Chapter 2: System Management

Table of Contents

Chapter 2 System Management

2.1 System Maintenance

2.1.1 Display System Status Information

Operation	Command	Remarks
Display version information	**display version**	
Display user information	**display terminal user**	
Display logged-in user information	**display login-users**	
Display system memory information	**display memory**	
Display system clock	**display time**	
Display system CPU utilization	**display cpu-info**	

【Example】

！   Display   system   version

[Switch]display version

2.1.2 Configure the System Clock

Operation	Command	Remarks
Enter super user view	**Enable**	
Set system clock	**time** HH:MM:SS YYYY/MM/DD	
Enter global configuration mode	**system-view**	

Set clock timezone	**time** zone*name hour minute*	
display system time	**display time**	

【Example】

！Set the system clock to 8:30: 0 on October 1, 2020

[Switch]time 08:30:0 2020/10/01

2.1.3 Configure System Host Name

Operation	Command	Remarks
Enter super user view	**enable**	
Enter global configuration mode	**system-view**	
Configure the host name	**SW** *SW*	
Delete the host name	**undo SW**	

【**Example**】

！Set the host name to Switch-ABCD [Switch]SW

Switch-ABCD

[Switch-ABCD]

2.1.4 Trace Route Command

Support tracert command and check network connection. The tracert command can be executed in any view：

Operation	Command	Remarks
Tracert test	**tracert** [-u	-c] [-p *udpport*	-f *first_ttl*	-h *maximum_hops*	-w *time_out*] *target_name*	

【*Parameter Description*】

-u：Send udp message;

-c：Send echo message of icmp;

-p udpport：The destination port , the value range is 1-65535, the default port is 62929;

-f first_ttl：The initial ttl value, the value range is 1-255, the default value is 1;

-h maximum_hops：The maximum ttl value, the value range is 1-255, the default value is 30;

-w time_out：The timeout period for waiting for a response, the value range is 10-60 seconds, and the default value is 10 seconds;

target_name：Destination host or router address

3

【**Example**】

！Trace the route that can reach 192.168.1.2

<Switch>tracert 192.168.1.2

2.1.5 Port Loopback Test Command

The system supports port loopback test function, used to test the internal and external connectivity of the port：

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Loopback test on all ports	**loopback** {internal | **external}**	
Enter interface view	**interface** {ethernet *interface-num*} | interface-name}	
Loopback test on a single port	**loopback** {internal | **external}**	

2.1.6 Line Detection VCT Command

VCT is used to detect network cable normal (NORMAL), open circuit (OPEN), short circuit (SHORT), impedance mismatch (IMPEDANCE MISMATCH) and other error conditions.

The normal connection of the network cable is NORMAL, the disconnection of the network cable is OPEN, and the short circuit of the network cable is SHORT. Impedance mismatch (IMPEDANCE MISMATCH) generally occurs when two network cables with different impedances are connected together. If an error is found, the location of the error can be detected. The longest detection distance of VCT is 181 meters for 100M ports and 175 metersfor Gigabit ports：

Operation	Command	Remarks
Enter global configuration mode	**system-view**	

Perform VCT detection on all ports	**vct run**	
Enter interface view	**interface** { { ethernet*interface-num* } | interface-name }	
Perform VCT detection on a single port	**vct run**	

【**Example**】

！ VCT test on Ethernet port 1 [Switch-ethernet-0/1]vct run **Notice:**

VCT detection is only for Cat 5 Ethernet ports and does not support VCT detection on opticalfiber ports.

2.1.7 Management IP Address Configuration

You can restrict the host IP address or a certain network segment that log in to the Switch's web, telnet, snmp agent, and other IP addresses other than the matching configuration cannotmanage the Switch.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure management IP address restrictions	**login-acl** { **web** | **snmp** | **telnet** } *ip-address wildcard*	
Remove management IP address restrictions	**undo login-acl** { all | { web | snmp | telnet { all | *ip-address wildcard* }}}	
Display management IP address restriction configuration information	**display login-acl**	

