



## QASA CLI GUIDE

# Basic Switch Configuration

## Contents

1. Commands for Basic Configuration.....	6
authentication line .....	6
banner .....	7
boot img .....	7
boot startup-config .....	8
clock set.....	8
config .....	9
disable .....	9
enable .....	9
enable password.....	10
end.....	11
exec-timeout .....	11
exit.....	12
help.....	12
hostname.....	13
ip host .....	14
ipv6 host .....	14
ip http server.....	15
login.....	15
password.....	16
privilege .....	16
reload .....	17
service password-encryption .....	17
service terminal-length .....	18
sysContact .....	18
sysLocation.....	19
set default .....	19
set boot password.....	20
setup .....	20
show clock .....	21
show cpu usage .....	21
show cpu utilization.....	22
show memory usage .....	22
show privilege .....	23

show privilege mode LINE .....	23
show tech-support.....	24
show version.....	24
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.....	29
authentication ip access-class .....	30
authentication ipv6 access-class.....	31
authentication line login .....	31
authentication securityip .....	33
authentication securityipv6 .....	33
authorization .....	34
authorization line vty command.....	35
clear line vty<0-31> .....	36
crypto key clear rsa .....	36
terminal length.....	37
telnet.....	37
telnet server enable .....	38
telnet-server max-connection .....	39
ssh-server authentication-retries.....	39
ssh-server enable .....	40
ssh-server host-key create rsa .....	40
ssh-server max-connection.....	41
ssh-server timeout.....	41
show crypto key .....	42
show ssh-server .....	42
show telnet login .....	42
show users .....	43
who .....	43

3. Commands for Configuring Switch IP .....	44
interface vlan .....	44
ip address .....	44
ipv6 address.....	45
ipbootp-client enable .....	46
ipdhcp-client enable.....	46
4. Commands for SNMP .....	48
rmon enable .....	48
show private-mib oid .....	48
show snmp.....	49
show snmpengineid .....	49
show snmp group .....	50
show snmp mib .....	50
show snmp status.....	51
show snmp user .....	51
show snmp view.....	52
snmp-server community .....	52
snmp-server enable .....	53
snmp-server enable traps.....	54
snmp-server engineid.....	54
snmp-server group .....	55
snmp-server host .....	56
snmp-server securityip.....	57
snmp-server securityip enable.....	57
snmp-server trap-source.....	58
snmp-server user .....	58
snmp-server view .....	59
switchport updown notification enable.....	60
5. Commands for Switch Upgrade .....	61
copy (FTP) .....	61
copy (TFTP) .....	62
ftp-dir.....	63
ftp-server enable .....	64
ftp-server timeout .....	64
ip ftp.....	65

show ftp .....	65
show tftp.....	66
tftp-server enable .....	66
tftp-server retransmission-number .....	67
tftp-server transmission-timeout.....	67
6. Commands for File System.....	68
cd .....	68
copy.....	68
delete .....	69
dir .....	70
pwd.....	70
rename .....	71

# 1. Commands for Basic Configuration

## authentication line

<b>Command</b>	<b>authentication line {console   vty   web} login {local   radius   tacacs}</b> <b>no authentication line {console   vty   web} login</b>
<b>Parameter</b>	<b>Console:</b> Log on the switch through the console serial port <b>vty:</b> Log on the switch through the vty(SSH or Telnet) <b>web:</b> Log on the switch through the web
<b>Default</b>	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<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.</p> <p>Preferences from left to right when the login method is in 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 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.</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><b>Local:</b> Use the local user account database for authentication.</p> <p><b>Tacacs:</b> Authentication using remote Tacacs server.</p> <p><b>Radius:</b> Authentication using remote Radius server.</p> <p>No command restores default authentication.</p>
<b>Example</b>	Configure Telnet and ssh login methods to Local and RADIUS authentication methods.  <b>Switch(config)#</b>

## banner

<b>Command</b>	<b>banner motd&lt;LINE&gt;</b> <b>no banner motd</b>
<b>Parameter</b>	<b>&lt;LINE&gt;</b> : The information is displayed when the authentication is successful, length limit is from 1 to 100 characters.
<b>Default</b>	By default, do not show the information when the authentication is successful.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Display "Welcome" after authentication is successful.  <b>Switch(config)# banner motd Welcome</b>

## boot img

<b>Command</b>	<b>boot img&lt;img-file-url&gt; {primary   backup}</b>
<b>Parameter</b>	<b>&lt;img-file-url&gt;</b> : Full path to the img file
<b>Default</b>	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.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Set flash:/nos.img as the second booting IMG file used in the next booting of the switch.

## boot startup-config

<b>Command</b>	<b>boot startup-config {NULL   &lt;file-url&gt; }</b>
<b>Parameter</b>	<b>NULL:</b> Use the factory primitive configuration as the next reboot boot configuration. <b>&lt;file-url&gt;:</b> Is the full path of CFG file used in the next booting.
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Set flash:/ startup.cfg as the CFG file used in the next booting of the switch.

## clock set

<b>Command</b>	<b>clock set &lt;HH:MM:SS&gt;&lt;YYYY.MM.DD&gt;</b>
<b>Parameter</b>	<b>&lt;HH:MM:SS&gt;:</b> Shows time. For HH, effective range is 0 to 23, For MM and SS, it is 0 to 59. <b>&lt;YYYY.MM.DD&gt;:</b> Year, month and date. For YYYY, valid range is 1970 to 2038, For month 1 to 12 and for date 1 to 31.
<b>Default</b>	By default, upon first time start-up, it is defaulted to 2006.1.1 0: 0: 0.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	To set the switch's current date and time to 2002.8.1 23: 0: 0.  <b>Switch#clock set 23:0:0 2002.8.1</b>



## config

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

## disable

<b>Command</b>	<b>disable</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	This command is used in switch to exit admin mode back to general user mode.
<b>Example</b>	Exit admin mode back to general user mode.  <b>Switch#disable</b> <b>Switch&gt;</b>

## enable

<b>Command</b>	<b>enable [&lt;1-15&gt;]</b>
<b>Parameter</b>	<b>[&lt;1-15&gt;]</b> : User Permission Level
<b>Default</b>	None.
<b>Mode</b>	User mode/ Admin mode.

