Atop Technologies, Inc.

Industrial Managed Layer-3 Switch

Command Line User Manual
V0.2
September 22st, 2022

Series covered by this manual:
EHG76XX, RHG76XX*

* The user interface on these products may be slightly different from the one shown on this user manual

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the Table of Contents to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
www.atoponline.com

Important Announcement

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch and use its software, a background in general theory is a must, when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations, and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com .

Warranty Period

Atop technology provides a limited 5-year warranty for managed Ethernet switches.

Documentation Control

Author:	Shawn Wu
Revision:	0.2
Revision History:	Initial
Creation Date:	26 November 2021
Last Revision Date:	22 22 September 2022
Product Reference:	Layer-3 Managed Switch Command Line
Document Status:	Released

Table of Contents

Table of Figures

Table of Tables

1 Configuring with a Serial Console

A managed switch such as EHG7XXX series can also be configured by using a serial console. Note that a special serial console cable is required to connect to the console port (an RJ45 connector) on top of the EHG7XXX's chassis. Please contact Atop Technologies to obtain the cable if it is needed. This configuring method is similar to the web browser one. The options are the same; therefore, users can take the same procedures as those descriptions and examples in device's standard user manual.

1.1 Serial Console Setup

Note: It is recommended that users obtain a terminal emulator program such as Tera Term or PuTTY and install it in their computer before configuring the device through the serial console.

After users installed the **Tera Term** which is a recommended terminal emulator program that can be used for serial communication, users can perform the following steps to access the serial console utility.

1. Start **Tera Term**. In **New Connection** window, select **Serial** radio button and select appropriate serial port that connect your computer to the EHG7XXX device as shown in Figure 1.1.

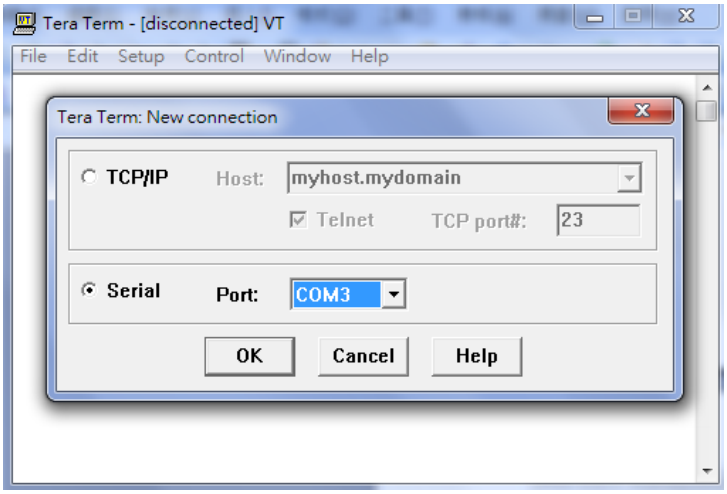


Figure 1.1 Setting of New Connection in Tera Term Program

2. Click **Setup** menu -> Choose **Serial Port...** option as shown in Figure 1.2.

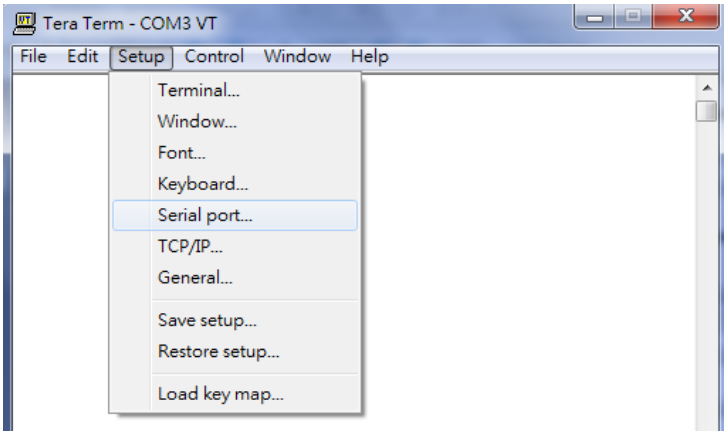


Figure 1.2 Setup Menu

3. After the **Serial Port Setup** window popped up, select an appropriate port's parameters for **Port number**, **115200** for **Baud Rate**, **8 bits** for **Data**, **none** for **Parity**, and **1 bit** for **Stop**, as shown in Figure 1.3.

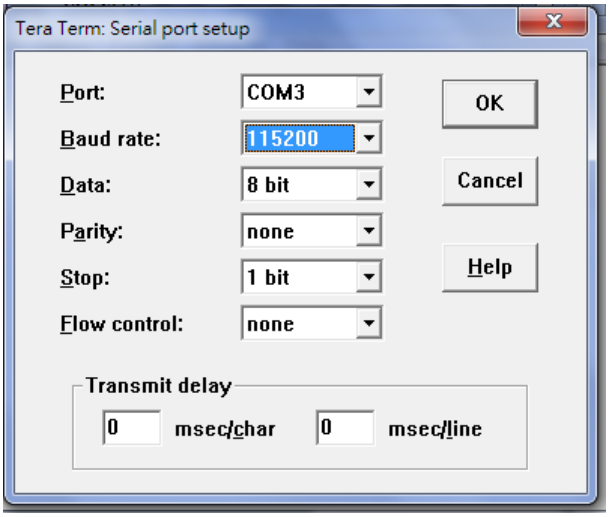


Figure 1.3 Parameter setting for the Serial Port

4. After finishing settings and clicking **OK**, a **Command Line Interface** (**CLI**) window will be brought up. Note that users can click **Enter** key to see any prompt on the window.

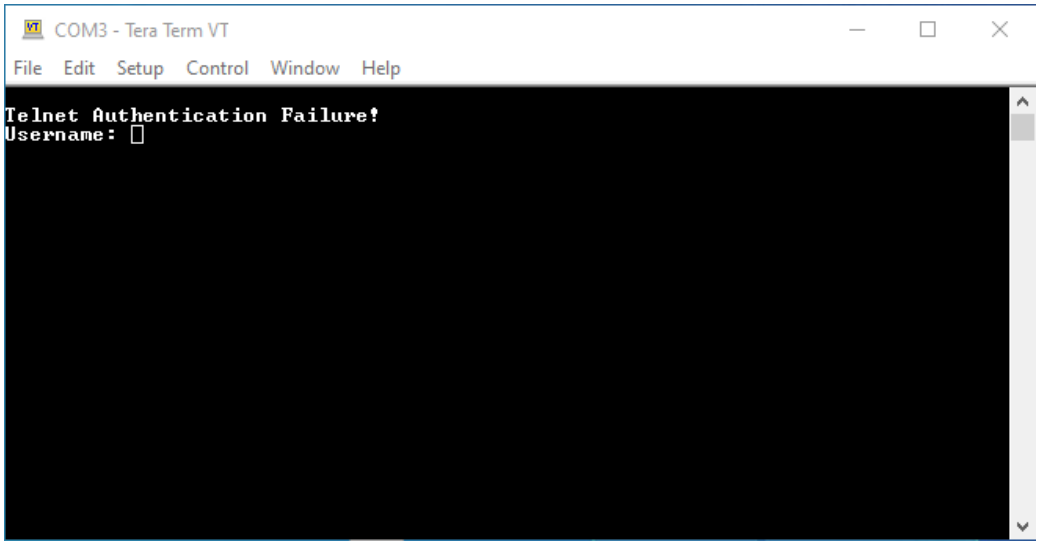


Figure 1.4 Command Line Interface Window

1.2 Command Line Interface Introduction

The Command Line Interface (CLI) supports two types of privileges, which are operator and manager privileges. Users with operator privileges may only view the information, while those with manager privileges are allowed to view information and configure settings. Operator and manager privileges are initially entered without the need for passwords, but a user may be assigned with a password for both the operator and manager privileges. If passwords are assigned, then the next time the user attempts to enter CLI, they will need to enter the correct username and password.

If a user is in the user mode and has an operator previledge, the user can login to the Command Line Interface by entering the correct Username and Password on the CLI window. The user should see a prompt as shown below:

Username: ***(enter username here)***
Password: ***(enter password here)***
switch>

If a user is in the user mode and wants to switch to the privileged mode, he/she may simply type in the command "**enable**" at the "*switch>*" prompt and then enter the correct username and password after the prompt:

switch> ***enable***
Username: ***(enter username here)***
Password: ***(enter password here)***
switch#

For the default admin account, the user can enter "**admin**" for the Username prompt and "**default**" for the Password prompt similar to the default WebUI password. Note that the admin account is considered as a user with manager priviledge. To identify the current priviledge, users can recognize the operator priviledge when users see the "*switch>*" prompt and the manager

priviledge when the users see the "*switch#*" prompt. An example of admin account login is shown in Figure 1.5.

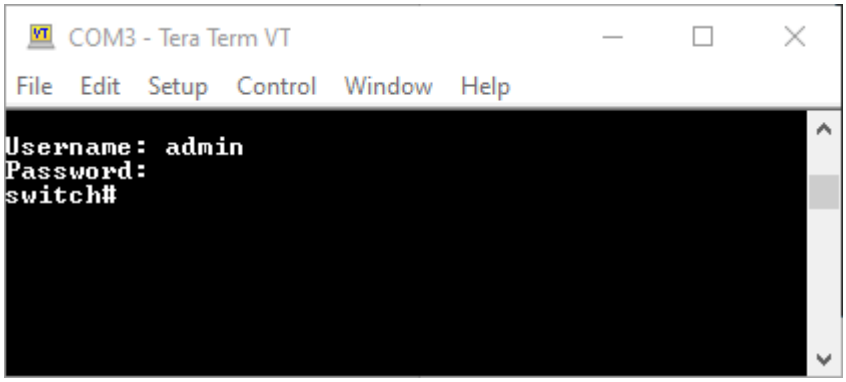


Figure 1.5 Sucessfully login of the admin account on the CLI window

To enter the "configuration" mode, you need to be in the privileged mode or manager priviledge first, then type in the command "**configure**":

switch# ***configure***
switch(config)#

To exit the "configuration" mode to just manager privilege mode, users can enter "**exit**" command at the "switch(config)#" prompt. If the users also need to exit the manager privilege to operator privilege, users can enter "**disable**" command at the "switch#" or "switch(config)#" prompt.

An illustration of the modes, related privileges and screen prompt is shown in Figure 1.6.

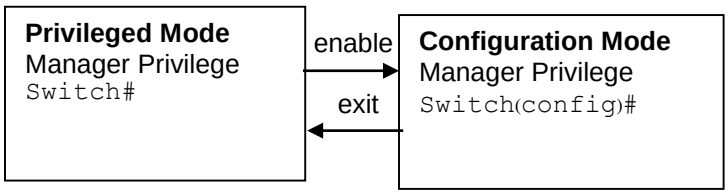


Figure 1.6 Modes, privileges, and prompts

Users may enter "**?**" at any command mode for help list and the CLI will return possible commands at that point, along with some description of the keywords. Examples of help lists for manager privilege and for operator privilege are shown in Figure 1.7.

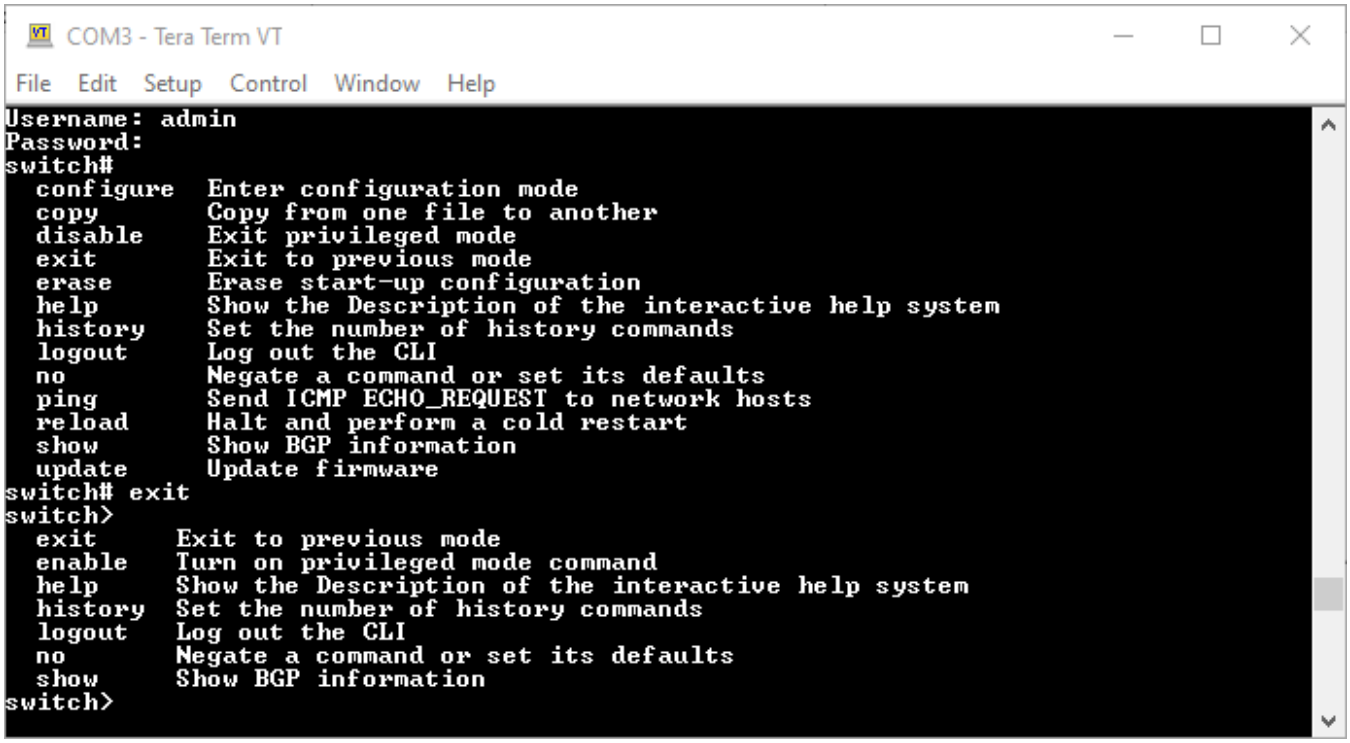


Figure 1.7 Help lists for manager and operator privileges

Additonally, users can append "**?**" to any command to list all possible options for that particular command such as the "*ip*" command in the following example.