【**Example**】

！ The configuration only allows addresses in the network segment 192.168.0.0/255.255.0.0 to access the Switch

through telnet

[Switch] login-acl telnet 192.168.0.1 0.0.255.255

[Switch]undo login-acl telnet 0.0.0.0 255.255.255.255

！Display the configuration of the management ip address restriction：[Switch]display

login-acl

2.1.8 Telnet User Limit for Login Privileged User View

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure the number of Telnet users	**telnet-server limit** *limit-num*	
Remove the limit on the number of users logging in to Telnet	**undo telnet-server limit**	
Display Telnet user limit configuration information	**display telnet-server**	

【**Example**】

！Configure to allow only two Telnet users to enter privileged user view at the same time [Switch] telnet-server

limit 2

2.1.9 CPU-CAR Command

CPU-CAR is mainly used to set the rate at which the CPU receives packets to limit the number of packets sent to

the CPU per second.

Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure CPU-CAR	**cpu-car** *target_rate*	
Restore the default CPU-CAR Value	**undo cpu-car**	
Display CPU-CAR	**display cpu-car**	

【**Example**】

！Set the rate of cpu receives packets to 100pps [Switch]cpu-

car 100

2.1.10 SSL

SSL (Secure Socket Layer)   Provide transport layer security services (according to the

7-layer protocol, it can also be considered as the session layer)，First developed by Netscape (1995), it was

widely used in Web and other security services, and later adapted to the Internet standard TLS (TLS1.0,

RFC2246, similar to SSL3.0)

Independent of application layer

The transport layer uses TCP to provide reliable services

SSL can be divided into two layers:

SSL handshake protocol: used to exchange security information before establishing a secure connection

between the client and the server

SSL recording protocol (low): determine the data security transmission mode
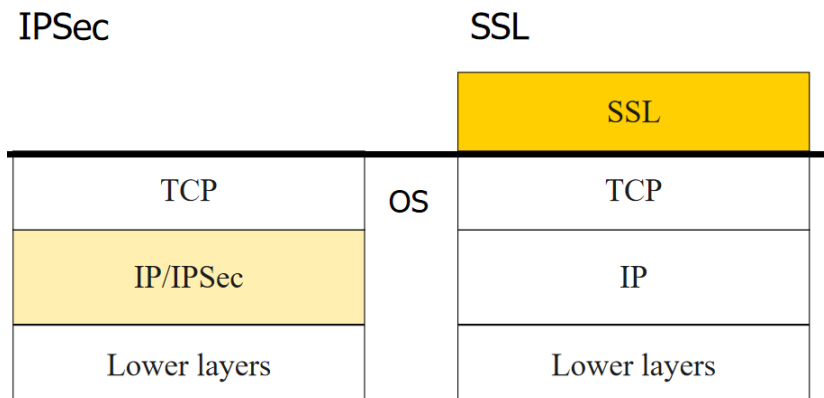
Operation	Command	Remarks
Enter global configuration mode	**system-view**	
Configure SSL	**http enable ssl**	The default is http mode
Restore the default	**http disable**	
Display CPU-CAR	**display http**	

【**Example**】

[Switch]display http Web Server status: Running:TRUE

Port:80

[Switch]http enable ssl

← → ✕ ⓘ 192.168.0.1/login.asp

2.2   Configuration Management

2.2.1   Save Configurations

After modified the configurations, you should same them so that these configurations can take effect next

time it restarts. Use the following commands to save configurations.

Operation	Command	Remarks
Enter super user view	**enable**	
Save configurations	**save current-config**	

2.2.2   Erase Configurations

If you need to reset to factory default, you can use the following commands to erase all configurations.

After erased, the device will reboot automatically.

Operation	Command	Remarks
Enter super user view	**enable**	
Erase configuration	**clear save-config**	

2.2.3 Execute save Configuration

Operation	Command	Remarks
Enter super user view	**enable**	
Execute save configuration	**update current-config**	

2.2.4 Show save Configurations

Use the following command to display the configurations you have saved.