<b>Usage Guide</b>	<p>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.</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>
<b>Example</b>	<p>Enter management mode from user mode.</p> <p><b>Switch&gt;enable</b> <b>Switch#</b></p>

### enable password

<b>Command</b>	<p><b>enable password [level &lt;1-15&gt;] [0   7] &lt;password&gt;</b> <b>no enable password [level &lt;1-15&gt;]</b></p>
<b>Parameter</b>	<p><b>level &lt;1-15&gt;]:</b> used to specify the privilege level, the default level is 15. <b>[0   7]:</b> 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. <b>&lt;password&gt;:</b> the password for the user.</p>
<b>Default</b>	<p>This password is empty by default by system.</p>
<b>Mode</b>	<p>Global Mode.</p>
<b>Usage Guide</b>	<p>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.</p> <p>The "no enable password" command deletes this password.</p>
<b>Example</b>	<p>Configure the command for general users to enter the admin mode by rule as test.</p> <p><b>Switch(config)#enable password 0 test</b></p>

## end

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

## exec-timeout

<b>Command</b>	<b>exec-timeout &lt;minutes&gt; [&lt;seconds&gt;]</b> <b>no exec-timeout</b>
<b>Parameter</b>	<b>&lt;minutes&gt;</b> : the time value shown in minute and ranges between 0~35791 <b>[&lt;seconds&gt;]</b> : the time value shown in seconds and ranges between 0~59
<b>Default</b>	Default timeout is 10 minutes.
<b>Mode</b>	Global mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Set the admin mode timeout value to 5 minutes, 30 seconds.  <b>Switch(config)#exec-timeout 5 30</b>

## exit

<b>Command</b>	<b>exit</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	All Modes.
<b>Usage Guide</b>	This command is used to quit current mode and return to its previous mode.
<b>Example</b>	Quit global mode to its previous mode  <b>Switch(config)#exit</b> <b>Switch#</b>

## help

<b>Command</b>	<b>help</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	All Modes.
<b>Usage Guide</b>	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.
<b>Example</b>	Get help in global mode.  <b>Switch(config)#help</b> 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

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

## ip host

<b>Command</b>	<b>ip host &lt;hostname&gt;&lt;ip_addr&gt;</b> <b>no ip host {&lt;hostname&gt; all}</b>
<b>Parameter</b>	<b>&lt;hostname&gt;</b> : the string for the prompt, up to 64 characters are allowed <b>&lt;ip_addr&gt;</b> : the corresponding IP address for the host name, takes a dot decimal format <b>all</b> : all of the host name
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Set IP address of a host with the hostname of "delhi" to 200.121.1.1.  <b>Switch(config)#ip host delhi 200.121.1.1</b>

## ipv6 host

<b>Command</b>	<b>ipv6 host &lt;hostname&gt;&lt;ipv6_addr&gt;</b> <b>no ipv6 host {&lt;hostname&gt;   all}</b>
<b>Parameter</b>	<b>&lt;hostname&gt;</b> : the string for the prompt, up to 64 characters are allowed. <b>&lt;ipv6_addr&gt;</b> : the corresponding IPv6 address for the host name, takes a dot decimal format. <b>all</b> : all of the host name
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.

<b>Example</b>	Set the IPv6 address of the host named Delhi to 2001:1:2:3::1.  <b>Switch(config)#ipv6 host Delhi 2001:1:2:3::1</b>
----------------	---

## ip http server

<b>Command</b>	<b>ip http server</b> <b>no ip http server</b>
<b>Parameter</b>	None.
<b>Default</b>	Enable.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Use this command to enable Web configuration.  The "no ip http server" command disables Web configuration.
<b>Example</b>	Enable Web Server function and enable Web configurations.  <b>Switch(config)#ip http server</b>

## login

<b>Command</b>	<b>login</b> <b>no login</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	No login by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Enable password.  <b>Switch(config)#login</b>

## password

<b>Command</b>	<b>password [0   7] &lt;password&gt;</b> <b>no password</b>
<b>Parameter</b>	<b>[0   7]:</b> if the input option is 0 on password setting, the password is not encrypted; if the input option is 7, the password is encrypted. <b>&lt;password&gt;:</b> password for the user.
<b>Default</b>	This password is empty by default by system.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	With this command, configure the password used to enter normal user mode on the console.  The "no password" command deletes this password.
<b>Example</b>	To configure the password used to enter normal user mode as test, password is not encrypted.  <b>Switch(config)#password 0 test</b>

## privilege

<b>Command</b>	<b>privilege mode level &lt;1-15&gt; LINE</b> <b>no privilege mode level &lt;1-15&gt; LINE</b>
<b>Parameter</b>	<b>mode:</b> register mode of the command, 'Tab' or '?' is able to show all register modes <b>&lt;1-15&gt;:</b> level, its range between 1 and 15 <b>LINE:</b> the command needs to be configured, it supports the command abbreviation.
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.



	<p>If the command line with the parameter, the parameter must be matched with the configured command.</p> <p>The no command restores the original level of the command.</p>
<b>Example</b>	<p>Change the level of show ip route command to level 5. Restore the original level of the show ip route command.</p> <p><b>Switch(config)#privilege exec level 5 show ip route</b> <b>Switch(config)#no privilege exec level 5 show ip route</b></p>

## reload

<b>Command</b>	<b>reload</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	The user can use this command to restart the switch continuously.
<b>Example</b>	<p>Hot restart switch.</p> <p><b>Switch#reload</b></p>

## service password-encryption

<b>Command</b>	<b>service password-encryption</b> <b>no service password-encryption</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	No service password-encryption by system default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p> <p>No service password-encryption cancels this function, however, encrypted passwords remain unchanged.</p>

<b>Example</b>	To encrypt system passwords.  <b>Switch(config)#service password-encryption</b>
----------------	---

### service terminal-length

<b>Command</b>	<b>service terminal-length &lt;0-512&gt;</b> <b>no service terminal-length</b>
<b>Parameter</b>	<b>&lt;0-512&gt;</b> : Columns of characters displayed on each screen of vty, ranging between 0-512.
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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 telnet.ssh client and the Console will be following this configuration. The "no service terminal-length" command cancels the screen shifting operation.
<b>Example</b>	Set the number of vty threads to 20.  <b>Switch(config)#service terminal-length 20</b>

### sysContact

<b>Command</b>	<b>sysContact&lt;LINE&gt;</b> <b>no sysContact</b>
<b>Parameter</b>	<b>&lt;LINE&gt;</b> : the prompt character string, range from 0 to 255 characters.
<b>Default</b>	The default is factory setting.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Set the factory contact mode to test.  <b>Switch(config)#sysContact test</b>

## sysLocation

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

## set default

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

## set boot password

<b>Command</b>	<b>set boot password</b> <b>no set boot password</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<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 configure it.</p> <p><b>Notice:</b> the characters length of the password is from 3 to 32.</p> <p>The no command cancels the password.</p>
<b>Example</b>	<p>Sets the password when entering boot mode.</p> <p><b>Switch(config)#set boot password</b> New password :***** Confirm password :***** Set password success!</p>

## setup

<b>Command</b>	<b>setup</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	Switch provides a Setup Mode, in which the user can configure IP addresses, etc.
<b>Example</b>	<p>Enter setup mode.</p> <p><b>Switch#setup</b></p>