switch(config)# ***ip ?***
ip *Configure network setting*
ipv6 *Configure network setting*
ip-routing *IP Routing configuration*

Moreover, users may use the <**Tab**> key to do keyword auto completion for the command:
switch(config)# ***sysl*** *<Tab>*
switch(config)# ***syslog***

1.3 Privileged Mode Command Line

Figure 1.8 shows all the options on CLI when the user is in the manager privilege or privileged mode and Table 1.1 shows list of privileged mode command lines that may be used anytime when using serial console.

```
switch#
  configure  Enter configuration mode
  copy       Copy from one file to another
  disable    Exit privileged mode
  exit       Exit to previous mode
  erase      Erase start-up configuration
  help       Show the Description of the interactive help system
  history    Set the number of history commands
  logout     Log out the CLI
  no         Negate a command or set its defaults
  ping       Send ICMP ECHO_REQUEST to network hosts
  reload     Halt and perform a cold restart
  show       Show BGP information
  update     Update firmware
```

Figure 1.8 Command Line of Privileged Mode

Table 1.1 Command Description of privileged mode

Commands	Descriptions
configure	Enter configuration mode
disable	Exit privileged mode
exit	Exit to previous mode
help	Show the Description of the interactive help system
logout	Log out the CLI
history [<0-256>]	Set the number of history commands
show history	Show the command history
no history	Disable the command history
ping [hostname]	Send ICMP ECHO_REQUEST to network hosts
reload	Halt and perform a warm restart
erase startup-config	Perform factory default DUT
copy running-config startup-config	Save all settings that modify by configuration mode to flash
show running-config	Show the currently running configuration of DUT
copy tftp running-config [server ip] [file_name]	Retrieve running-config configuration from TFTP server
copy tftp startup-config [server ip] [file_name]	Retrieve startup-config configuration from TFTP server
update firmware tftp [server ip] [file_name]	Update firmware from TFTP server

1.4 Configuration Mode Command Line

When users are in the privilege mode on the serial console, they can add/delete/change configuration of the device in the same manner as via the web browser or WebUI method. Figure 1.9 shows a list of all commands in the CLI's privilege mode. The following subsections will describe each command and provide information related to its options. These will enable the users to configure the device in **Configuration mode** through the CLI interface.

```
access-list          Configure ACL setting
alert                Configure Alert setting
auth-server          Configure log-in authentication server setting
arp-spoof-prevention Set arp-spoof-prevention configure
black-list-mac       Configure Black-List MAC filter
bgp                  Configure BGP setting
clear                Clear values in destination protocol
c-ring               Configure Compatible-Ring setting
cos-mapping          Configure CoS-Mapping setting
cchain               CCHAIN configuration
disable              Exit privileged mode
dev-info             Configure device information
dhcp                 DHCP configuration
dot1x                Configure 802.1x setting
dipswitch            DIP Switch information
daylight-saving-time Daylight Saving Time
dscp-mapping         Configure DSCP-Mapping setting
dos                  Configure Denial of Service setting
diagnosis_code       The diagnosis code
exit                 Exit to previous mode
erps                 Configure ERPS setting
garp                 Configure GARP setting
gmrp                 Configure GMRP setting
gvrp                 Configure GVRP setting
help                 Show the Description of the interactive help system
history              Set the number of history commands
https                Configure HTTPS setting
ip                   Configure network setting
ipv6                 Configure network setting
igmp                 Configure IGMP setting
ia-ring              Configure iA-Ring setting
ip-routing           IP Routing configuration
logout               Log out the CLI
lldp                 Configure LLDP setting
lacp                 Configure LACP setting
mac-age-time         Configure MAC address aging time
monitor              Configure Port mirror
mac-address-table    Add an entry to MAC address table
mld_snooping         configure mld snopping
no                   Negate a command or set its defaults
ntp-server           Configure NTP server setting
option66_67          Configure Option66/67 setting
ospf                 Configure OSPF setting
password             Configure account/password
port                 Configure port setting
ping                 Send ICMP ECHO_REQUEST to network hosts
ping6                Send ICMP ECHO_REQUEST to network hosts
ptp                  Configure PTP setting
poe                  Power Over Ethernet information
qinq                 Configure QinQ setting
qos                  Configure QoS setting
radius-server        Configure Radius server setting
rip                  Configure RIP setting
router               Setting Router
show                 Show BGP information
storm-control        Confiture storm filter for controlling broadcast, multicast, unitcast
security             Configure Port security setting
sntp                 Configure SNTP setting
sys-time             Configure system time
syslog               Configure Syslog setting
smtp                 Configure SMTP setting
snmp                 Configure SNMP setting
ssh                  Configure SSH setting
spanning-tree        Configure STP setting
static-routing       Configure static route setting
timeout              Configure CLI timeout
temperature          temperature logreset data
trunk                Configure Trunk setting
telnet               Configure Telnet setting
traceroute           Configure network setting
udld                 Configure UDLD setting
u-ring               Configure U-Ring setting
vlan                 Configure VLAN setting
vrrp                 Configure VRRP setting
```

Figure 1.9 List of Commands in Configuration Mode

1.4.1 ACCESS-LIST

The first command in Configuration mode is the “access-list”. This command enables the user to configure the ACL (Access Control List) setting, which is equivalent to the ACL webpage under the Security menu on the Web UI. This setting can either deny or permit for traffic (frames/packets) to a port or ports on this device (EHG7XXX) based on either their MAC address, IPv4 address, or IPv6 address. To show the current ACL settings, users can enter the “show access-list” command on the prompt. To remove all or any specific ACL table from the device, the user can enter the “no access-list” command as shown in Table 1.2.

Table 1.2 Descriptions of Commands for ACL Setting

Command	Description
show access-list [id]	Show ACL settings [id] refers to the index of the ACL table or rule which can be at most 128 rules/tables.
access-list id [access-list-number | auto] name [name-string] [deny/permit] mac src-mac [src-mac-value] src-mac-mask [src-mac-mask-value] dst-mac [dst-mac-value] dst-mac-mask [dst-mac-mask-value] vlan-id [vlan-id-value] pcp [pcp-value] ether-type [ether-type-value] [port-list]	Set ACL for MAC based filtering. - Option “[access-list-number|auto]” sets the index number for the ACL table. When id is set to auto, the smallest unused value will be given. - Option “[name-string]” set the name for the ACL table using the given text. - Option “[deny/permit]” is used to set the ACL table as black-list or white-list table. - Option “[src-mac-value]” is used to specify a MAC address of the source. - Option “[src-mac-mask-value] is used to specify the value of mask for the source MAC address. Note: For every non-zero bit in the Mask, its relative bit in the MAC address will be compared. If the Mask is all zeros, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of all ones and all of bits in the MAC Address are compared. - Option “[dst-mac-value]” is used to specify a MAC address of the destination. - Option “[dst-mac-mask-value] is used to specify the value of mask for the destination MAC address. - Option “[vlan-id-value]” can be set between 1~4094. - Option “[pcp-value]” is refered to Priority field of 802.1Q VLAN tag in the Ethernet frame header and value is between 0~7.

Command	Description
	- Option “[ether-type-value]” is the Ethernet type field in the Ethernet frame header. It can have a value between 0~0xFFFF. - Option “[port-list]” is the port list. If it is blank, it will be regarded as specifying all ports.
access-list id [access-list-number | auto] name [name-string] [deny/permit] ip ip-protocol [ip-protocol-value] src-ip-address [src-ip-address-value] src-ip-address-mask [src-ip-address-mask-value] dst-ip-address [dst-ip-address-value] dst-ip-address-mask [dst-ip-address-mask-value] src-port [src-port-value] dst-port [dst-port-value] tos [tos-value] [port-list]	Set ACL for IPv4 based filtering. - Option “[access-list-number|auto]” sets the index number for the ACL table. When id is set to auto, the smallest unused value will be given. - Option “[name-string]” set the name for the ACL table using the given text. - Option “[deny/permit]” is used to set the ACL table as black-list or white-list table. - Option “[ip-protocol-value]” is the Protocol field of the IPv4 packet header. The value is between 0~65535. The value 6 is for the TCP packet. The value 17 is for the UDP packet. - Option “[src-ip-address-value]” is used to specify an IP address of the source. - Option “[src-ip-address-mask-value] is used to specify the value of subnet mask for the source IP address. Note: For every non-zero bit in the Mask, its relative bit in the IP address will be compared. If the Mask is all zeros, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of all ones and all of bits in the IP Address are compared. - Option “[dst-ip-address-value]” is used to specify an IP address of the destination. - Option “[dst-ip-address-mask-value] is used to specify the value of subnet mask for the destination IP address. - Option “[src-port-value]” is the fields of TCP/UDP frame header. It is used to filter the application services. The item value is between 0~65535. - Option “[dst-port-value]” is the fields of TCP/UDP frame header. It is used to filter the application services. The item value is between 0~65535.

Command	Description
	- Option “[tos-value] is the Differentiated Service Code Point (DSCP) field in an IPv4 header. It is used for providing Quality of Service (QoS). The item value is between 0~63. - Option “[port-list]” is the port list. If it is blank, it will be regarded as specifying all ports.
access-list id [access-list-number | auto] name [name-string] [deny/permit] ipv6 next-header [next-header-value] src-ipv6-address [src-ipv6-address-value] src-ipv6-address-mask [src-ipv6-address-mask-value] dst-ipv6-address [dst-ipv6-address-value] dst-ipv6-address-mask [dst-ipv6-address-mask-value] src-port [src-port-value] dst-port [dst-port-value] traffic-class [traffic-class-value] [port-list]	Set ACL for IPv6 based filtering. - Option “[access-list-number|auto]” sets the index number for the ACL table. When id is set to auto, the smallest unused value will be given. - Option “[name-string]” set the name for the ACL table using the given text. - Option “[deny/permit]” is used to set the ACL table as black-list or white-list table. - Option “[next-header-value]” is the Protocol field of the IPv6 packet header. - Option “[src-ipv6-address-value]” is used to specify an IPv6 address of the source. - Option “[src-ipv6-address-mask-value] is used to specify the value of subnet mask for the source IPv6 address. Note: For every non-zero bit in the Mask, its relative bit in the IP address will be compared. If the Mask is all zeros, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of all ones and all of bits in the IP Address are compared. - Option “[dst-ipv6-address-value]” is used to specify an IPv6 address of the destination. - Option “[dst-ipv6-address-mask-value] is used to specify the value of subnet mask for the destination IPv6 address. - Option “[src-port-value]” is the fields of TCP/UDP frame header. It is used to filter the application services. The item value is between 0~65535. - Option “[dst-port-value]” is the fields of TCP/UDP frame header. It is used to filter the application services. The item value is between 0~65535.

Command	Description
	- Option “[traffic-class-value] is the field in an IPv6 header. It is used for providing Quality of Service (QoS). The item value is between 0~256. - Option “[port-list]” is the port list. If it is blank, it will be regarded as specifying all ports.
no access-list [access-list-number | all]	Delete the specified ACL table or all ACL tables

1.4.2 ALERT

To configure the warning condition, users can use this “alert” command on the CLI. It is equivalent to the Warning/Alarm Setting page on WebUI. There are three different types of Warning or Alarm: Link Status Alarms, Power Status Alarms, and System Log Alarms. The Link Status Alarms are related to the activities of particular port(s). Power Status Alarms keep track of power status of the switch based on the available input connectors. System Log Alarms are related to the overall functionalities of the switch. Table 1.3 describes the “alert” command and its options.

Table 1.3 Descriptions of Commands for Alert Setting

Command	Description
alert email-warning link-status [linkdown/ linkup/ linkupdown]	Configure trigger condition for link status. - Option “email-warning” sends the warning message via e-mail. - Option “[linkdown/linkup/linkupdown]” is used to select the trigger condition.
alert email-warning power-status [on/ off]	Configure trigger condition for power status. - Option “email-warning” sends the warning message via e-mail. - Option “[on/off]” is used to select the trigger condition.
alert email-warning syslog level [log level value <0-7>]	Configure trigger condition for syslog level. - Option “email-warning” sends the warning message via e-mail. - Option “[log level value <0-7>]” is used to select the syslog level which can be a value from 0 to 7.
alert led-warning link-status [linkdown/ linkup/ linkupdown]	Configure trigger condition for link status. - Option “led-warning” sends the warning notification by turning on an LED. - Option “[linkdown/linkup/linkupdown]” is used to select the trigger condition.
alert led-warning power-status [on/ off]	Configure trigger condition for power status. - Option “led-warning” sends the warning notification by turning on an LED.

Command	Description
	- Option “[on/off]” is used to select the trigger condition.
alert relay-warning link-status [linkdown/ linkup/ linkupdown]	Configure trigger condition for link status. - Option “relay-warning” sends the warning notification by triggering a relay. - Option “[linkdown/linkup/linkupdown]” is used to select the trigger condition.
alert relay-warning power-status [on/ off]	Configure trigger condition for power status. - Option “relay-warning” sends the warning notification by triggering a relay. - Option “[on/off]” is used to select the trigger condition
alert relay-warning reset	Reset the relay. - Option “relay-warning reset” is used to reset a relay.
alert relay-warning syslog-level [log level value <0-7>]	Configure trigger condition for syslog level. - Option “relay-warning” sends the warning notification by triggering a relay. - Option “[log level value <0-7>]” is used to select the syslog level which can be a value from 0 to 7.