Operation	Command	Remarks
Show configuration	**display save-config** [*module-list*]	

【Example】

！ Display all contents of the configuration file

<Switch>display save-config

！Display the contents of GARP and OAM modules in the configuration file

<Switch>display save-config garp oam

2.2.5   Show Running Configurations

Operation	Command	Remarks
Show running configurations	**display current-config** [*module-list*] [perlines*num*]	

【Example】

！Display all configuration information

<Switch>display current-config

！Display configuration information for vlan

<Switch>display current-config vlan

2.3 Load Files and Upgrade Programs Online

2.3.1 Upload and Download Files by TFTP

Operation	Command	Remarks
Enter super user view	**enable**	
upload files	**upload** { configuration | info-center } tftp *tftpserver-ip filename*	configuration is the system save configuration file. info-center is the system log file
download file	l**oad** { configuration | host | bootrom } tftp *tftpserver-ip filename*	configuration is the system save configuration file. application is the device upgrade host program. whole-bootrom is the bootrom program for the device

tftpserver-ip is the IP address of the TFTP server, and filename is the name of the file to be uploaded. Before entering the command, open the TFTP server and set the destination pathfor the file upload.

【Example】

！Upload the configuration file by TFTP and name the configuration file config.txt

<Switch>upload configuration tftp 192.168.1.100 config.txt

After the upload is successful, the file config.txt in the computer with the IP address of

192.168.1.100 saves the current configuration.

！Download the configuration file config.txt by TFTP,

<Switch>load configuration tftp 192.168.1.100 config.txt

After downloading successfully and restarting the system, the system will use the new configuration file

config.txt

！Upload the log file by TFTP and name the log file log.txt

<Switch>upload info-center tftp 192.168.1.100 log.txt

！Download the upgrade file host.bin by TFTP

<Switch>load host tftp 192.168.1.100 host.bin

After downloading successfully and restarting the system, host.bin will run.

！Download the bootrom program boot.bin by TFTP

<Switch>load bootrom tftp 192.168.1.100 boot.bin

2.3.2 Upload and Download Files by FTP

Operation	Command	Remarks
Enter super user view	**enable**	
upload files	**upload** { configuration	info-center } ftp *ftpserver-ip filename usename password*	
download file	**load** { configuration	host	bootrom } ftp *ftpserver-ip filename usename password*	

ftpserver-ip is the IP address of the FTP server, and filename is the name of the file to be

uploaded. username and userpassword are the username and password set in the FTP server. Before

entering the command, you should open the FTP server, and set the user name, password, and the

destination path of the file upload.

【**Example**】

！Upload the configuration file by FTP and name the configuration file config.txt

<Switch>upload configuration ftp 192.168.1.100 config.txt admin 123

！Download configuration files by FTP

<Switch>load configuration ftp 192.168.1.100 config.txt admin 123

！Download the upgrade file host.bin by ftp

<Switch>load host ftp 192.168.1.100 host.bin admin 123

！Upload the log file by FTP and name the log file log.txt

<Switch>upload info-center ftp 192.168.1.100 log.txt admin 123

！Download the bootrom program boot.bin by FTP

<Switch>load bootrom ftp 192.168.1.100 boot.bin admin 123

2.3.3 Download Files by Xmodem

Operation	Command	Remarks
Enter super user view	**enable**	
download file	l**oad** { configuration	host	bootrom } xmodem	

After entering the command, select "Transfer" ->"Send File" in the HyperTerminal menu, and enter the full path and file name of the file in the "File Name" column of the "Send File" dialog box that pops up, and the "Protocol" drop-down Select Xmodem in the list, and then click the

[Send] button.

【**Example**】

！Download the host program by Xmodem

<Switch>load application xmodem

2.4 Reboot Switch

Operation	Command	Remarks
Enter super user view	**enable**	
Restart the Switch immediately	**reboot**	
Enter system view	**system-view**	
Auto restart at specified time	**auto-reboot** { in { minutes *min*	hours *hour* }	at { *YYYY/MM/DD hh:mm:ss*	*hh:mm:ss* daily	*hh:mm:ssweekday* weekly } }	
Cancel scheduled automatic restart	**undo auto-reboot**	

【**Example**】

！Set to restart at 03:30:30 on May 15,

2020 [Switch]auto-reboot   at   03:30:30

2020/05/15

！Set to restart at 03:30:30 every Monday morning.

[Switch]auto-reboot at 03:30:30 mon weekly

【**Example**】