## show clock

<b>Command</b>	<b>show clock</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	Displays the current system clock.
<b>Example</b>	<p>Displays the current system clock.</p> <p><b>Switch#show clock</b> Current time is TUE AUG 22 11 : 00 : 01 2002</p>

## show cpu usage

<b>Command</b>	<b>show cpu usage [&lt;slotno&gt;]</b>
<b>Parameter</b>	<b>[&lt;slotno&gt;]:</b> Specify slots
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	<p>Displays current, past 5 seconds, past 30 seconds, past 5 minutes CPU usage.</p> <p>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.</p>
<b>Example</b>	<p>Show the current usage rate of CPU.</p> <p><b>Switch#showcpu usage</b> Last 5 second CPU IDLE: 87% Last 30 second CPU IDLE: 89% Last 5 minute CPU IDLE: 89% From running CPU IDLE: 89%</p>

## show cpu utilization

<b>Command</b>	<b>show cpu utilization</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	This command is used to show CPU utilization rate in the past 5 seconds, 30 seconds and 5 minutes.
<b>Example</b>	To display CPU utilization.  <b>Switch#showcpu utilization</b> 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

<b>Command</b>	<b>show memory usage [&lt;slotno&gt;]</b>
<b>Parameter</b>	<b>[&lt;slotno&gt;]:</b> Specify slots
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Show the current usage rate of the memory.  <b>Switch#show memory usage</b> The memory total 128 MB, free 58914872 bytes, usage is 56.10%

## show privilege

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

## show privilege mode LINE

<b>Command</b>	<b>show privilege mode LINE</b>
<b>Parameter</b>	<b>mode:</b> register mode of the command, 'Tab' or '?' is able to show all register modes <b>LINE:</b> the command needs to be configured, it supports the command Abbreviation.
<b>Default</b>	None.
<b>Mode</b>	Admin Mode/Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Show the level of privilege command.  <b>Switch(config)#show privilege exec show ip route</b> The command : show ip route Privilege is : 15

## show tech-support

<b>Command</b>	<b>show tech-support [no-more]</b>
<b>Parameter</b>	<b>[no-more]:</b> Display the operational information and the task status of the switch directly, do not connect the user by "more".
<b>Default</b>	None.
<b>Mode</b>	Admin Mode/Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Displays the operational information and the task status of the switch.  <b>Switch#show tech-support</b>

## show version

<b>Command</b>	<b>show version</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode/Global Mode.
<b>Usage Guide</b>	This command is used to show the version of the switch, it includes the information of hardware version and the software version.
<b>Example</b>	Displays the version information of the switch.  <b>Switch#show version</b>



## username

<b>Command</b>	<b>username &lt;username&gt; [privilege &lt;privilege&gt;] [password [0   7]&lt;password&gt;]</b> <b>no username &lt;username&gt;</b>
<b>Parameter</b>	<b>&lt;username&gt;</b> : The username, its range should not exceed to 32 characters. <b>&lt;privilege&gt;</b> : 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. <b>[0   7]</b> : 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) <b>&lt;password&gt;</b> : password for the user
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	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.  <b>Switch(config)#username admin privilege 15 password 0 admin</b> <b>Switch(config)# username user1 privilege 1 password 7 4a7d1ed414474e4033ac29ccb8653d9b</b> <b>Switch(config)# username user2 password 0 user2</b> <b>Switch(config)# authentication line console login local</b>

## web-auth privilege <1-15>

<b>Command</b>	<b>web-auth privilege &lt;1-15&gt;</b> <b>no web-auth privilege</b>
<b>Parameter</b>	<b>&lt;1-15&gt;</b> : Appoint the level of logging in the switch by web and the range is from 1 to 15.
<b>Default</b>	The default level is 15.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure the level of logging in the switch by web as 10.  <b>Switch(config)# web-auth privilege 10</b>

## write

<b>Command</b>	<b>write</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None
<b>Mode</b>	Admin Mode/Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Save the current configuration.  <b>Switch#write</b>

## write running-config

<b>Command</b>	<b>write running-config [&lt;startup-config-file-name&gt;]</b>
<b>Parameter</b>	<b>write running-config [&lt;startup-config-file-name&gt;]:</b> the full path of the cfg file.
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	<p>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.</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>
<b>Example</b>	<p>Save the current running config as .cfg file with name of 123.</p> <p><b>Switch#write running-config 123.cfg</b></p>

## 2. Commands for Telnet

### aaa authorization config-commands

<b>Command</b>	<b>aaa authorization config-commands</b> <b>no aaa authorization config-commands</b>
<b>Parameter</b>	<b>none:</b> none
<b>Default</b>	By default, disable.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Enable VTY command authorization function.  <b>Switch(config)#aaa authorization config-commands</b>

### accounting exec

<b>Command</b>	<b>accounting line {console   vty} exec {start-stop   stop-only   none} method1 [method2...]</b> <b>no accounting line {console   vty} exec</b>
<b>Parameter</b>	<b>Console:</b> log in through serial port <b>Vty:</b> log in through telnet or ssh <b>start-stop:</b> sends the accounting start or the accounting stop when the user is logging or exit the login <b>stop-only:</b> sends the accounting stop when the user exits the login only <b>none:</b> does not send the accounting start or the accounting stop <b>method:</b> the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
<b>Default</b>	By default there is no accounting.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure the login accounting with the telnet method.  <b>Switch(config)#accounting line vty exec start-stop tacacs</b>

### accounting command

<b>Command</b>	<b>accounting line {console   vty} command &lt;1-15&gt; {start-stop   stop-only [none] method1 [method2...]} no accounting line {console   vty} command &lt;1-15&gt;</b>
<b>Parameter</b>	<b>console:</b> log in through serial port <b>vty:</b> log in through telnet or ssh <b>command &lt;1-15&gt;:</b> the level of the accounting command <b>start-stop:</b> sends the accounting start or the accounting stop when the user is logging or exit the login <b>stop-only:</b> sends the accounting stop when the user exits the login only <b>none:</b> does not send the accounting start or the accounting stop <b>method:</b> the list of the accounting method, it only supports tacacs keyword; tacacs uses the remote TACACS+ server to count
<b>Default</b>	By default there is no accounting method.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure command audit methods through telnet login, command level 15.