1.4.3 AUTH-SERVER

This section allows the users to configure the authentication server which is used in IEEE 802.1X standards. shows how users can configure Auth-Server setting. It provides an authentication mechanism to devices that want to attach to a LAN or WLAN. This protocol restricts unauthorized clients from connecting to a LAN through ports that are opened to the Internet. Authentication Server performs the actual authentication and can use either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ as the authentication server. Table 1.4 describes the “auth-server” command and its options.

Table 1.4 Descriptions of Commands for Auth-Server Setting

Command	Description
auth-server enable	Enable Auth Server Setting
no auth-server enable	Disable Auth Server Setting
auth-server host [ip address]	Configure authentication server ip address value. - Option “[ip address]” is used to set the IP address of the authentication server.
auth-server key [shared key value]	Configure authentication server shared key value. - Option “[shared key value]” is used to set the shared key between the managed switch and the RADIUS Server. Both ends

	must be configured to use the same key. Max. Of 30 characters.
auth-server timeout [time out value<1~255>]	Configure authentication server timeout value. - Option "[time out value <1~255>]" has a range of 1~255 seconds.
auth-server type [radius/ tacacs+]	Configure authentication server type. - Option "[radius/tacacs+]" is used to set the authentication server type to either RADIUS or TACACS+.
auth-server auth-type [ascii/ chap/ md5/ mschap/ pap]	Configure authentication type for the authentication server. - Option "[ascii/chap/md5/mschap/pap]" is used to set the authentication type for an authentication server: Note that a. RADIUS supports "md5" option. b. TACACS+ supports "ascii", "chap", "mschap", or "pap" options.

1.4.4 ARP-SPOOF-PREVENTION

ARP (Address Resolution Protocol) Spoof Prevention is a security mechanism supported by Atop's EHG7XXX series to prevent ARP spoof attacks. The ARP spoof attack is a kind of network security attacks that a malicious host or node sends a falsify ARP messages over a local area network. This type of attack is also called ARP spoofing, ARP cache poisoning, or ARP poison routing. Typically, the attacker would like other hosts/nodes in the network to link or map the malicious Ethernet MAC address to a legitimate IP address of a victim host/node. To enable this feature and configure it on your device, you can use the "apr-spoof-prevention" command which is described in Table 1.5.

Table 1.5 Descriptions of Commands for Arp-Spoof-Prevention setting

Command	Description
arp-spoof-prevention enable	Enable arp-spoof-prevention feature
no arp-spoof-prevention enable	Disable arp-spoof-prevention feature
show arp-spoof-prevention	Show the current arp-spoof-prevention configuration on your device
arp-spoof-prevention [ip address value] [MAC address value] [port-list]	Configure arp-spoof-prevention setting by adding an entry to arp-spoof-prevention table. - Option "[ip address value]" is used to set the IP address of an entry. - Option "[MAC address value]" is used to set the MAC address of an entry. Note that the IP Address and the MAC address in each entry belong to a legitimate or valid host/node that the administrator assigned or approved and the administrator of EHG7XXX want to

	protect that host/node from being spooffed. - Option "[port-list]" lists all the port numbers for arp-spoof-prevention. Note that port list must be separated by ","s or "-"s.
no arp-spoof-prevention [ip address value]	Delete the entry with the specified IP address from table, if you don't assign the IP address, it will delete all the entries in the table

1.4.5 BLACK-LIST-MAC

The managed switch also allows users to set MAC filtering manually through this "black-list-mac" command. Using this command, users can add or remove an entry to or from the black-list-mac table. Table 1.6 summarizes the options for "black-list-mac" command.

Table 1.6 Descriptions of Commands for Black-List-Mac Setting

Command	Description
show black-list-mac	Show the current Black-List MAC filter table in Unicast/Multicast MAC
black-list-mac [MAC address value]	Add the specified Black-List MAC address entry to MAC filter table in Unicast/Multicast MAC
no black-list-mac [MAC address value]	Delete the specified Black-List MAC address entry from the MAC filter table in Unicast/Multicast MAC

1.4.6 BGP

This section shows how users can inspect BGP information and make changes using commands.
The following command line interface (CLI) in Table 1.7 can be used to configure BGP feature of the switch.

Table 1.7 Descriptions of Commands for Setting up BGP Function

Command	Description
bgp bestpath as-path confed	This command specifies that the AS confederation path length must be used when it is available in the BGP best path decision process. Putting "no" in the front of the command to reset to the default, where the device ignores AS confederation path length in the BGP best path selection process.
bgp bestpath compare-routerid	By default, when comparing similar routes from peers, BGP does not consider the router ID of

	neighbors advertising the routes - BGP simply selects the first received route. Use this command to include router ID in the selection process. That is the similar routes are compared and the route with the lowest router ID is selected. Putting “no” in the front of the command to disable this feature and return the device to the default state, where the device ignores the router ID in the BGP best path selection process.
neighbor <neighborid> port<portnum>	Use this command to specify the TCP port to which packets are sent to on a BGP neighbor. <neighborid> specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “port <portnum>”: ranging from 0 to 65535, specifies the TCP port number. Putting “no” in the front of the command to reset the port number back to the default value (TCP port 179).
neighbor <neighborid> weight <weight>	Use this command to set default weights for routes from this BGP or BGP4+ neighbor. <neighborid> specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “weight <weight>”: ranging from 0 to 65535 specifies the weight that this command assigns to the route. Putting “no” in the front of the command to remove a weight assignment.
neighbor <neighborid> version <version>	Use this command to configure the device to accept only a particular BGP version. <neighborid> specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “version <version>”: {4} specifies the BGP version number. Use the **no** variant of this command to use the default BGP version (version 4).
neighbor <neighborid> ebgp-multihop [<count>]	Use this command to accept and attempt BGP or BGP4+ connections to external peers on indirectly connected networks. - Option “neighbor <neighborid>” specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

	- Option “ebgp-multihop [<count>]” ranging from 1 to 255 is the maximum hop count set in the TTL field of the BGP packets. Use the **no** variant of this command to delete BGP connections to external peers on indirectly connected networks.
neighbor <ipaddress> interface <interface>	Use this command to configure the interface name of a BGP4+ speaking neighbor. - Option “neighbor <neighborid>” specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “interface <interface>” specifies the interface name of BGP neighbor, e.g. vlan2. Use the **no** variant of this command to disable this function.
show ip bgp filter-list<listname>	Use this command to display routes conforming to the filter-list within an IPv4 environment. Use the show bgp ipv6 filter-list (BGP4+ only) command to display routes conforming to the filter-list within an IPv6 environment. - Option “filter-list<listname>” specifies the regular-expression access list name.
neighbor <neighborid> distribute-list <access-list> {in|out}	This command filters route updates from a particular BGP or BGP4+ neighbor using an access control list. - Option “neighbor <neighborid>”: The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “distribute-list<access-list>”: The access-list used to filter routes. The following types of access-lists: - <WORD> The name of IP access-list. - <1-199> The ID number of a standard IP access-list. - - <1300-2699> The ID number of an extended IP access-list. in Indicates that incoming advertised routes will be filtered. out Indicates that outgoing advertised routes will be filtered. The **no** variant of this command removes a previously configured BGP or BGP4+ distribute-list.
neighbor <peer-group> peer-group	Use this command to create a peer-group for BGP and BGP4+. - Option “peer-group<peer-group>”: Enter the name of the peer-group.

	Use the **no** variant of this command to disable this function.
neighbor <neighborid> send-community {both/extended/standard}	Use this command to specify that a community attribute should be sent to a BGP or BGP4+ neighbor. - Option “<neighborid>”: Specify the IPv4 address of the BGP neighbor, entered in the format A.B.C.D. - Option “both” : Sends Standard and Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no standard or extended community attributes being sent. - Option “extended” : Sends Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no extended community attributes being sent. - Option “standard” : Sends Standard Community attributes. Specifying this parameter with the **no** variant of this command results in no standard community attributes being sent. Use the **no** variant of this command to remove the entry for the community attribute.
neighbor <neighborid> attribute-unchanged {as-path/next-hop/med}	Use this command to advertise unchanged BGP or BGP4+ attributes to the specified BGP or BGP4+ neighbor. <neighborid> specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “<neighborid>”: Specify the IPv4 address of the BGP neighbor, entered in the format A.B.C.D. - Option “as-path” is AS path attribute. - Option “next-hop” is next hop attribute. - Option “med” is Multi Exit Discriminator.
neighbor <neighborid> capability orf prefix-list {both/receive/send}	Use this command to advertise ORF (Outbound Route Filters) capability to neighbors. Use this command to dynamically filter updates. The BGP speaker can advertise a prefix list with prefixes it wishes the peer to prune or filter from outgoing updates. - Option “<neighborid>”: Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

	- Option “both”: Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer. - Option “receive”: Indicates that the local router is willing to receive ORF entries from its peer. - Option “Send”: Indicates that the local router is willing to send ORF entries to its peer. Use the **no** variant of this command to disable this function.
neighbor <neighborid> unsuppress-map <route-map-name>	Use this command to selectively leak more specific routes to a particular BGP or BGP4+ neighbor. - Option “<neighborid>”: specifies the IPv4 address of the BGP neighbor, entered in the format A.B.C.D. - Option “unsuppress-map<route-map-name>” specifies the name of the route-map used to select routes to be unsuppressed. Use the **no** variant of this command to remove selectively leaked specific routes to a particular BGP or BGP4+ neighbor.
neighbor {<neighborid>} default-originate [route-map <routemap-name>]	Use this command to control the number of prefixes that can be received from a BGP or a BGP4+ neighbor. - Option “<neighborid>” specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. - Option “default-originate”→ If a route-map is specified, then the route table must contain at least one route that matches the permit criteria of the route map before the default route will be advertised to the specified neighbor. - “Option “route-map<routemap-name>” is the route-map name. Use the **no** variant of this command to send no route as a default route.
neighbor <neighborid> capability route-refresh	Use this command to advertise route-refresh capability to the specified BGP and BGP4+ neighbors. - Option “<neighborid>” specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.

	Use the **no** variant of this command to disable this function.
neighbor <neighborid> dont-capability-negotiate	Use this command to disable capability negotiation for BGP and BGP4+. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to enable capability negotiation for BGP and BGP4+.
neighbor <neighborid> next-hop-self	Use this command to configure the BGP router as the next hop for a BGP speaking neighbor or peer group. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to Disable the BGP router as the next hop for a BGP speaking neighbor or peer group.
neighbor <neighborid> override-capability	Use this command to override a capability negotiation result for BGP. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to Delete a capability negotiation result for BGP.
neighbor <neighborid> passive	Use this command to configure the local BGP or BGP4+ router to be passive with regard to the specified BGP or BGP4+ neighbor. This has the effect that the BGP or BGP4+ router will not attempt to initiate connections to this BGP or BGP4+ neighbor but will accept incoming connection attempts from the BGP or BGP4+ neighbor. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to disable this function.
neighbor <neighborid> route-server-client	Use this command to specify the peer as route server client. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to delete route-server-client.

neighbor <neighborid> soft-reconfiguration inbound	Use this command to configure the device to start storing all updates from the BGP or BGP4+ neighbor, without any consideration of any inward route filtering policy that might be applied to the connection with this BGP or BGP4+ neighbor. - Option "<neighborid>" specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to disable this function for a BGP or BGP4+ neighbor.
bgp cluster-id <ip-address>	This command configures the cluster-id if the BGP cluster has more than one route reflector. A cluster includes one or more route reflectors and their clients. Usually, each cluster is identified by the router-id of its single route reflector. - Option "<ip-address>": A.B.C.D Route Reflector Cluster-id in IP address format. Use the **no** variant of this command removes the cluster ID.
set local-preference <pref-value>	This command changes the default local preference value. The local preference indicates the BGP local preference path attribute when there are multiple paths to the same destination. The path with the higher preference is chosen. - Option "<pref-value>" ranging from 0 to 4294967295, configures local preference value. The default local preference value is 100. The **no** variant of this command reverts to the default setting.
bgp default local-preference <pref-value>	This command changes the default local preference value. - Option "<pref-value>" ranging from 0 to 4294967295 configures default local preference value. The default local preference value is 100. The **no** variant of this command reverts to the default local preference value of 100.
distance <1-255> <ip-address/m> [<listname>]	This command sets the administrative distance for BGP and BGP4+ routes. The device uses this value to select between two or more routes to the same destination from two different routing protocols. Set the administrative distance for BGP routes in the Router Configuration mode,

	and for BGP4+ routes in IPv6 Address Family Configuration mode. - Option “<1-255>”: The administrative distance value you are setting for the route. - Option “<ip-address/m>”: The IP source prefix that you are changing the administrative distance for, entered in the form A.B.C.D/M. This is an IPv4 address in dotted decimal notation followed by a forward slash, and then the prefix length. - Option “<listname>”: The name of the access list to be applied to the administrative distance to selected routes. The **no** variant of this command sets the administrative distance for the route to the default for the route type.
set metric <metric value>	Use this command to add a metric set clause to a route map entry. - Option “<metric-value>”: ranging from 0 to 4294967295. The **no** variant of this command to delete a metric set clause to a route map entry.
bgp bestpath med {[confed] [missing-as-worst]}	This command controls how the Multi Exit Discriminator (MED) attribute comparison is performed. - Option “Confed”: Compares MED among confederation paths. - Option “missing-as-worst”: Treats missing MED as the least preferred one. Use the **no** variant of this command to prevent BGP from considering the MED attribute when comparing paths.
ip as-path access-list <listname> {deny/permit} <reg-exp>	This command defines a BGP and BGP4+ Autonomous System (AS) path access list. The named AS path list is a filter based on regular expressions. If the regular expression matches the AS path in a BGP update message, then the permit or deny condition applies to that update. Use this command to define the BGP access list globally, then use neighbor configuration commands to apply the list to a particular neighbor. - Option “<listname>” specifies the name of the access list.

