFTP server.
Example	Display the parameter settings for the TFTP server. **Switch#showtftp** timeout : 60 Retry Times : 10

tftp-server enable

Command	**tftp-server enable** **no tftp-server enable**
Parameter	None.
Default	Disable TFTP Server.
Mode	Global Mode.
Usage Guide	This command is used to start the TFTP server. The "no ftp-server enable" command shuts down TFTP server and prevents TFTP user from logging in.
Example	Start the TFTP server. **Switch(config)#tftp-server enable**

tftp-server retransmission-number

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

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	Sets 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	Changes the working directory for the storage device. After this command is 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: o starting with "flash:/" o "ftp://username:pass@server-ip/file-name" o "tftp://server-ip/file-name" 2. The prefix of the destination file URL should be in one of the following

	forms: o starting with "flash:/" o "ftp://username:pass@server-ip/file-name" o "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** **Copyed 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	Deletes 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:/nos.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	Displays 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:/". **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#**

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. **Switch#pwd** flash:/

rename

Command	**rename <source-file-url><new-filename >**
Parameter	**<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.
Usage Guide	Used to rename a designated file on the switch. 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 **!**