### authentication enable

<b>Command</b>	<b>authentication enable method1 [method2...] no authentication enable</b>
<b>Parameter</b>	<b>method :</b> 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

	<p>authenticate ;</p> <p>radius: uses the remote RADIUS authentication server to authenticate.</p>
<b>Default</b>	The local authentication is enable command by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>Configures 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 configured 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 is used. And TACACS server should be configured before the TACACS configuration method is used.</p> <p>The no command restores the default authentication method.</p>
<b>Example</b>	<p>Configure the enable authentication method to be tacacs and local.</p> <p><b>Switch(config)#authentication enable tacacs local</b></p>

### authentication ip access-class

<b>Command</b>	<p><b>authentication ip access-class {&lt;num-std&gt; &lt;name&gt;}</b></p> <p><b>no authentication ip access-class</b></p>
<b>Parameter</b>	<p><b>&lt;num-std&gt;</b>: the access-class number for standard numeric ACL, ranging between 1-99.</p> <p><b>&lt;name&gt;</b>: the access-class name for standard ACL, the character string length is ranging between 1 and 32.</p>
<b>Default</b>	The binding ACL to Telnet/SSH/Web function is closed by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>Binding standard IP ACL protocol to login with Telnet/SSH/Web.</p> <p>The no form command will cancel the binding ACL.</p>

<b>Example</b>	Binding standard IP ACL protocol to access-class 1.  <b>Switch(config)#authentication ip access-class 1 in</b>
----------------	--

### authentication ipv6 access-class

<b>Command</b>	<b>authentication ipv6 access-class {&lt;num-std&gt; &lt;name&gt;} no authentication ipv6 access-class</b>
<b>Parameter</b>	<b>&lt;num-std&gt;</b> : the access-class number for standard numeric ACL, ranging between 500-599. <b>&lt;name&gt;</b> : the access-class name for standard ACL, the character string length is ranging between 1 and 32.
<b>Default</b>	The binding ACL to Telnet/SSH/Web function is closed by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Binding standard IPv6 ACL protocol to login with Telnet/SSH/Web.  The no form command will cancel the binding ACL.
<b>Example</b>	Binding standard IP ACL protocol to access-class 500.  <b>Switch(config)#authentication ipv6 access-class 500 in</b>

### authentication line login

<b>Command</b>	<b>Authentication line {console   vty   web} login method1 [method2...] no authentication line {console   vty   web} login</b>
<b>Parameter</b>	<b>console</b> : log in through serial port <b>vty</b> : log in through telnet or ssh <b>web</b> : log in through web <b>method</b> : 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
<b>Default</b>	No configuration is enabled for the console login method by default. Local authentication is enabled for the VTY and Web login method by

	default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p> <p>When login method is configured 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 configuration 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 of command restores the default authentication method.</p>
<b>Example</b>	<p>Configure the telnet and ssh login with the remote RADIUS authentication.</p> <p><b>Switch(config)#authentication line vty login radius</b></p>



## authentication securityip

<b>Command</b>	<b>authentication securityip&lt;ip-addr&gt;</b> <b>no authentication securityip&lt;ip-addr&gt;</b>
<b>Parameter</b>	<b>&lt;ip-addr&gt;</b> : The trusted IP address of the client in dotted decimal format which can login into the switch.
<b>Default</b>	No trusted IP address is configured by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	To configure 192.168.1.21 as the trusted IP address.  <b>Switch(config)#authentication securityip 192.168.1.21</b>

## authentication securityipv6

<b>Command</b>	<b>authentication securityipv6 &lt;ipv6-addr&gt;</b> <b>no authentication securityipv6 &lt;ipv6-addr&gt;</b>
<b>Parameter</b>	<b>&lt;ip-addr&gt;</b> : the security IPv6 address which can login the switch.
<b>Default</b>	No security IPv6 addresses are configured by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure the security IPv6 address is 2001:da8:123:1::1.  <b>Switch(config)#authentication securityipv6 2001:da8:123:1::1</b>

## authorization

<b>Command</b>	<b>authorization line {console   vty   web} exec method [method...] no authorization line {console   vty   web} exec</b>
<b>Parameter</b>	<p><b>console:</b> log in through serial port</p> <p><b>vty:</b> log in through telnet or ssh</p> <p><b>web:</b> log in through web</p> <p><b>method:</b> the list of the authentication method, it must be among local, tacacs and radius keywords ;</p> <p>local: uses the local database to authenticate ;</p> <p>tacacs: uses the remote TACACS+ authentication server to authenticate ;</p> <p>radius: uses the remote RADIUS authentication server to authenticate</p>
<b>Default</b>	There is no authorization method by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</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 is used. And TACACS server should be configured before the TACACS configuration method is 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>
<b>Example</b>	<p>To configure the telnet authorization method to RADIUS.</p> <p><b>Switch(config)#authorization line vty exec radius</b></p>

## authorization line vty command

<b>Command</b>	<b>authorization line vty command &lt;1-15&gt; {local   radius   tacacs} (none )</b> <b>no authorization line vty command &lt;1-15&gt;</b>
<b>Parameter</b>	<b>command &lt;1-15&gt;:</b> Level scope of authorization orders 1~15. <b>local:</b> Authorization is granted locally. <b>radius:</b> Authorization for remote radius <b>tacacs:</b> Authorization for remote tacacs <b>none:</b> Authorization mode is empty
<b>Default</b>	The authorization manner is not configured as default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p>
<b>Example</b>	Configure level 1 command authorization manner of telnet login user as TACACS.  <b>Switch(config)#authorization line vty command 1 tacacs</b>

### clear line vty<0-31>

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

### crypto key clear rsa

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

## terminal length

<b>Command</b>	<b>terminal length &lt;0-512&gt;</b> <b>terminal no length</b>
<b>Parameter</b>	<b>&lt;0-512&gt;</b> : Length of characters displayed in each screen, ranging between 0-512 (0 refers to non-stop display).
<b>Default</b>	Default Length is 25.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure length of characters in each display to 20.  <b>Switch#terminal length 20</b> ssh is closed successfully.

## telnet

<b>Command</b>	<b>telnet [vrf&lt;vrf-name&gt;] {&lt;ip-addr&gt;   &lt;ipv6-addr&gt;   host &lt;hostname&gt;}[&lt;port&gt;]</b>
<b>Parameter</b>	<b>&lt;vrf-name&gt;</b> : the specific VRF name <b>&lt;ip-addr&gt;</b> : the IP address of the remote host, shown in dotted decimal notation <b>&lt;ipv6-addr&gt;</b> : the IPv6 address of the remote host <b>&lt;hostname&gt;</b> : the name of the remote host, containing max 64 characters <b>&lt;port&gt;</b> : the port number, ranging between 0 and 65535
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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+ \".