	- Option “<deny>” denies access to matching conditions. - Option “<permit>” permits access to matching conditions. - Option “<reg-exp>” specifies a regular expression to match the BGP AS paths. - “^” Caret Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. - “$” Dollar sign Used to match the end of the input string. - “.” Period Used to match a single character (white spaces included). - “*” Asterisk Used to match none or more sequences of a pattern. - “+” Plus sign Used to match one or more sequences of a pattern. - “?” Question mark Used to match none or one occurrence of a pattern. - “_” Underscore Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string. - “[ ]” Brackets Specifies a range of single-characters. - “-“ Hyphen Separates the end points of a range The **no** variant of this command disables the use of the access list.

1.4.7 CLEAR

The user can use “clear” command to clear settings or to revert to default settions of protocols in the device as shown in Table 1.8.

Table 1.8 Descriptions of Commands for Clear Settings

Command	Description
clear bgp	Clear BGP information
clear gmrp	Disable GMRP or set it to default settings
clear gvrp	Disable GVRP or set it to default settings
clear igmp	Disable IGMP or set it to default settings
clear ip	Clear BGP IP information
clear mac-address-table	Clear all dynamic MAC address table entries
clear statistic	Clear statistic counter
clear vlan	Disable VLAN or set it to default settings

1.4.8 C-RING

C-Ring or Compatible-Ring is one of the redundant ring protocol available in the managed switch. It is similar to iA-Ring. To set the C-Ring protocol, use the "c-ring" command as summarized in Table 1.9.

Table 1.9 Descriptions of Commands for Compatible-Ring setting

Command	Description
show c-ring	Show compatible-ring status and settings
c-ring enable	Enable compatible-ring feature
no c-ring enable	Disable compatible-ring feature
c-ring ringport [1st ring port] [2nd ring port]	Configure compatible-ring ring port. - Option "ringport [1st ring port][2nd port] is used to set the ring port by specifying the port number for the 1st and 2nd ports.

1.4.9 COS-MAPPING

This command is used to set the CoS (Class of Service) Queue Mapping settings. It is one of the mechanisms use to provide Quality of Service (QoS) for traffic that flows through the manage switch. The users can set up this CoS Queue mapping using the command in Table 1.10.

Table 1.10 Descriptions of Commands for CoS Queue Mapping setting

Command	Description
cos-mapping priority-queue [CoSQ value <0-7>] [CoS List value <0-7>]	Configure CoS-Mapping setting - Option "[CoSQ value <0-7>]": The priority queue from Q0 to Q7 that a specific Ethernet frame needs to be assigned into. - Option "[CoS List value <0-7>]: Priority Code Point within the Ethernet frame header. PCP 0 is the lowest priority and 7 is the highest priority.

1.4.10 CCHAIN

This section shows how users can configure Compatible-Chain settings using "cchain" command. The Compatible-Chain setting is provided on Atop's managed switches for compatible networking with MOXA switch's Turbo Chain. The MOXA's Turbo Chain is a technique that uses the chain network topology and links the two ends (two network devices such as industrial managed switches) of the chain to a common LAN. This can also be viewed as a form of Ring Topology. This Turbo Chain can provide redundancy on any type of network topology or on complex network topology such as multi-ring architecture. The Turbo Chain can create flexible and scalable topologies with a fast media-recovery time. Table 1.11 summarizes the options for "cchain" command.

Table 1.11 Descriptions of Commands for Compatible-Chain setting

Command	Description

show cchain	Show compatible-chain status and settings
cchain enable	Enable compatible-chain feature
cchain disable	Disable compatible-chain feature
cchain role [head/ member/ tail]	Configure compatible-chain role setting. - Option "[head/member/tail]" is used to set the role for the current switch. Note that the fist switch on the Compatible-Chain will have a Role State as Head switch. The other switches along the Compatible-Chain will have a Role State as Member switches. The last switch on the Compatible-Chain will have a Role State as Tail switch.
cchain ringport [1st ring port] [2nd ring port]	Configure compatible-chain's ring port - Option "[1st ring port/2nd ring port] is used to set the port number for the 1st ring port and the 2nd ring port.

1.4.11 DISABLE

To exist the privileged mode, users can use "disable" command.

Table 1.12 Descriptions of Commands for exist privileged mode

Command	Description
disable	Exit privileged mode

1.4.12 DEV-INFO

Users can assign device's details to the managed switch using "dev-info" command as summarized in Table 1.13. This is similar to the Device Information Setting webpage in the WebUI. By entering unique and relevant system information such as device name, device description, location, and contact, this information can help identify one specific switch among all other devices in the network that supports SNMP.

Table 1.13 Descriptions of Commands for Device Information setting

Command	Description
dev-info name [name]	Configure the device's name, length limition is from 0 to 30.
dev-info description [description]	Configure the device's description, length limition is from 0 to 64.
dev-info location [location]	Configure the device's location, length limition is from 0 to 64.
dev-info contact [contact]	Configure the device's contact information, length limition is from 0 to 64.

1.4.13 DHCP

The Layer-3 Series industrial managed switch has two different approaches for setting up the IP addresses for the devices connected to its ports: DHCP mapping IP and DHCP relay agent. This section shows how users can configure the Client IP settings using “dhcp” command as described in Table 1.14. The user can reserve or map IP addresses to the device connected on the selected ports via DHCP mapping IP method. On the other hand, users can enable DHCP relay agent which is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets.

Table 1.14 Descriptions of Commands for Client IP setting

Command	Description
show dhcp mapping	Show the dhcp mapping setting table
dhcp mapping set [port number] [IP address value]	Configure ip address of specify port for DHCP mapping - Option “[port number]” is used to specify port number on the managed switch. - Option “[IP address value]” is used to specify IP address value.
dhcp mapping remove [port number]	Remove the ip address of specify port - Option “[port number]” is the port to be removed from the dhcp mapping.
show dhcp relay	Show the current dhcp relay setting table
dhcp relay enable	Enable DHCP Relay feature
no dhcp relay enable	Disable DHCP Relay feature
dhcp relay address [index<1-4>] [ip address value]	Configure the ip address of DHCP Relay Agent - Option “[index]” can be a value from 1 to 4. - Option “[ip address value]” is the IP address for the DHCP/BOOTP server IP addresses
dhcp relay option82 enable	Enable DHCP Relay Option82 feature which is the DHCP Relay Agent Information Option.
no dhcp relay option82 enable	Disable DHCP Relay Option82 feature
dhcp relay option82 type [client-id/ ip/ mac/ other]	Configure the type of use for DHCP Relay Option82 feature - Option “[client-id/ ip /mac/ other]” is the option82 type field that can be chosen from IP, MAC, Client-ID, or Other.
dhcp relay option82 type other [defined value]	Configure the defined value (length limition is from 1 to 32) of other type for DHCP Relay Option82 feature. - Option “[defined value]” can be a number from 1 to 32.

1.4.14 DHCP SERVER

This section shows how users can see DHCP Server information and change setting commands. The following command line interface (CLI) and options in Table 1.15 can be used to configure VLANs in the DHCP Server's setting configuration.

Table 1.15 Descriptions of Commands for DHCP Server setting

Command	Description
show dhcp server	Show the running state of DHCP server
dhcp server	Enable DHCP server
no dhcp server	Disable DHCP server
dhcp server vlan <1-4094>	Add VLAN interface of the DHCP server
show dhcp server vlan [<1-4094>]	Show configuration of DHCP server's VLAN - Option "[<1-4094>]" indicates the VLAN identification number from 1 to 4094.
dhcp server vlan <1-4094> leasetime *<3200-7200>*	Set lease time for specified VLAN ID. - Option "<1-4094> indicates the VLAN ID from 1 to 4094. - Option "leasetime <3200-7200>" is used to set lease time.
dhcp server vlan <1-4094> range <A.B.C.D> <P.Q.R.S>	Add dynamic IP range for the DHCP server address pool. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "range <A.B.C.D><P.Q.R.S>" are the range with the starting IP address and the ending IP address.
dhcp server vlan <1-4094> dns <A.B.C.D> <P.Q.R.S>	Set domain name servers of a VLAN (0.0.0.0 if not used) - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D><P.Q.R.S>" is used to specify the IP addresses of the domain name servers.
dhcp server vlan <1-4094> gateway <A.B.C.D> <P.Q.R.S>	Set gateways of a VLAN (0.0.0.0 if not used) - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D> <P.Q.R.S>" is used to specify the IP addresses of the gateway.
dhcp server vlan <1-4094> netbios-server <A.B.C.D> <P.Q.R.S>	Set netbios servers of a VLAN (0.0.0.0 if not used) - Option "v<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D> <P.Q.R.S>" is used to specify the IP addresses of the NETBIOS server.

Command	Description
dhcp server vlan <1-4094> staticip *<A.B.C.D>* **host** *<STRING_Y>* **mac** *<AA:BB:CC:DD:EE:FF>*	Add static IP DHCP server address pool. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" is used to enter the static IP address for the DHCP server. - Option "<STRING_Y>" specifies the name of the host (DHCP server). - Option "<AA:BB:CC:DD:EE:FF>" specifies the MAC address of the dhcp server.
no dhcp server vlan <1-4094> range *<A.B.C.D>*	Delete dynamic IP range from DHCP server address pool. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" specifies the IP address range to be deleted.
no dhcp server vlan <1-4094> dns *<A.B.C.D>*	Delete domain name server from the DHCP server VLAN. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" specifies the IP address of the DNS to be deleted.
no dhcp server vlan <1-4094> gateway *<A.B.C.D>*	Delete gateway from the DHCP server VLAN. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" specifies the IP address of the gateway to be deleted.
no dhcp server vlan <1-4094> netbios-server *<A.B.C.D>*	Delete netbios server from the DHCP server VLAN. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" specifies the IP address of the netbios server to be deleted.
no dhcp server vlan <1-4094> staticip *<A.B.C.D>*	Delete static IP from the DHCP server VLAN. - Option "<1-4094>" indicates the VLAN ID from 1 to 4094. - Option "<A.B.C.D>" specifies the static IP address to be delete from the DHCP server.

1.4.15 DOTLX

802.1X is an IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices. This protocol restricts unauthorized clients connect to devices. Table 1.16 lists the "dotlx" command for setting 802.1X on the managed switch.

Table 1.16 Descriptions of Commands for 802.1X setting

Command	Description
show dotlx	Show the 802.1X setting and status
dotlx enable	Enable 802.1X feature
no dotlx enable	Disable 802.1X feature
dot1x max-req <2-10>	Configure 802.1X maximum request retries - Option "<2-10>" can be configured from 2 to 10 times.
dot1x port [au/ fu/ fa/ no] [port-list]	Configure 802.1X mode of specify port: - Option "[au/fu/fa/no]" where au: IEEE 802.1X Standard Authorization fu: Force Unauthorized fa: Force Authorized no: No IEEE 802.1X mode - Option "[port-list]" specifies the list of the ports to be configure to specified mode.
dot1x timeout quiet-period [Quiet Period value <10-65535>]	Configure 802.1X Quiet period parameter value setting. - Option "[Quiet Period value <10-65535>]" specifies the timeout quiet period from 10 to 65535 seconds. Default value is 60 seconds.
dot1x timeout radius-server [Radius Server Timeout value <10-300>]	Configure 802.1X Radius Server timeout parameter value setting. - Option "[Radius Server Timeout value <10-300>]" specifies the RADIUS server timeout value from 10 to 300 seconds. Default value is 30 seconds.
dot1x timeout re-authperiod [Re-auth Period value <30-65535>]	Configure 802.1X re-authentication period parameter value setting. - Option "[Re-auth Period value <30-65535>]" specifies the re-authentication timeout period value from 30 to 65535 seconds. Default value is 3600 seconds.
dot1x timeout supplicant [Supplicant Timeout value <10-300>]	Configure 802.1X Supplicant timeout parameter value setting. - Option "[Supplicant Timeout value] <10-300>" specifies the supplicant timeout value from 10 to 300 seconds. Default value is 30 seconds.
dot1x timeout tx-period [Tx Period value <10-65535>]	Configure 802.1X TX period parameter value setting. - Option "[Tx Period value <10-65535>]" specifies the transmission period value from 10 to 65535 seconds. Default value is 15 seconds.

1.4.16 DAYLIGHT-SAVING-TIME

This section shows how users can configure daylight-saving-time setting. In certain regions (e.g. US), local time is adjusted during the summer season in order to provide an extra hour of daylight in the afternoon, and one hour is usually shifted forward or backward. To configure the daylight saving feature in your device, you can use the "daylight-saving-time" command as described in Table 1.17.

Table 1.17 Descriptions of Commands for daylight-saving-time setting

Command	Description
show daylight-saving-time	Show Daylight Saving Time
daylight-saving-time [Month of start day<1-12>][The week in start month<1-5>][Day of week<1-7>][Day hour of start day<0-23>][Month of end day<1-12>][The week in end month<1-5>][Day of week<1-7>][Day hour of end day<0-23>][Offset in hours<1-12>]	Configure Daylight Saving Time. - Option [Month of start day <1-12>]" specifies the month which the daylight saving begins. - Option "[The week in start month<1-5>]" specifies the week number from 1 to 5 wihin the starting month. - Option [Day of week<1-7>] specifies the day of the week that the daylight saving begins. - Option "[Day hour of start day`<0-23>]" specifies the hour of the day that the daylight saving begins. - Option [Month of end day <1-12>]" specifies the month which the daylight saving ends. - Option "[The week in end month<1-5>]" specifies the week number from 1 to 5 wihin the ending month. - Option [Day of week<1-7>] specifies the day of the week that the daylight saving ends. - Option "[Day hour of end day`<0-23>]" specifies the hour of the day that the daylight saving ends. - Option "[Offset in hours<1-12>]" specifies the amount of hours that will be offset during the daylight saving period.
no daylight-saving-time	Disable Daylight Saving Time

1.4.17 DSCP-MAPPING

DiffServ/ToS stands for Differentiated Services/Type of Services. It is a networking architecture that specifies a simple but scalable mechanism for classifying network traffic and providing QoS guarantees on networks. DiffServ uses a 6-bit Differentiated Service Code Point (DSCP) in

the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. Users can configure DSCP Mapping setting using “cos-mapping” command as shown in Table 1.18.