	<p>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.</p>
<b>Example</b>	<p>The switch telnets to a remote host whose IP address is 20.1.1.1.</p> <p><b>Switch#telnet 20.1.1.1 23</b></p> <p>Connecting Host 20.1.1.1 Port 23...          Service port is 23          Connected to 20.1.1.1          login:123          password:***          router&gt;</p>

### telnet server enable

<b>Command</b>	<p><b>telnet server enable</b>  <b>no telnet server enable</b></p>
<b>Parameter</b>	<p><b>none: none</b></p>
<b>Default</b>	<p>None.</p>
<b>Mode</b>	<p>Global Mode.</p>
<b>Usage Guide</b>	<p>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.</p> <p>The "no telnet server enable "command disables the Telnet function in the switch.</p>
<b>Example</b>	<p>Disable the Telnet server function in the switch.</p> <p><b>Switch(config)#no telnet server enable</b></p>

## telnet-server max-connection

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

## ssh-server authentication-retries

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

## ssh-server enable

<b>Command</b>	<b>ssh-server authentication-retries &lt;authentication-retries&gt;</b> <b>no ssh-server authentication-retries</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	SSH function is disabled by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Enable SSH function on the switch.  <b>Switch(config)#ssh-server enable</b>

## ssh-server host-key create rsa

<b>Command</b>	<b>ssh-server host-key create rsa [modulus &lt; modulus &gt;]</b>
<b>Parameter</b>	<b>&lt; modulus &gt;</b> : the modulus is used to compute the host key; valid range is 768 to 2048. The default value is 1024.
<b>Default</b>	The system uses the key generated when the ssh-server started at the first time.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	To generate new host key.  <b>Switch(config)#ssh-server host-key create rsa</b>



## ssh-server max-connection

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

## ssh-server timeout

<b>Command</b>	<b>ssh-server timeout &lt;timeout&gt;</b> <b>no ssh-server timeout</b>
<b>Parameter</b>	<b>&lt;timeout&gt;</b> : timeout value; valid range is 10 to 600 seconds
<b>Default</b>	SSH authentication timeout is 180 seconds by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Configures timeout value for SSH authentication.  The "no ssh-server timeout" command restores the default timeout value for SSH authentication.
<b>Example</b>	Set SSH authentication timeout to 240 seconds.  <b>Switch(config)#ssh-server timeout 240</b>

### show crypto key

<b>Command</b>	<b>show crypto key</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	Shows the secret key of ssh.
<b>Example</b>	Show the secret key of ssh.  <b>Switch#show crypto key</b>

### show ssh-server

<b>Command</b>	<b>show ssh-server</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	None.
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	Displays SSH state and users which log on currently.
<b>Example</b>	Display SSH state and users which log on currently.  <b>Switch#showssh-server</b> 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

<b>Command</b>	<b>show telnet login</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.

<b>Example</b>	To display SSH state and users which log on currently.  <b>ssh-server login user number 2</b>
----------------	---

### show users

<b>Command</b>	<b>show users</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Displays user information.  <b>Switch#show users</b> <b>Line User Location</b> 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

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

## 3. Commands for Configuring Switch IP

### interface vlan

<b>Command</b>	<b>interface vlan&lt;vlan-id&gt;</b> <b>no interface vlan&lt;vlan-id&gt;</b>
<b>Parameter</b>	<b>&lt;vlan-id&gt;</b> : the VLAN ID of an existing VLAN, ranging from 1 to 4094.
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Enter the VLAN interface configuration mode of VLAN1.  <b>Switch(config)#interface vlan 1</b> <b>Switch(Config-if-Vlan1)#</b>

### ip address

<b>Command</b>	<b>ip address &lt;ip-address&gt;&lt;mask&gt; [secondary]</b> <b>no ip address [&lt;ip-address&gt;&lt;mask&gt;] [secondary]</b>
<b>Parameter</b>	<b>&lt;ip-address&gt;</b> : the IP address in dot decimal format <b>&lt;mask&gt;</b> : the subnet mask in dot decimal format <b>[secondary]</b> : indicates the IP configured is a secondary IP address
<b>Default</b>	No IP address is configured upon switch shipment.
<b>Mode</b>	VLAN Interface Mode.
<b>Usage Guide</b>	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.

<b>Example</b>	<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

<b>Command</b>	<pre>ipv6 address &lt;ipv6address   prefix-length&gt; [eui-64] no ipv6 address &lt;ipv6address   prefix-length&gt; [eui-64]</pre>
<b>Parameter</b>	<p><b>&lt;ipv6address &gt;</b>: the prefix of an IPV6 address.</p> <p><b>&lt;prefix-length&gt;</b>: the length of the prefix of an IPV6 address, ranging from 3 to 128.</p> <p><b>[eui-64]</b>: means that the eui64 interface id of the interface will automatically create an IPV6 address.</p>
<b>Default</b>	No IPv6 address is configured upon switch shipment.
<b>Mode</b>	VLAN Interface Mode.
<b>Usage Guide</b>	<p>Configures aggregately 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>
<b>Example</b>	<p>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.</p> <pre>Switch(config)#interface vlan 1 Switch(Config-if-Vlan1)# Switch(Config-if-Vlan1)#exit Switch(config)#</pre>

## ipbootp-client enable

<b>Command</b>	<b>ipbootp-client enable</b> <b>no ipbootp-client enable</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	BootP client function is disabled by default.
<b>Mode</b>	VLAN Interface Mode.
<b>Usage Guide</b>	<p>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.</p> <p>The no command disables the BootP Client function and releases the IP address obtained in BootP.</p>
<b>Example</b>	<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>

## ipdhcp-client enable

<b>Command</b>	<b>ipdhcp-client enable</b> <b>no ipdhcp-client enable</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	By default, the dhcp service is disabled.
<b>Mode</b>	VLAN Interface Mode.
<b>Usage Guide</b>	<p>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.</p>

	No command disables the DHCP client function and releases the IP address obtained in DHCP.
<b>Example</b>	<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

<b>Command</b>	<b>rmon enable</b> <b>no rmon enable</b>
<b>Parameter</b>	None.
<b>Default</b>	RMON is enabled by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	This command is used to enable RMON remote network monitoring protocol.  The no command disables RMON.
<b>Example</b>	To disable RMON.  <b>Switch(config)#no rmon enable</b>

### show private-mib oid

<b>Command</b>	<b>show private-mib oid</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Shows the original oid of the private mib. Check the beginning oid of the private mib by show private-mib oid command.
<b>Example</b>	Show the original oid of the private mib.  <b>Switch#show private-mib oid</b> Private MIB OID:1.3.6.1.4.1.6339



## show snmp

<b>Command</b>	<b>show snmp</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays all SNMP counter information.
<b>Example</b>	<p>Display all SNMP counter information.</p> <pre> <b>Switch#showsnmp</b> 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 </pre>

## show snmpengineid

<b>Command</b>	<b>show snmpengineid</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays the engine ID commands.
<b>Example</b>	Display the engine ID commands.