Table 1.18 Descriptions of Commands for DSCP Mapping Setting

Command	Description
cos-mapping priority-queue [Queue number <0-7>] [DSCP number <0-63>]	Configure DSCP-Mapping setting - Option “[Queue number <0-7>]” specifies the queue number of the priority queue. This is the priority number that can be between 0 to 7 where the number 7 is the highest priority and 0 is the lowest priority. - Option “[DSCP number <0-63>]” specifies the Differentiated Service Code Point (DSCP) number which can be from 0 to 63.

1.4.18 DOS

Denial of Service (DoS) is a malicious attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. EHG7XXX industrial managed switch is designed so that uses can filter out various types of attack. Users can configure Denial of Service setting using “dos” command as listed in Table 1.19.

Table 1.19 Descriptions of Commands for Denial-of-Service setting

Command	Description
show dos	Show Denial of Service setting and status
dos icmp enable	Enable ICMP feature or allow filtering ICMP that has packet size higher than the maximum ICMP size defined in the max-icmp-size as listed in the last command of this table.
no dos icmp enable	Disable ICMP feature
dos land-packets enable	Enable (Land Packets feature) prevention over the attack using TCP SYN packet that has the same source and destination’s IP and port.
no dos land-packets enable	Disable Land Packets feature
dos l4-port enable	Enable Layer 4 port (L4 Port feature) prevention over various types of L4 port DoS attacks that are intended to overload the server.
no dos l4-port enable	Disable L4 Port feature
dos tcp-fragment enable	Enable prevention over the TCP fragmentation attack which is targeting TCP/IP reassembly mechanism
no dos tcp-fragment enable	Disable TCP Fragment feature

dos tcp-flag enable	Enable prevention over the TCP flag DOS attack which force the server to keep dropping the packets, causing resource exhaustion.
no dos tcp-flag enable	Disable TCP Flag feature
dos max-icmp-size [size value <0-1023>]	Configure Max ICMP Size value for ICMP dos prevsion feature above. - Option "[size value <0-1023>]" specifies the maximum size of ICMP packet from 0 to 1023. Default value is 512 Bytes.

1.4.19 DIAGNOSIS_CODE

This section shows how users can configure Diagnosis Code setting.

Table 1.20 Descriptions of Commands for Diagnosis Code

Command	Description
diagnosis_code [code]	Configure the code you want to check - Option "[code]"

1.4.20 EXIT

The "exit" command is used to exit from the previous mode of the user. For example, if you are currently in configuration mode, you can exit from the configuration mode by typing in "exit" command.

Table 1.21 Descriptions of Commands for exit to previous mode

Command	Description
exit	Exit to previous mode

1.4.21 ERPS

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability. Note that the users should disable the DIP Switch Control first in order to set up ERPS parameters. Users can configure ERPS settings using "erps" command and its options as described in Table 1.22.

Table 1.22 Descriptions of Commands for ERPS Setting

Command	Description
show erps raps_vlan [RAPS VLAN ID <1-4094>]	Show ERPS Status of the RAPS VLAN ID. - Option "[RAPS VLAN ID<1-4094>]" specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094.
erps enable	Enable ERPS feature

no erps enable	Disable ERPS feature
erps heartbeat interval [interval value <50-10000>]	Configure Heartbeat Interval (millisecond) of ERPS. - Option "[inverval value<50-10000>]" specifies the heartbeat interval from 50 to 10000 milliseconds.
erps log [off/ on]	Turn on or turn off ERPS log state. - Option "[off/on]" is used to disable or enable the log.
erps uerps [off/ on]	Turn on or turn off ERPS uerps state - Option "[off/on]" is used to disable or enable UERPS state. When UERPS is enabled, ring ports periodically sent a "heartbeat" packet to peer ring ports in order to determine whether the link path (etc. wireless bridge) is failure or alive. If peer ring port cannot receive "heartbeat" packets over 3 packets, the ring port will enter protection state. Note: This function affects the recovery time to more than 20 ms.
erps add raps_vlan [RAPS VLAN ID <1-4094>]	Add new RAPS VLAN for ERPS Ring. - Option "[RAPS VLAN ID <1-4094>]" specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094.
erps raps_vlan [RAPS VLAN ID <1-4094>] [on/ off]	Enable/ Disable the Status of RAPS VLAN for ERPS Ring - Option "[RAPS VLAN ID <1-4094>]" specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option [on/off] is used to enable or disable the specified RAPS VLAN ID.
erps raps_vlan [RAPS VLAN ID <1-4094>] east_port [port number]	Configure the east port of ERPS Ring. - Option "[RAPS VLAN ID <1-4094>]" specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option "[port number]" specifies which port number will be the East Port of Ring Protection Link (RPL). Default value is port 2.
erps raps_vlan [RAPS VLAN ID <1-4094>] west_port [port number]	Configure the west port of ERPS Ring. - Option "[RAPS VLAN ID <1-4094>]" specifies the Ring Automatic Protection

	Switch (RAPS) VLAN identification number from 1 to 4094. - Option “[port number]” specifies which port number will be the West Port of the RPL. Default value is port 1.
erps raps_vlan [RAPS VLAN ID <1-4094>] virtual_channel [east_port/ west_port/ none]	Configure the virtual channel of ERPS Ring. - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option “[east_port/west_port/ none]” specifies which port or none of the ports will be the virtual channel.
erps raps_vlan [RAPS VLAN ID <1-4094>] owner	Configure the Owner state of ERPS Ring. - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option “owner” can be enabled or disabled
erps raps_vlan [RAPS VLAN ID <1-4094>] rpl_port	Configure the RPL port of ERPS Ring. - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094.
erps raps_vlan [RAPS VLAN ID <1-4094>] wtr [timer <0-12>]	Configure the WTR timer of ERPS Ring. - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option “[timer<0-12>]” can set the wait-to-restore (WTR) time of the ring in minutes. Lower value has lower protection time. Range of the WTR Timer is from 0 to 12 minutes. Default value is 5 minutes.
erps raps_vlan [RAPS VLAN ID <1-4094>] holdoff [timer <0-10000>]	Configure the Holdoff timer of ERPS Ring. - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option “holdoff [timer <0-10000>]” set the holdoff time of the ring. Range of the Holdoff Timer is from 0 to 10000 milliseconds. Default value is 0 ms.
erps raps_vlan [RAPS VLAN ID <1-4094>] guard [timer <10-2000>]	Configure the Guard timer of ERPS Ring - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection

	Switch (RAPS) VLAN identification number from 1 to 4094. - Option “[timer <10-2000>]” set the guard time of the ring. Range of the guard timer is from 0 to 2000 milliseconds. Default value is 500 ms.
erps raps_vlan [RAPS VLAN ID <1-4094>] mel [<0-7>]	Configure the MEL value of ERPS Ring - Option “[RAPS VLAN ID <1-4094>]” specifies the Ring Automatic Protection Switch (RAPS) VLAN identification number from 1 to 4094. - Option “[<0-7>]” set the maintenance entity group level (MEL) of the ring. Range of MEL is from 0 to 7. Default value is 1.

1.4.22 GARP

GARP: Generic Attribute Registration Protocol, previously called Address Registration Protocol, is a LAN protocol that defines procedures by which end stations and switches can register and de-register attributes, such as network identifiers or addresses with each other. Every end station and switch thus have a record, or list, of all the other end stations and switches that can be reached at a given time. Specific rules are used to modify set of participants in the network topology called reachability tree. This section lists “garp” command and its options for setting up the GARP in Table 1.23.

Table 1.23 Descriptions of Commands for Configuring GARP Settings

Command	Description
show garp timer	Show the current GARP settings on the device
garp timer join [timer <10-65535>]	Configure the join timer of GARP. - Option “[timer <10-65535>]” specifies the join timer from 10 to 65535 step in 10 milliseconds. Default value is 20 in 10 milliseconds.
garp timer leave [timer <10-65535>]	Configure the leave timer of GARP. - Option “[timer <10-65535>]” specifies the leave timer from 10 to 65535 steps in 10 milliseconds. Default value is 60 in 10 milliseconds.
garp timer leave-all [timer <10-65535>]	Configure the leave all timer of GARP. - Option “[timer <10-65535>]” specifies the leave-all timer from 10 to 65535 step in 10 milliseconds. Default value is 1000 in 10 milliseconds.

1.4.23 GMRP

GMRP: GARP Multicast Registration Protocol provides a mechanism that allows bridges (or switches in this case) and end stations to dynamically register group membership information with the MACs of bridges (switches) attached to the same LAN segment and for that information to be disseminated across all bridges (switches) in the Bridged (switched) LAN that supports extend filtering services. GMRP provides a constrained multicast flooding facility similar to IGMP snooping. The difference is that IGMP is IP-based while GMRP is MAC-based. This section lists “gmrp” command and its options for setting up the GMRP in Table 1.24.

Table 1.24 Descriptions of Commands for GMRP Setting

Command	Description
show gmrp db	Show GMRP Database Information
show gmrp gip	Show GMRP Propagation Ring Information
show gmrp machine	Show GMRP Applicant/Registrar State Machine
show gmrp status	Show GMRP Operation Status
show gmrp statistics	Show GMRP Packet Counter
gmrp enable	Enable GMRP feature
no gmrp enable	Disable GMRP feature
clear gmrp statistics	Clear GMRP Statistics information

1.4.24 GVRP

GVRP: GARP VLAN Registration Protocol. GVRP is similar to GARP, but work with VLAN instead of other network identifiers. It provides a method to exchange VLAN configuration information with other devices and conforms to IEEE 802.1Q. This section lists “gvrp” command and its options for setting up the GVRP in Table 1.25.

Table 1.25 Descriptions of Commands for GVRP Setting

Command	Description
show gvrp db	Show GVRP Database Information
show gvrp gip	Show GVRP Propagation Ring Information
show gvrp machine	Show GVRP Applicant/Registrar State Machine
show gvrp status	Show GVRP Status
show gvrp statistics	Show GVRP Packet Counter
gvrp enable	Enable GVRP feature
no gvrp enable	Disable GVRP feature
clear gvrp statistics	Clear GVRP Statistics information

1.4.25 HELP

When the users enter the “help” command on the command line interface (CLI), they will be shown with explanation of how to use “?” symbol with any command and option as shown in Figure 1.10. The description of “help” command is provided in Table 1.26.

```
switch# help
  When you need help, anytime at the command line please press '?'.
  If nothing matches, the help list will be empty and you must
  backup until entering a '?' shows the available options.
  Two styles of help are provided:
  1. Full help is available when you are ready to enter a command
     argument (e.g. 'show ?') and describes each possible argument.
  2. Partial help is provided when an abbreviated argument is
     entered and you want to know what arguments match the input
     (e.g. 'show hi?'.)
switch#
```

Figure 1.10 How to use help or "?" in the CLI.

Table 1.26 Descriptions of Commands for CLI description

Command	Description
help	Show two styles description of help description.

1.4.26 HISTORY

On the CLI, users can check the history of commands that they entered by using "show history" command. The command's history can be disabled with "no history" command. The number of commands in the history list can be set too as shown in Table 1.27.

Table 1.27 Descriptions of history commands

Command	Description
show history	List the commands previously entered by the users.
history [number <0-256>]	Set the number of commands in the history list. - Option "[number<0-256>] specifies the number of commands in the history list.
no history	Disable command's history feature

1.4.27 HTTPS

Table 1.28 shows how to configure secure HTTP or Hypertext Transfer Protocol Secure (HTTPS) login setting using the "https" command.

Table 1.28 Descriptions of Commands for HTTPs setting

Command	Description
https enable	Enable Web GUI login by HTTPS
no https enable	Disable Web GUI login by HTTPS

1.4.28 IP ARP INSPECTION

Dynamic ARP Inspection (DAI) is another security feature provided by EHG7XXX managed switch to prevent a class of man-in-the-middle attacks. This type of attacks occurs when a malicous node intercepts packets intended for other nodes by poisoning the ARP caches of its unsuspecting neighbors. To create the attack, the malicous node sends ARP requests or responses mapping another node's IP address to its own MAC address.

To prevent this kind of attack, EHG7XXX managed switch ensures that only valid ARP requests and responses are forwarded. Invalid and malicous ARP packets will be dropped by the switch. DAI relies mainly on DHCP snooping mechanism that listens to DHCP message exchanges. Then, DAI creates a bindings database of valid tuples of MAC address, IP address, and VLAN interface. DAI is related to the function of ARP Spoof Prevention (another security feature in EHG7XXX). DAI will drop all ARP packets if the IP-to-MAC binding is not present in the DHCP snooping bindings database. However, if some static IP address is needed to pass through the switch, the user should add this static IP-to-MAC binding in the ARP Spoof Prevention. This static mapping is useful when nodes configure static IP addreses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection.

Note that you cannot configure the Dynamic ARP inspection (DAI) without enabling DHCP Snooping feature. Please enable DHPC Snooping using command in Section 1.4.31 and obtain DHCP data first. Table 1.29 summarizes the “ip arp inspection” command and its options.

Table 1.29 Descriptions of Commands for IP ARP Inspection

Command	Description
ip arp inspection enable	Enable IP ARP Inspection feature
no ip arp inspection enable	Disable IP ARP Inspection feature
ip arp inspection trust [port-list]	Configure IP ARP Inspection trust port settings. - Option “[port-list]” is the list of trust ports which can be separated by symbol ","s or "-"s.

1.4.29 IP DEFAULT-GATEWAY

One of the IP protocol settings is the default gateway, using “ip default-gateway” command users can set the IP address for EHG7XXX as shown in Table 1.30.

Table 1.30 Descriptions of Commands for IP Default Gateway

Command	Description
ip default-gateway [ip address]	Configure Default gateway IP address. - Option “[ip address]” specifies the IP address of the default gateway.