	<b>Switch#showsnmpengineid</b> SNMP engineID:3138633303f1276c
--	--

### show snmp group

<b>Command</b>	<b>show snmp group</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays the group information.
<b>Example</b>	Display the group information.  <b>Switch#showsnmp group</b> Group Name: initial Security Level: noAuthnoPriv Read View: one Write View:<no writeview specified> Notify View: one

### show snmp mib

<b>Command</b>	<b>show snmp mib</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays all MIB supported by the switch.
<b>Example</b>	Display all MIB supported by the switch.  <b>Switch#showsnmp mib</b>

## show snmp status

<b>Command</b>	<b>show snmp status</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays SNMP configuration information.
<b>Example</b>	<p>Display SNMP configuration information.</p> <p><b>Switch#showsnmp status</b>            Trap enable            RMON enable            Community Information:            V1/V2c Trap Host Information:            V3 Trap Host Information:            Security IP Information:</p>

## show snmp user

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

## show snmp view

<b>Command</b>	<b>show snmp view</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and configuration mode.
<b>Usage Guide</b>	Displays the view information.
<b>Example</b>	<p>Display the view information.</p> <pre>Switch#showsnmp view View Name: readview 1. -Included active 1.3. Excluded active</pre>

## snmp-server community

<b>Command</b>	<pre>snmp-server community {ro   rw} {0   7} &lt;string&gt; [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}] [read &lt;read- view-name&gt;] [write &lt;write-view-name&gt;] no snmp-server community {ro   rw} {0   7} &lt;string&gt; [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}]</pre>
<b>Parameter</b>	<p><b>{ro   rw}</b>: The specified access mode to MIB, ro for read-only and rw for read-write</p> <p><b>{0   7}</b>: 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.</p> <p><b>&lt;string&gt;</b>: The configured community string.</p> <p><b>&lt;num-std&gt;</b>: The access-class number for standard numeric ACL, ranging between 1-99.</p> <p><b>&lt;name&gt;</b>: The access-class name for standard ACL, the character string length is ranging between 1-32.</p> <p><b>&lt;ipv6-num-std&gt;</b>: The access-class number for standard numeric IPv6 ACL, ranging between 500-599.</p> <p><b>&lt;ipv6-name&gt;</b>: The access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.</p> <p><b>&lt;read-view-name&gt;</b>: The name of readable view which includes 1-32 characters.</p>

	<b>&lt;write-view-name&gt;</b> : The name of writable view which includes 1-32 characters.
<b>Default</b>	None.
<b>Mode</b>	Global mode.
<b>Usage Guide</b>	<p>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.</p> <p>The no command deletes the configured community string.</p>
<b>Example</b>	<p>Add a community string named "private" with read-write permission.</p> <p><b>Switch(config)#snmp-server community rw 0 private</b></p> <p>Delete the community string named "private".</p> <p><b>Switch(config)#no snmp-server community 0 private</b></p>

### snmp-server enable

<b>Command</b>	<b>snmp-server enable</b> <b>no snmp-server enable</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p> <p>The "no snmp-server enable" command disables the SNMP proxy server function.</p>
<b>Example</b>	<p>Enable the SNMP proxy server function on the switch.</p> <p><b>Switch(config)#snmp-server enable</b></p>

## snmp-server enable traps

<b>Command</b>	<b>snmp-server enable traps</b> <b>no snmp-server enable traps</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	By default, forbid to send Trap message.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Enable to send Trap messages.  <b>Switch(config)#snmp-server enable traps</b>

## snmp-server engineid

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

## snmp-server group

<b>Command</b>	<pre>snmp-server group &lt;group-string&gt; {NoauthNopriv   AuthNopriv   AuthPriv} [[read &lt;read-string&gt;] [write &lt;write-string&gt;] [notify &lt;notify-string&gt;]] [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}] no snmp-server group &lt;group-string&gt; {NoauthNopriv   AuthNopriv   AuthPriv} [access {&lt;num-std&gt;   &lt;name&gt;}] [ipv6-access {&lt;ipv6-num-std&gt;   &lt;ipv6-name&gt;}]</pre>
<b>Parameter</b>	<p><b>&lt;group-string&gt;</b>: Group name which includes 1-32 characters</p> <p><b>NoauthNopriv</b>: Applies the non-recognizing and non-encrypting safety level</p> <p><b>AuthNopriv</b>: Applies the recognizing but non encrypting safety level</p> <p><b>AuthPriv</b>: Applies the recognizing and encrypting safety level</p> <p><b>&lt;read-string&gt;</b>: Name of readable view which includes 1-32 characters</p> <p><b>&lt;write-string&gt;</b>: Name of writable view which includes 1-32 characters</p> <p><b>&lt;notify-string&gt;</b>: Name of trappable view which includes 1-32 characters</p> <p><b>&lt;num-std&gt;</b>: the access-class number for standard numeric ACL, ranging between 1-99</p> <p><b>&lt;name&gt;</b>: the access-class name for standard ACL, the character string length is ranging between 1-32</p> <p><b>&lt;ipv6-num-std&gt;</b>: the access-class number for standard numeric IPv6 ACL, ranging between 500-599</p> <p><b>&lt;ipv6-name&gt;</b>: the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32.</p>
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Configures the engine ID.
<b>Example</b>	<p>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.</p> <pre>Switch (config)#snmp-server group CompanyGroupAuthPriv read readview</pre>

## snmp-server host

<b>Command</b>	<pre>snmp-server host { &lt;host-ipv4-address&gt;   &lt;host-ipv6- address&gt; } {v1   v2c   {v3 {NoauthNopriv   AuthNopriv   AuthPriv}}} &lt;user-string&gt; no snmp-server host { &lt;host-ipv4-address&gt;   &lt;host-ipv6- address&gt; } {v1   v2c   {v3 {NoauthNopriv   AuthNopriv   AuthPriv}}}</pre>
<b>Parameter</b>	<p><b>&lt;host-ipv4-address&gt;</b>: IP address of NMS management station which receives Trap message</p> <p><b>&lt;host-ipv6-address&gt;</b>: IPv6 address of NMS management station which receives Trap message</p> <p><b>v1   v2c   v3</b>: The version number when sending the trap</p> <p><b>NoauthNopriv</b>: Applies the non-recognizing and non-encrypting safety level</p> <p><b>AuthNopriv</b>: Applies the recognizing but non encrypting safety level</p> <p><b>AuthPriv</b>: Applies the recognizing and encrypting safety level</p> <p><b>&lt;user-string&gt;</b>: the community character string applied when sending the Trap message at v1/v2, and will be the user name at v3</p>
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p> <p>The "no" form of this command cancels this IPv4 or IPv6 address.</p>
<b>Example</b>	Configure an IP address to receive Trap.