1.4.30 IP DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a routing protocol for IP multicast packets. It is described in RFC 1075 as an interior gateway protocol (IGP) within a multicast domain and is derived from Routing Information Protocol (RIP), which is suitable for use within an autonomous system. DVMRP uses the Internet Group Management Protocol (IGMP) to exchange routing information with other routers. It operates via a reverse path flooding technique in which it sends a copy of received IGMP message (containing routing information) out through each interface except the one at which the message arrived. By using flooding technique, the DVMPR may not scale very well in some network topologies. DVMRP creates a routing table with route entries that map between multicast group (IP address) and source address. The purpose of DVMRP is to keep track of the return paths to the source of multicast

datagrams. DVMRP router dynamically discovers their Neighbors by sending Neighbor probe messages periodically to an IP multicast group address that is reserved for all DVMRP routers.

To enable DVMRP on EHG7XXX, you first need to configure at least two VLAN interfaces, set all relevant parameters for the interfaces such as IP addresses, DVMRP VLAN and enable IP Routing. To setup the DVMRP, users can use the “ip dvmrp” command and its options as listed in Table 1.31.

Table 1.31 Descriptions of Commands for DVMRP Setting

Command	Description
show ip dvmrp routing	Show IP DVMRP routing information
ip dvmrp restart	Enable/Restart IP DVMRP feature
no ip dvmrp	Disable IP DVMRP feature
ip dvmrp vlan [vlan id<1-4094>] metric [<1-31>]	Add IP DVMRP rule. - Option “[vlan id<1-4094>]” specifies the VLAN ID to be added. - Option “[<1-31>]” specifies the route matric for the VLAN ID. Note that the Route Metric is the cost of the path (or VLAN interface) through which the packet will be sent. Note that the default metric is 1.
no ip dvmrp vlan [vlan id<1-4094>]	Delete IP DVMRP rule. - Option “[vlan id<1-4094>]” specifies the VLAN ID to be deleted.

1.4.31 IP DHCP SNOOPING BINDING

A rogue DHCP (Dynamic Host Control Protocol) server may be set up by an attacker in the network to provide falsify network configuration to a DHCP client such as wrong IP address, incorrect subnetmask, malicious gateway, and malicous DNS server. The purpose of DHCP spoofing attack may be to redirect the traffic of the DHCP client to a malicous domain and try to eavesdrop the traffic or simply try to prevent a successful network connection establishment. To protect againt a network security attack of rogue DHCP server or DHCP spoofing attack, Atop’s EHG7XXX managed switch provides DHCP Snooping feature. When this feature is enabled on specific port(s) of EHG7XXX managed swicth, the EHG7XXX will allow the DHCP messages from trusted ports to pass through while it will discard or filter the DHCP messages from untrusted ports. To enable the DHCP Snooping feature, users can use the “ip dhcp snooping” command and its options listed in Table 1.32.

Table 1.32 Descriptions of Commands for IP DHCP Snooping

Command	Description
show ip dhcp snooping binding	Show IP DHCP Snooping Binding information
ip dhcp snooping enable	Enable IP DHCP Snooping Binding
no ip dhcp snooping enable	Disable IP DHCP Snooping Binding

ip dhcp snooping trust [port-list]	Configure IP DHCP Snooping Binding trust port settings. - Option “[port-list]” is the list of trust ports which can be separated by symbol ","s or "-"s.
no ip dhcp snooping trust [port-list]	Delete IP DHCP Snooping Binding trust port setting. - Option “[port-list]” is the list of trust ports which can be separated by symbol ","s or "-"s.

1.4.32 IP MANAGEMENT

The management VLAN Identification number (ID) is configured based on the IEEE 802.1Q standard. The default value is VID = 1. To configure IP management VLAN ID, users can use the “ip management” command as shown in Table 1.33.

Table 1.33 Descriptions of Commands for IP Management Setting

Command	Description
ip management [vlan id<1-4094>]	Modify Interface Management VID. - Option “[vlan id<1-4094>]” specifies the VLAN ID to be management VLAN. Default value is 1.

1.4.33 IP PIM

Table 1.34 lists the command “ip pim debug” that can configure IP Protocol Independent Multicast (PIM) Debug setting.

Table 1.34 Descriptions of Commands for IP PIM debug

Command	Description
ip pim debug enable	Enable debugging the IP Protocol Independent Multicast (PIM)
ip pim debug disable	Disable debugging the IP Protocol Independent Multicast (PIM)

1.4.34 IP PIM-SM

PIM Sparse Mode (SM) uses the concept of Rendezvous Point (RP) as a meeting point for any routers or Layer-3 switches that will involve in multicasting as multicast source and receivers. The RP can be manually configured as Static Rendezvous or can be automatically discover in the network using some protocols such as Bootstrap Rendezvous. Each router or Layer-3 switch that receives multicast traffic from a source will forward it to the RP. Routers or Layer-3 switches in PIM SM will not forward any multicast traffic unless some node requests it. Each router or Layer-3 switch called Designated Router (DR) that would like to receive multicast traffic will have to send or forward a PIM Join message to the RP.

PIM Sparse Mode (PIM SM) explicitly builds unidirectional root path tree (RPT) or shared distributed tree rooted at a Rendezvous Point (RP) per multicast group. PIM SM can optionally create shortest-path tree per source so that the router or Layer-3 switch can switch to Source Path Tree (SPT) or Shortest-Path Tree (SPT) which is the most optimal path. This switch operation can remove the RP from the shared distributed tree and get multicast traffic directly from the multicast source. Note that receivers that never switch to shortest-path tree are effectively running Core Based Trees (CBT).

PIM SM generally scales fairly well for wide-area usage. The RP helps reduce the amount of states in other non-RP routers or switches in the network. However, all routers or Layer-3 switches in PIM SM domain must provide mapping to a Rendezvous Point router/switch. The following command line interface (CLI) in Table 1.35 can be used to configure PIM SM to support multicast routing.

Table 1.35 Descriptions of Commands for PIM SM Configuration

Command	Description
ip pim-sm	Enable PIM-SM
no ip pim-sm	Disable PIM-SM
ip pim-sm hello interval <30-18724>	Configure hello interval for PIM-SM. - Option “<30-18724>” set the duration of hello interval from 30 to 18724 seconds. Default value is 30 seconds. PIM Hello messages are sent periodically on each PIM-enabled interface. They allow a router to learn about neighboring PIM routers on each interface.
ip pim-sm spt-switchover no ip pim-sm spt-switchover	Enable or disable shortest path switch-over feature. Default setting is enabled.
ip pim-sm vid <1-4094> dr-priority <1-4294967294> route-distance <1-255> route-metric <1-1024>	Configure DR-Priority, Route-Distance and Route-Metric - Option “<1-4094>” specifies the VLAN ID. - Option “<1-4294967294>” specifies the Designated Router (DR) priority. When there are multiple PIM routers on the same LAN the DR (Designated Router) is usually elected based on the highest numerical IP address. This setting can be used to control the DR Priority option in PIM Hello messages, When the DR Priority option is advertised by all PIM routers on the same LAN the highest priority router wins the DR election, regardless of its IP. If any router does not advertise the DR Priority option, or the same priority is advertised by more

Command	Description
	than one router, the protocol falls back to using the IP address. - Option “<1-255>” specifies the route distance. The default route distance option has nothing to do with system default route, it is rather the default value for unicast routing protocol’s administrative distance. It is used in PIM assert election to determine upstream router. - Option “<1-1024>” specifies the route metric. When there are multiple PIM enabled routers on a shared segment, it is possible that these routers encounter duplicate multicast traffic. PIM assert messages which are triggered when you receive a multicast packet on the Outgoing Interface List (OIL). These assert messages contain metrics which are then used to calculate who will become assert winner. When comparing assert_metrics, the rpt_bit_flag, metric_preference, and route metric fields are compared in order, where the first lower value wins. If all fields are equal, the primary IP address of the router that sourced the Assert message is used as a tie-breaker, with the highest IP address winning.
ip pim-sm rp-priority <0-255> bsr-priority <0-255>	Configure Rendezvous Point (RP) priority and Bootstrap Router (BSR) priority - Option “<0-255>” specifies the priority of rendezvous point. - Option “<0-255>” specifies the priority of bootstrap router.
ip pim-sm election <static/bootstrap>	Configure PIM-SM election type as either static or bootstrap. - Option “<static/bootstrap>” is used to select between static or bootstrap election type.
ip pim-sm rp-candidate vid <vlan-id> group <A.B.C.D/M>	Configure RP candidate group IP addresses. - Option “<vlan-id>” specifies the VLAN ID of the RP candidate. - Option “<A.B.C.D/M>” specifies the IP address and subnet mask.

Command	Description
ip pim-sm rp-address <A.B.C.D> group <A.B.C.D/M>	Configure Static RP address and group address. - Option "<vlan-id>" specifies the VLAN ID of the static RP address. - Option "<A.B.C.D/M>" specifies the IP address and subnet mask.
Static-routing add <name> <Dest. IP> <mask> <Gateway IP>	Add static routing. - Option "<name> <Dest. IP> <mask> <Gateway IP>" is used to add required network information for static route.
show ip pim-sm	Display PIM Sparse Mode (SM) Configuration
show ip pim-sm bsr	Display PIM Sparse Mode (SM) bootstrap router (BSR)
show ip pim-sm rp-address	Display PIM Sparse Mode Static RP Address
show ip pim-sm neighbor	Display PIM Sparse Mode Neighbor Table
show ip pim-sm routing	Display PIM Sparse Mode (SM) Multicast Routing Table
ip pim-sm restart	Restart PIM Sparse Mode (SM) process
igmp-query-interval	Display IGMP's Query Interval
ip igmp join vid <vlan-id> group <group-address>	Send IGMP join message (*,G) - Option "join vid<vlan-id>" specifies the VLAN ID to join. - Option "group <group-address>" specifies the group address to join.
ip igmp leave vid <vlan-id> group <group-address>	Send IGMP leave message (*,G) - Option "<vlan-id>" specifies the VLAN ID to leave. - Option "<group-address>" specifies the group address to join.

1.4.35 IP PIM-SSM

PIM Source Specific Mode (SSM) uses a subset of PIM Sparse Mode and IGMP version 3 (IGMPv3). It allows a client to receive multicast traffic directly from a source which is more secure and scalable. PIM SSM only supports the one-to-many multicasting model. Thus, it is simpler than the PIM Sparse Mode. It is suitable for most broadcasting of content such as Internet video applications. An SSM group, called a channel, is identified as (S, G) where S is the source address and G is the group address. The IPv4 address range reserved for mulitcast group of SSM is 232.0.0.0/8 but it can technically be used in the entire 224/4 multicast address range. PIM SSM builds shortest path trees (SPTs) rooted at the source immediately after receivers issued join message (or subscribing message) toward the source. It bypasses the procedures of Rendezvous Point (RP) connection as used in PIM SM and goes directly to the source-based distribution tree. Since PIM SSM does not rely on RP mechanism, it may require manual configuration or external method to learn in advance about the address of multicast source(s). In EHG7XXX Layer-3 Managed Switch, you will need to know the Source Address and enter it in

the IGMP join/leave message. The following command line interfaces (CLI) in Table 1.36 can be used to configure PIM SSM to support multicast routing.

Table 1.36 Descriptions of Commands for PIM SSM Configuration

Command	Description
ip pim-ssm	Enable PIM-SSM (Source Specific Mode)
no ip pim-ssm	Disable PIM-SSM
ip pim-ssm hello interval <30-18724>	Configure hello interval for PIM-SSM. - Option “<30-18724>” specifies the hell interval from 30 to 18724 seconds.
ip pim-ssm add-group <A.B.C.D/M>	Configure source group IP addresses. - Option “<A.B.C.D/M>” is used to add source group IP addresses and subnetmasks.
no ip pim-ssm group <A.B.C.D/M>	Delete source group IP addresses. - Option “<A.B.C.D/M>” specifies the IP addresses to be deleted.
show ip pim-ssm	Display PIM SSM configuration
show ip pim-ssm neighbor	Display PIM SSM Neighbor table
show ip pim-ssm routing	Display PIM SSM multicast routing table
ip pim-ssm restart	Restart PIM SSM
ip pim-ssm vid <1-4094> dr-priority <1-4294967294> route-distance <1-255> route-metric <1-1024>	Configure Designated Router (DR) Priority, Route-Distance and Route Metric. - Option “<1-4094>” specifies the VLAN ID. - Option “<1-4294967294>” specifies the priority of Designated Router. - Option “<1-255>” specifies the route distance. - Option “<1-1024>” specifies the route metric.
ip igmp join vid <vlan-id> group <group-address>	Send IGMP join message (*,G) for any source multicast. - Option “<vlan-id>” specifies the VLAN ID. - Option “<group-address>” specifies the group address.
ip igmp join vid <vlan-id> group <group-address. source <source-address>	Send IGMP join message (S,G) for SSM. - Option “<vlan-id>” specifies the VLAN ID. - Option “<group-address>” specifies the group address. - Option “<source-address>” specifies the source address.

Command	Description
ip igmp leave vid <vlan-id> group <group-address>	Send IGMP leave message (*,G) for any source multicast - Option "<vlan-id>" specifies the VLAN ID. - Option "<group-address>" specifies the group address.
ip igmp leave vid <vlan-id> group <group-address> source <source-address>	Send IGMP leave message (S,G) for SSM - Option "<vlan-id>" specifies the VLAN ID. - Option "<group-address>" specifies the group address. - Option "<source-address>" specifies the source address.

1.4.36 IP PIM-DM

PIM Dense Mode (PIM DM) is a multicast routing protocol which is designed under the assumption that the receivers for any multicast group are distributed densely throughout the network. Its assumption is opposite to the PIM Sparse Mode. As a PIM protocol, PIM DM utilizes unitcast routing tables built by other routing protocol. PIM DM control message processing and data packet forwarding is integrated with PIM SM operations such that a single router or Layer-3 switch can run different PIM modes for different multicast groups.

Multicast packet is initially sent to all hosts in the network. PIM DM relies on Reverse Path Multicasting (RPM) in which multicast packet is forwarded if the receiving interface is the one used to forward unicast packets to the source of the packet. If not, the packet is dropped. This mechanism prevents forwarding loops from occurring. The multicast packet is then forwarded out on all other interfaces. PIM Dense Mode uses explicit trigger grafts/prunes to manage its source-based acyclic tree. Routers that do not have any interested hosts then send PIM Prune messages to remove themselves from the tree. Note that grafts are messages sent towards known sources and used by new members to add themselves onto an existing distribution tree. Prunes are messages sent toward a source by a router when it wants to leave the distribution tree.
A node in PIM DM such as EHG7XXX will create a multicast forwarding entry for a particular source-rooted distribution tree when a data packet from that source to the group first arrives. PIM DM only uses source-based trees. As a result, it does not use Rendezvous Points (RPs), which makes it simpler than PIM SM to implement and deploy. It is an efficient protocol when most receivers are interested in the multicast data but it does not scale well across larger domains in which most receivers are not interested in the data. The following command line interfaces (CLI) in Table 1.37 can be used to configure PIM DM to support multicast routing.

Table 1.37 Descriptions of Commands for PIM DM Configuration

Command	Description
ip pim-dm	Enable PIM-DM
no ip pim-dm	Disable PIM-DM

Command	Description
ip pim-dm vlan <1-4094> preference <1-255> metric <1-255>	Adding VLAN to PIM-DM. - Option "<1-4094>" specifies the VLAN ID to be added. - Option "<1-255>" specifies Route Preference. Note that the Route Preference is used by assert elections to determine upstream routers. - Option "<1-255>" specifies the Route Metric. Note that the Route Metric is the cost of the path through which the packet is to be sent.
no ip pim-dm vlan <1-4094>	Delete VLAN from PIM-DM. - Option "<1-4094>" specifies the VLAN ID to be deleted.
ip pim-dm vlan <1-4094> preference <1-255>	Updating the preference ID for PIM-DM. - Option "<1-4094>" specifies the VLAN ID to be updated. - Option "<1-255>" specifies Route Preference to be updated.
ip pim-dm vlan <1-4094> metric <1-255>	Updating the metric for PIM-PM. - Option "<1-4094>" specifies the VLAN ID to be updated. - Option "<1-255>" specifies Route Metric to be updated.

1.4.37 IP SOURCE BINDING

The IP Source Binding is a static IP Source Guard that creates a Layer-2 packet filtering on each port of the EHG7XXX. This packet filter will require specific Source IP Address and Source MAC Address to be entered for each port. Using "ip source binding" command and its options listed in Table 1.39, users can configure IP Source Binding setting.

Table 1.38 Descriptions of Commands for IP Source Binding

Command	Description
show ip source binding config	Show current IP source binding configuration.
ip source binding [MAC address] [ip address] [port-list]	Configure IP source binding settings. - Option "[MAC address]" specifies the source MAC address. - Option "[ip address]" specifies the source IP address. - Option "[port-list]" specifies the list of ports which can be separated by ","s or "-"s.
no ip source binding [index<1-128>]	Delete IP source binding rule

Command	Description
	- Option “[index <1-128>]” specifies the index of the IP source binding rule to be deleted.

1.4.38 IP VERIFY SOURCE

The IP Verify Source is a dynamic IP Source Guard that creates a Layer-2 packet filtering on each port of the EHG7XXX. The filter types can be IP or IP-MAC. For IP filter type, EHG7XXX will check only the Source IP address of the packets. For IP-MAC filter type, EHG7XXX will consider both Source IP address and Source MAC address of the packets. To configure IP Verify Source DHCP-Snooping, users can use “ip verify source” command as shown in Table 1.39.

Table 1.39 Descriptions of Commands for IP Verify Source DHCP-Snooping

Command	Description
show ip verify source config	Show IP Verify Source DHCP-Snooping setting
ip verify source dhcp-snooping [ip/ip-mac] [port-list]	Configure IP Verify Source DHCP-Snooping settings - Option “[ip/ip-mac]” indicates filter types which can be either IP filter type or IP-MAC filter type. - Option “[port-list]” specifies the list of ports which can be separated by ","s or "-"s.
no ip verify source dhcpsnooping [port-list]	Delete IP Verify Source DHCP-Snooping rule - Option “[port-list]” specifies the list of ports which can be separated by ","s or "-"s.

1.4.39 IPV6

Atop’s industrial managed switch can operate in Internet Protocol version 6 (IPv6) network. The users can configure parameters for IPv6 network using “ipv6” command and its options as listed in Table 1.40.

Table 1.40 Descriptions of Commands for IPv6 Setting

Command	Description
show ipv6 status	Show IPv6 status of DUT
ipv6 default-gateway [ipv6 address]	Configure IPv6 default gateway of DUT - Option “[ipv6 address]” specifies the IPv6 address of the default gateway.
no ipv6 default-gateway	Remove IPv6 default gateway
ipv6 dns [ipv6 address] [ipv6 address]	Configure IPv6 primary dns and secondary dns

Command	Description
	- Option “[ipv6 address] [ipv6 addresss]” specify primay DNS IPv6 address and secondary DNS IPv6 address.
no ipv6 dns	Remove IPv6 DNS
ipv6 manual-dns enable	Enable IPv6 Manual DNS
no ipv6 manual-dns enable	Disable IPv6 Manual DNS

1.4.40 IGMP

The managed switch supports Internet Group Management Protocol (IGMP) which is a communication protocol used on IP version 4 networks to establish multicast group memberships among switches in the network. IGMP is an integral part of IPv4 multicast. It operates above the network layer of OSI model. To configure IGMP, users can use the command “igmp” and its options listed in Table 1.41.

Table 1.41 Descriptions of Commands for IGMP Setting

Command	Description
show igmp groups	Show IGMP membership table
show igmp querrier	Show IGMP query interval
show igmp router	Show IGMP multicast routers
show igmp status	Show IGMP status
show igmp table	Show IP multicast table
igmp enable	Enable IGMP feature
no igmp enable	Disable IGMP feature
igmp debug	Enable IGMP debug feature
no igmp debug	Disable IGMP debug feature
igmp fastleave	Enable IGMP fastleave feature
no igmp fastleave	Disable IGMP fastleave feature
igmp proxy	Enable IGMP proxy feature
no igmp proxy	Disable IGMP proxy feature
igmp querrier interval [interval <12-60>]	Configure IGMP Querrier Interval. - Option “[interval <12-60>]” specifies querrier interval from 12 to 60
igmp table static [multicast ip address] [vlan id<1-4094>] [port-list]	Configure IGMP IP Multicast table. - Option “[multicast ip address]” specififes the multicast IP address to be added. - Option “<1-4094>” specifies VLAN ID. - Option “[port-list]” specifies the list of ports or trunk list, e.g. 3, 6-8, Trk2.
no igmp table static [multicast ip address]	Clear IGMP IP Multicast table - Option “[multicast ip address]” specifies the multicast IP address to be deleted.

1.4.41 IA-RING

The Atop's managed switch is designed to be compatible with iA-Ring protocol for providing better network reliability and faster recovery time for redundant ring topologies. It is in the same category as R Rings, but with its own protocol. It has been a successful development that reduces recovery time to less than 20 ms. iA-Ring can be used for any single ring. Note that the users should disable DIP Switch Control and disable ERPS first in order to enable/configure iA-Ring parameters. To configure iA-Ring protocol, users can use "ia-ring" command and its options listed in Table 1.42.

Table 1.42 Descriptions of Commands for iA-Ring Setting

Command	Description
show ia-ring	Show ia-ring status and setting
ia-ring enable	Enable ia-ring feature
no ia-ring enable	Disable ia-ring feature
ia-ring master	Configure DUT as ring master
no ia-ring master	Disable DUT as ring master
ia-ring ringport [1st ring port] [2nd ring port]	Configure ia-ring 1st/2nd port setting. - Option "[1st ring port] [2nd ring port]" specifies the 1st and 2nd ring ports.

1.4.42 IP-ROUTING

To enable the Internet Protocol (IP) routing or Layer-3 (L3) routing function on the EHG7XXX Industrial L3 Managed, users can use "ip-routing" commands listed in Table 1.43. This IP routing option should be enabled before any other IP routing functions (static routing and dynamic routing) can be used.

Table 1.43 Descriptions of Commands for IP-Routing Setting

Command	Description
show ip-routing	Show ip-routing feature status
ip-routing enable	Enable ip-routing feature
no ip-routing enable	Disable ip-routing feature

1.4.43 LOGOUT

When you finished your configuration tasks, you can logout of the CLI by issuing "logout" command shown in Table 1.44.

Table 1.44 Descriptions of Logout Command

Command	Description
logout	To logout of the CLI and return to the username prompt.

1.4.44 LLDP

Link Layer Discovery Protocol (LLDP) is an IEEE802.1ab standard OSI layer-2 protocol. LLDP allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification. The advertise packets are periodically sent to directly connected devices on the network that are also using LLDP or so called its neighbors. LLDP is a “one hop” unidirectional protocol in an advertising mode.

LLDP information can only be sent to and received by devices, no solicit information or state changes between nodes. The device has a choice to turn on and off sending and receiving function independently. Advertised information is not forward on to other devices on the network. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply. To configure LLDP, users can use “lldp” command and its options listed in Table 1.45.

Table 1.45 Descriptions of Commands for LLDP Setting

Command	Description
show lldp neighbors	Show LLDP neighbors’ information
show lldp status	Show LLDP feature status
show lldp txttl	Show LLDP Transmit (Tx) Time-To-Live (TTL) setting value. Note that it is the amount of time to keep neighbors’ information.
show lldp txinterval	Show LLDP Tx Interval setting value
lldp enable	Enable LLDP feature
no lldp enable	Disable LLDP feature
lldp txinterval [interval <5-65535>]	Configure LLDP Tx (Transmit) Interval setting value. - Option “[interval <5-65535>]” specifies the transmit interval.
lldp txttl [interval <5-65535>]	Configure LLDP Tx TTL setting value. - Option “[interval <5-65535>]” specifies the interval of Tx Time-To-Live (TTL). Note that the recommend TTL value is 4 times of Tx Interval. The information is only removed when the timer is expired. Range from 5 to 65535 seconds.

1.4.45 LACP

The users have an option to enable Link Aggregation Control Protocol (LACP) which is an IEEE standard (IEEE 802.3ad, IEEE 802.1AX-2008) in each port group or trunk. LACP allows the managed switch to negotiate an automatic bindling of links by sending LACP packets to the LACP partner or another device that is directly connected to the managed switch and also implements LACP. The LACP packets will be sent within a multicast group MAC address. If LACP finds a device on the other end of the link that also has LACP enabled, it will also

independently send packets along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. During the detection period LACP packets are transmitted every second. Subsequently, keep alive mechanism for link membership will be sent periodically. Each port in the group can also operate in either LACP active or LACP passive modes. The LACP active mode means that the port will enable LACP unconditionally, while LACP passive mode means that the port will enable LACP only when an LACP partner is detected. Note that in active mode LACP port will always send LACP packets along the configured links. In passive mode however, LACP port acts as “speak when spoken to”, and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode). Users can check the status of LACP and set the LACP system priority using “lacp” commands as shown in Table 1.46.

Table 1.46 Descriptions of Commands for LACP Setting

Command	Description
show lacp status	Show LACP setting status and each port status
lacp system-priority [priority <1-65535>]	Configure LACP system priority setting (default: 32768) - Option “[priority <1-65535>]” specifies the LACP system priority. Note that system priority is used during the negotiation with other systems. System priority and switch’s MAC address is used to form a system ID. A higher number means a lower priority.

1.4.46 MAC-AGE-TIME

This “mac-age-time” command in

Table 1.47 allows users to set MAC address age-out or aging time manually. In the managed switch, a MAC address table is stored in the memory to map a MAC address and a port number to forward frames. The aging time is the duration of time to keep MAC addresses in the MAC address table. For a longer aging time, the learned MAC address will stay in the memory longer. As a result, the switch will be able to forward the frames to a specific port quickly instead of forwarding to all the ports to prevent frame flooding. A shorter aging time will allow the switch to free up the old MAC addresses in the table to learn new MAC addresses. This will be useful when there are large number of MAC addresses (or end devices) in the network and when the traffic between any two end devices are short-lived.

Table 1.47 Descriptions of Commands for MAC address table setting

Command	Description
mac-age-time [time <0-600>]	Configure MAC address aging time, “0” means disabled. - Option “[time <0-600>]” specifies MAC aging time in seconds.

1.4.47 MONITOR

In order to help the network administrator keeps track of network activities, the managed switch supports port mirroring, which allows incoming and/or outgoing traffic to be monitored by a single port that is defined as a mirror port. Note that the mirrored network traffic can be analyzed by a network analyzer or a sniffer for network performance or security monitoring purposes. Port mirror feature in the managed switch can be configured by using “monitor” commands as shown in Table 1.48.

Table 1.48 Descriptions of Commands for Port Mirror Setting

Command	Description
show monitor	Show Port Mirror feature status
monitor [direction<both/rx/tx] [mirror-to-port] [mirrored ports list]	Configure port mirror feature. - Option “[direction <both/rx/tx]” specifies the monitoring direction which can be both direction or input (rx) or output (tx). - Option “[mirror-to-port]” specifies the mirror port that will be used to monitor the activity of the other monitored ports. - Option “[mirrored ports list]” specifies the list of mirrored ports which can be separated by ","s or "-"s.
no monitor	Disable port mirror feature

1.4.48 MAC-ADDRESS-TABLE

Information of current static Unicast and Multicast MAC addresses in the memory of the managed switch is the static MAC address table. Users can configure static MAC Address Table using “mac-address-table” command and its options as listed in Table 1.49.