## snmp-server securityip

<b>Command</b>	<b>snmp-server securityip {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;} no snmp-server securityip {&lt;ipv4-address&gt;   &lt;ipv6-address&gt;}</b>
<b>Parameter</b>	<b>&lt;ipv4-address&gt;</b> : NMS security IPv4 address, dotted decimal notation <b>&lt;ipv6-address&gt;</b> : NMS security IPv6 address, colon hexadecimal
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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 management 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.
<b>Example</b>	To configure security IP address of NMS management station.  <b>Switch(config)#snmp-server securityip 1.1.1.5</b>

## snmp-server securityip enable

<b>Command</b>	<b>snmp-server securityip {enable   disable}</b>
<b>Parameter</b>	<b>enable   disable</b> : SNMP security ip configuration enabled or disabled
<b>Default</b>	Enable the security IP address authentication function.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	Enables/disables the security IP address authentication on NMS management station.
<b>Example</b>	Disable the security IP address authentication function.  <b>Switch(config)#snmp-server securityip disable</b>

## snmp-server trap-source

<b>Command</b>	<b>snmp-server trap-source</b> {<ipv4-address>   <ipv6-address>} <b>no snmp-server trap-source</b> {<ipv4-address>   <ipv6-address>}
<b>Parameter</b>	<b>&lt;ipv4-address&gt;</b> : IPv4 address is used to send trap packet in dotted decimal Notation <b>&lt;ipv6-address&gt;</b> : IPv6 address is used to send trap packet in colon hexadecimal
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	To set the IP address which is used to send trap packet.  <b>Switch(config)#snmp-server trap-source 1.1.1.5</b>

## snmp-server user

<b>Command</b>	<b>snmp-server user</b> <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>}]  <b>no snmp-server user</b> <user-string> [access {<num-std> <name>}] [ipv6-access {<ipv6-num-std> <ipv6-name>}]
<b>Parameter</b>	<b>&lt;use-string&gt;</b> : the user name containing 1-32 characters <b>&lt;group-string&gt;</b> : the name of the group the user belongs to, containing 1-32 characters <b>authPriv</b> : use DES for the packet encryption <b>authNoPriv</b> : not use DES for the packet encryption <b>auth</b> : perform packet authentication <b>md5</b> : packet authentication using HMAC MD5 algorithm <b>sha</b> : packet authentication using HMAC SHA algorithm <b>3des</b> : packet authentication using 3DES to encrypt <b>aes</b> : packet authentication using AES to encrypt <b>des</b> : packet authentication using DES to encrypt

	<p><b>&lt;word&gt;</b>: user password, containing 8-32 character</p> <p><b>&lt;num-std&gt;</b>: the access-class number for standard numeric ACL, ranging between 1-99</p> <p><b>&lt;name&gt;</b>: the access-class name for standard ACL, the character string length is ranging between 1-32</p> <p><b>&lt;ipv6-num-std&gt;</b>: the access-class number for standard numeric IPv6 ACL, ranging between 500-599</p> <p><b>&lt;ipv6-name&gt;</b>: the access-class name for standard IPv6 ACL, the character string length is ranging between 1-32</p>
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>Adds 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>
<b>Example</b>	<p>Add a new user tester in the User Group with HMAC md5 for authentication, the password is hellohello; delete a User.</p> <p><b>Switch (config)#</b> <b>Switch (config)#no snmp-server user tester</b></p>

### snmp-server view

<b>Command</b>	<p><b>snmp-server view &lt;view-string&gt;&lt;oid-string&gt; {include   exclude}</b> <b>no snmp-server view &lt;view-string&gt; [ &lt;oid-string&gt; ]</b></p>
<b>Parameter</b>	<p><b>&lt;view-string&gt;</b>: view name, containing 1-32 characters</p> <p><b>&lt;oid-string&gt;</b>: OID number or corresponding node name, containing 1-255 characters</p> <p><b>include   exclude</b>: include/exclude this OID</p>
<b>Default</b>	None.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<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</p>

	<p>node name of the parameter.</p> <p>The "no" form of this command deletes the view information.</p>
<b>Example</b>	<p>Create a view named readview, include iso nodes but not iso.3 nodes, and then delete them.</p> <p><b>Switch(config)#snmp-server view readview iso include</b>  <b>Switch(config)#snmp-server view readview iso.3 exclude</b></p> <p><b>Switch(config)#no snmp-server view readview</b></p>

### switchport updown notification enable

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

## 5. Commands for Switch Upgrade

### copy (FTP)

<b>Command</b>	<b>copy &lt;source-url&gt;&lt;destination-url&gt; [ascii   binary]</b>														
<b>Parameter</b>	<p><b>&lt;source-url&gt;</b>: the location of the source files or directories to be copied</p> <p><b>&lt;destination-url&gt;</b>: the destination address to which the files or directories to be copied</p> <p><b>ascii</b>: ASCII standards will be adopted</p> <p><b>binary</b>: File transfer will be in binary mode (default transfer method)</p>														
<b>Default</b>	None.														
<b>Mode</b>	Admin Mode.														
<b>Usage Guide</b>	<p>This command is used to transfer files by TFP.</p> <p>When URL represents an FTP address, it should be:  ftp://&lt;username&gt;:&lt;password&gt;@{&lt;ipaddress&gt; &lt;ipv6address&gt; &lt;hostname&gt; }/&lt;filename&gt;, a mongst&lt;username&gt; is the FTP user name, &lt;password&gt; is the FTP user password, &lt;ipaddress&gt; &lt;ipv6address&gt; is the IPv4 or IPv6 address of the FTP server/client, &lt;hostname&gt; 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, &lt;filename&gt; is the name of the FTP upload/download file.</p> <p>Special keywords of the filename</p> <table border="1"> <thead> <tr> <th>keywords</th> <th>explanation</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>This command supports command line hints, namely if the user can enter commands in following forms: copy &lt;filename&gt; ftp:// or copy ftp:// &lt;filename&gt; and press Enter, following hints will be provided by the system :</p> <p>ftp server ip/ipv6 address [x.x.x.x]/[x::x:x] &gt;</p>	keywords	explanation	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	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	explanation														
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														
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														

	<pre>ftp username&gt; ftp password&gt; ftp filename&gt; Requesting for FTP server address, user name, password and file name</pre>
<b>Example</b>	<p>To save images in the FLASH to the FTP server of 10.1.1.1, FTP server username is Switch, password is superuser:</p> <p><b>Switch#copy nos.img ftp://Switch:superuser@10.1.1.1/nos.img</b> Obtain system file nos.img from the FTP server 10.1.1.1, the username is Switch, password is superuser</p> <p><b>Switch#copy ftp://Switch:superuser@10.1.1.1/nos.img nos.img</b> To save the running configuration files.</p> <p><b>Switch#copy running-config startup-config</b></p>

### copy (TFTP)

<b>Command</b>	<b>copy &lt;source-url&gt;&lt;destination-url&gt; [ascii   binary]</b>
<b>Parameter</b>	<p><b>&lt;source-url&gt;</b>: the location of the source files or directories to be copied</p> <p><b>&lt;destination-url&gt;</b>: the destination address to which the files or directories to be copied</p> <p><b>ascii</b>: ASCII standards will be adopted</p> <p><b>binary</b>: File transfer will be in binary mode (default transfer method)</p>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	<p>This command is used to transfer files by TFTP.</p> <p>When URL represents a TFTP address, it should be: tftp://{&lt;ipaddress&gt; &lt;ipv6address&gt; &lt;hostname&gt;}/&lt;filename&gt;, among st &lt;ipaddress&gt; </p> <p>&lt;ipv6address&gt; is the IPv4 or IPv6 address of the TFTP server/client, &lt;hostname&gt; 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, &lt;filename&gt; is the name of the TFTP upload/download file.</p> <p>Special keyword of the filename</p>

	<b>keywords</b>	<b>explanation</b>
	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
	<p>This command supports command line hints, namely if the user can enter commands in following forms: copy &lt;filename&gt; tftp:// or copy tftp:// &lt;filename&gt; and press Enter, following hints will be provided by the system:tftp server ip/ipv6 address[x.x.x.x]/[x::x::x]&gt;tftp filename&gt;            Requesting for TFTP server address, file name</p>	
<b>Example</b>	<p>Save images in the FLASH to the TFTP server of 10.1.1.1  <b>Switch#copy nos.img tftp://10.1.1.1/nos.img</b>            Obtain system file nos.img from the TFTP server 10.1.1.1  <b>Switch#copy tftp://10.1.1.1/nos.img nos.img</b>            Save the running configuration files  <b>Switch#copy running-config startup-config</b></p>	

## ftp-dir

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

## ftp-server enable

<b>Command</b>	<b>ftp-server enable</b> <b>no ftp-server enable</b>
<b>Parameter</b>	<b>none: none</b>
<b>Default</b>	FTP server is not started by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>This command is used to start the FTP server. 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>
<b>Example</b>	<p>Enable FTP server services.</p> <p><b>Switch(config)# ftp-server enable</b></p>

## ftp-server timeout

<b>Command</b>	<b>ftp-server timeout &lt;seconds&gt;</b>
<b>Parameter</b>	<b>&lt;seconds&gt;</b> : the idle time threshold (in seconds) for FTP connection, the valid range is 5 to 3600
<b>Default</b>	The system default is 600 seconds.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	<p>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.</p>
<b>Example</b>	<p>Modify the idle threshold to 100 seconds.</p> <p><b>Switch(config)#ftp-server timeout 100</b></p>



## ip ftp

<b>Command</b>	<b>ip ftp username &lt;username&gt; password [0   7] &lt;password&gt;</b> <b>no ip ftp username &lt;username&gt;</b>
<b>Parameter</b>	<b>&lt;username&gt;</b> : the username of the FTP link, its range should not be exceeded to 32 characters <b>[0   7]</b> : 0 means password is not encrypted ,7 means password is encrypted <b>&lt;password&gt;</b> : FTP link password
<b>Default</b>	The system uses anonymous FTP links by default.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Configure the username as Switch and the password as superuser.  <b>Switch(config)#ip ftp username Switch password 0 superuser</b>

## show ftp

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

## show tftp

<b>Command</b>	<b>show tftp</b>
<b>Parameter</b>	None.
<b>Default</b>	None.
<b>Mode</b>	Admin and Global Mode.
<b>Usage Guide</b>	Displays the parameter settings for the TFTP server.
<b>Example</b>	Display the parameter settings for the TFTP server.  <b>Switch#showtftp</b> timeout : 60 Retry Times : 10

## tftp-server enable

<b>Command</b>	<b>tftp-server enable</b> <b>no tftp-server enable</b>
<b>Parameter</b>	None.
<b>Default</b>	Disable TFTP Server.
<b>Mode</b>	Global Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Start the TFTP server.  <b>Switch(config)#tftp-server enable</b>

### tftp-server retransmission-number

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

### tftp-server transmission-timeout

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

## 6. Commands for File System

### cd

<b>Command</b>	<b>cd &lt;directory&gt;</b>
<b>Parameter</b>	<b>&lt;directory&gt;</b> : the sub-directory name, a sequence of consecutive characters whose length ranges from 1 to 80.
<b>Default</b>	The default working directory is Flash.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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.
<b>Example</b>	Change the working directory of the current storage device to flash.  <b>Switch#cd flash:</b> <b>Switch#pwd</b> flash:/

### copy

<b>Command</b>	<b>copy &lt;source-file-url&gt;&lt;dest-file-url&gt;</b>
<b>Parameter</b>	<b>&lt;source-file-url&gt;</b> : The source address of the file or directory to be copied <b>&lt;dest-file-url&gt;</b> : The destination address of the file or directory to be copied
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	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: <ul style="list-style-type: none"> <li>o starting with "flash:"</li> <li>o "ftp://username:pass@server-ip/file-name"</li> <li>o "tftp://server-ip/file-name"</li> </ul>

	<p>2. The prefix of the destination file URL should be in one of the following forms:</p> <ul style="list-style-type: none"> <li>o starting with "flash:/"</li> <li>o "ftp://username:pass@server-ip/file-name"</li> <li>o "tftp://server-ip/file-name"</li> </ul> <p>When the prefix of the source file URL is ftp:// or tftp://, that of the destination file URL should not be either of them.</p> <p>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.</p> <p>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.</p>
<b>Example</b>	<p>Copy the file "flash:/nos.img" and store it as "flash/ 6.1.11.0.img".</p> <pre>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</pre>

## delete

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

## dir

<b>Command</b>	<b>dir [WORD]</b>
<b>Parameter</b>	<b>[WORD]:</b> The name of the shown directory. There may be the following formats: directory name, slot-xx#directory name, flash:/directory name, cf:/directory name.
<b>Default</b>	No <WORD> means to display information of the current working directory.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	Displays the information of the designated directory on the storage device. This command does not support a recursive display of all sub-directories.
<b>Example</b>	<p>Display information of the directory "flash:/".</p> <pre> <b>Switch#dir flash:/</b> 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) <b>Switch#</b> </pre>

## pwd

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

## rename

<b>Command</b>	<b>rename &lt;source-file-url&gt;&lt;new-filename &gt;</b>
<b>Parameter</b>	<p><b>&lt;source-file-url&gt;</b>: the source file, in which whether specifying or not its path are both acceptable.</p> <p><b>&lt;new-filename &gt;</b>: filename without specifying its path.</p>
<b>Default</b>	None.
<b>Mode</b>	Admin Mode.
<b>Usage Guide</b>	<p>Used to rename a designated file on the switch.</p> <p>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.</p>
<b>Example</b>	<p>Change the name of file "nos.img" in the current working directory to "nos-6.1.11.0.img".</p> <p><b>Switch# rename nos5.img nos-6.1.11.0.img</b>  Rename flash:/nos5.img to flash:/nos-6.1.11.0.img ok !</p>