Table 1.49 Descriptions of Commands for Add Static MAC address rule

Command	Description
show mac-address-table static	Show Static MAC-Address-Table information
mac-address-table static [MAC address] [vlan ID <1-4094>] [port list]	Add Static MAC-Address-Table rule. - Option “static [MAC address]” specifies the static MAC address to be added. - Option “[vlan ID <1-4094>]” specifies the VLAN ID. - Option “[port list]” specifies the list of ports which can be separated by ","s or "-"s.
no mac-address-table static [MAC address] [vlan ID <1-4094>]	Remove Static MAC-Address-Table rule. - Option “static [MAC address]” specifies the static MAC address to be removed.

	- Option “[vlan ID <1-4094>]” specifies the VLAN ID.

1.4.49 MLD_SNOOPING

Multicast Listener Discovery (MLD) is a protocol used by EHG7XXX in Internet Protocol Version 6 (IPv6) network to discover nodes on its directly attached interfaces that would like to receive multicast packets. These neighboring nodes are called multicast listenters. MLD is embedded in ICMPv6 (Internet Control Message Protocol Version 6) as a part of IPv6 protocol suit.

Typically, MLD device can be classified as one of the follows: a querier, a snooper, or a proxy. An MLD querier is a device that coordinate multicast streams and MLD membership information. The MLD querier can generate membership query message to check which nodes are group members. It can process membership reports and leave messages. An MLD snooper is a device that spies on MLD messages to create flow efficiencies by allowing only subscribed interfaces to receive multicast packets. The MLD snooper can decide on the best path to send multicast packets at Layer 2; however, it cannot alter those packets or generate its own MLD messages. An MLD proxy is a device that passes membership reports upstream towards a source in anoter subnet. On the downstream, the MLD proxy will forward multicast packets and queries towards one or more IP subnets.

Table 1.50 lists the command “mld_snooping” which allows users to configure MLD snooping settings.

Table 1.50 Descriptions of Commands for MLD Snooping Setting

Command	Description
show mld_snooping status	Show MLD_Snooping feature status and information
show mld_snooping group vlan	Show MLD_Snooping VLAN group status and information
show mld_snooping vlan	Show MLD_Snooping VLAN status and information
mld_snooping enable	Enable MLD Snooping feature
mld_snooping disable	Disable MLD Snooping feature
mld_snooping config vlan [vlan id <1-4094>]	Add MLD Snooping VLAN rule. - Option “[vlan id <1-4094>]” specifies VLAN ID to be added.
mld_snooping [vlan id <1-4094>] donetimer [timer <1-16711450>]	Configure MLD Snooping of specified VLAN donetimer setting. - Option “[vlan id <1-4094>]” specifies the VLAN ID to set donetimer. - Option “donetimer [timer <1-16711450>]” specifies the duration of done timer in seconds.
mld_snooping [vlan id <1-4094>] nodetimeout [timer <1-16711450>]	Configure MLD Snooping of specified VLAN nodetimeout setting.

Command	Description
	- Option “[vlan id <1-4094>]” specifies the VLAN ID to set nodetimeout. - Option “[timer <1-16711450>]” specifies the node timeout in seconds. This is the amount of time that a node on a port will no longer be considered as a multicast listener.
mld_snooping [vlan id <1-4094>] fastdone [0/1]	Configure MLD Snooping of specified VLAN fastdone setting. - Option “[vlan id <1-4094>]” specifies the VLAN ID to set fastdone function. - Option “[0/1]” is used to enable (1) or disable (0) fastdone function.
mld_snooping [vlan id <1-4094>] status [0/1]	Configure MLD Snooping of specified VLAN status setting. - Option “[vlan id <1-4094>]” specifies the VLAN ID to set status. - Option “status [0/1]” is used to enable (1) or disable (0) status.

1.4.50 NTP-SERVER

This section shows how users can configure NTP Server setting using “ntp-server” commands as listed in Table 1.51.

Table 1.51 Descriptions of Commands for NTP Server Setting

Command	Description
show ntp-server	Show NTP Server status
ntp-server enable	Enable NTP Server feature
no ntp-server enable	Disable NTP Server feature

1.4.51 OPTION66/67

This section shows how users can configure option66/67 setting which is related to Trivial File Transfer Protocol (TFTP). Enable this option to allow the managed switch to learn of TFTP Server Name and the filename to be used from a DHCP packet.

Table 1.52 Descriptions of Commands for Option66/67

Command	Description
show option66_67 status	Show option66_67 feature status
option66_67 enable	Enable option66_67 feature
no option66_67 enable	Disable option66_67 feature

1.4.52 OSPF

OSPF (Open Shortest Path First) version 2 is another routing protocol supported by EHG7XXX industrial L3 managed switch. It is described in RFC2328. OSPF is an IGP (Interior Gateway Protocol) which uses link states for route selection. It propagates link-state advertisements (LSAs) to its Neighbor switches. When compared with RIP (Routing Information Protocol) which is a distance vector-based routing protocol, OSPF can provide scalable network support and faster convergence time for network routing state. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and enterprise networks. To configure OSPF routing protocol, users can use "ospf" command and its options as listed in Table 1.53.

Table 1.53 Descriptions of Commands for OSPF

Command	Description
show ospf area setting	Show OSPF area setting
show ospf area-range setting	Show OSPF area-range setting
show ospf global setting	Show OSPF global setting
show ospf interface setting	Show OSPF interface setting
show ospf neighbor	Show OSPF neighbor table
show ospf route	Show OSPF routing table
show ospf setting	Show OSPF settings
show ospf virtual-link setting	Show OSPF virtual link settings
ospf enable	Enable OSPF feature
no ospf enable	Disable OSPF feature
ospf router-id [ip address]	Configure OSPF Router ID. - Option "router-id [ip address]" specifies OSPF router-id in IP address format.
ospf area [ip address/Prefix] [normal/nssa/stub] [metric <0-16777215>]	Configure OSPF area setting as normal/nssa/stub area type. - Option "area [IP address/Prefix]" sets OSPF Area ID which is in a form of IP address. - Option "[normal/nssa/stub]" sets OSPF Area Type which can be selected from Stub Area, NSSA (Not-So-Stubby-Area), and Normal option. - Option "[metric <0-16777215>]" specifies routing metric which can set the value between 0 and 16777215. Note that metric can only be set to 0 under the "Normal" Area Type.
ospf area [ip address] range [IP address/Prefix]	Configure OSPF area setting as range. - Option "[ip address]" specifies OSPF Area ID. - Option "[IP address/Prefix]" specifies the range in IP address and subnet prefix range between 4~30.

ospf area [ip address] virtual-link [ID]	Configure OSPF area setting as virtual-link - Option “[ip address]” specifies OSPF Area ID. - Option “[ID]” specifies OSPF Virtual Link in which ID is the Router ID of the remote ABR.
ospf distribution connected enable	Enable OSPF distribution as connected
no ospf distribution connected enable	Disable OSPF distribution as connected
ospf distribution rip enable	Enable OSPF distribution as rip
no ospf distribution rip enable	Disable OSPF distribution as rip
ospf distribution static enable	Enable OSPF distribution as static
no ospf distribution static enable	Disable OSPF distribution as static
ospf interface [vlan ID<1-4094>] area [OSPF area]	Configure OSPF interface setting. - Option “[vlan ID <1-4094>]]” specifies OSPF Area ID. - Option “[OSPF area]” specifies OSPF area in IP address format.
ospf interface [vlan ID<1-4094>] auth-type [md5/none/simple]	Configure OSPF interface authentication type setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[md5/none/simple]” sets authentication type for the interface which can be None, Simple, or MD5. Note that MD5 is more secure and recommended.
ospf interface [vlan ID<1-4094>] auth-key [keystring]	Configure OSPF interface authentication key setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[md5/none/simple]” sets authentication key or password for OSPF interface according to the authentication type. Note that for simple Auth. Type the key can be 1 to 8 characters. For MD5 Auth. Type the key can be 1 to 16 characters.
ospf interface [vlan ID<1-4094>] dead-interval [interval <1-65535>]	Configure OSPF interface Dead Interval setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[interval <1-65535>]” sets dead interval in second which can have a value between 1 to 65535.
ospf interface [vlan ID<1-4094>] hello-interval [interval <1-65535>]	Configure OSPF interface Hello Interval setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID.

	- Option “[interval <1-65535>]” sets hello interval in second which can have a value between 1 to 65535.
ospf interface [vlan ID<1-4094>] interface-metric [<1-65535>]	Configure OSPF interface Metric setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[<1-65535>]” sets metric or cost of the OSPF interface which can have a value between 1 to 65535.
ospf interface [vlan ID<1-4094>] md5-key-id [<1-255>]	Configure OSPF interface MD5-Key-ID setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[<1-255>]” sets MD5 key ID that can be value between 1 to 255.
ospf interface [vlan ID<1-4094>] router-priority [<0-255>]	Configure OSPF interface Router Priority setting. - Option “[vlan ID <1-4094>]” specfies OSPF interface with VLAN ID. - Option “[<1-255>]” sets Router Priority which can be value between 1 to 255. Note that if router priority is set to 0, it is a non-designated router (NDR). That is this interface will not be elected as Designated Router (DR) or Backup Designated Router (BDR).

1.4.53 PASSWORD

This section shows how users can configure GUI login username/password setting using “password manager” command as shown in Table 1.54.

Table 1.54 Descriptions of Commands for GUI login setting

Command	Description
password manager [username] [password]	Configure Web GUI login username and password. - Option “[username]” is a string with length between 0 and 16 characters. - Option “[password]” is a string with length between 5 and 9 characters.

1.4.54 PORT

Atop’s industrial managed switch provides full control on all of its network interfaces. In this section, the users can enable or disable each port and set preferred physical layer mode such as copper or fiber. Moreover, the users will be able to configure negotiation mechanism, data rate (speed), duplexing, flow control, and rate control for each port. All port’s status and statistics can also be viewed. Using “port” command and its options as listed in Table 1.55, users can configure managed switch’s port settings.

Table 1.55 Descriptions of Commands for Port Setting

Command	Description
show port status [port list]	Show switch's specified port(s) status. - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
show port statistics [port list]	Show switch's specified port(s) statistics. - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
show port gmrp [port list]	Show switch's specified port(s) gmrp status. - Option "[port list]" specifies the list of port(s) or trunk list, e.g. 3, 6-8, Trk2.
show port gvrp [port list]	Show switch's specified port(s) gvrp status. - Option "[port list]" specifies the list of port(s) or trunk list, e.g. 3, 6-8, Trk2.
port flow [on/off] [port-list]	Enable/Disable switch's specified port(s) port flow. - Option "[on/off]" is used to enable or disable the flow on specified port(s). - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
port nego [auto/force] [port-list]	Configure switch's specified port(s) negotiation type. - Option "[auto/force]" is used to configure negotioation on specified port(s). - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
port rate [egress/ingress] [rate <0-10000000>] [port-list]	Configure switch's specified port(s) rate control settings. - Option "[egress/ingress]" is used to configure rate control on specified port(s). - Option "[rate <0-10000000>]" sets the data rate on specified port(s). - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
port state [on/off] [port-list]	Configure switch's specified port(s) state. - Option "[on/off]" sets the state of specified port(s) to either on or off. - Option "[port list]" specifies the list of ports separated by ","s or "-"s.
port speed [10/100/1000/10000] [duplex <full/half>] [port-list]	Configure switch's specified port(s) speed settings. - Option "[10/100/1000/10000]" sets the speed of specified port(s).

Command	Description
	- Option “[dulex <full/half>]” sets the duplex of specified port(s) to either full dulex or half duplex. - Option “[port list]” specifies the list of ports separated by ","s or "-"s.
port gmrp [port-list]	Configure switch’s specified port(s) gmrp settings. - Option “[port list]” specifies the list of port(s) or trunk list, e.g. 3, 6-8, Trk2.
port gvrp [port-list]	Configure switch’s specified port(s) gmrp settings. - Option “[port list]” specifies the list of port(s) or trunk list, e.g. 3, 6-8, Trk2.

1.4.55 PING

Atop’s managed switch provides a network tool called Ping for testing network connectivity in this subsection. Ping is a network diagnostic utility for testing reachability between a destination device and the managed switch. Note that this utility is only for IPv4 address. Users can use “ping” command and its options as shown in

Table 1.56.

Table 1.56 Descriptions of Commands for IPv4 Ping

Command	Description
ping [hostname or ip address] [times <1-999>]	User can use this command to execute ping ipv4. - Option “[hostname or ip address]” specifies the destination hostname or IP address to be checked for reachability, - Option “[times <1-999>]” specifies the number of repetitions for sending ping message. Default value is 4 times.

1.4.56 PING6

Ping6 is a corresponding network diagnostic utility for testing reachability between a destination device and the managed switch in IPv6 network. Users can use “ping6” command and its options as shown in Table 1.57.

Table 1.57 Descriptions of Commands for IPv6 Ping

Command	Description
ping6 [hostname or ip address] [times <1-999>]	User can through this command to execute ping IPv6.

	- Option “[hostname or ip address]” specifies the destination hostname or IP address to be checked for reachability, - Option “[times <1-999>]” specifies the number of repetitions for sending ping message. Default value is 4 times.

1.4.57 PTP

The Precision Time Protocol (PTP) is a high-precision time protocol. It can be used with measurement and control systems in local area network that require precise time synchronization. The PTP can be configured using “ptp” command and its options as listed in Table 1.58.

Table 1.58 Descriptions of Commands for PTP Setting

Command	Description
show ptp hw	Show status of H/W PTP.
show ptp port	Show the PTP’s status of all ports
ptp enable	Enable PTP feature
no ptp enable	Disable PTP feature
ptp announce [interval <1-1024>]	Configure the announce interval of PTP - Option “[interval <1-1024>]” specifies the announce interval. Note: The value shall be the logarithm to the base 2 of the mean AnnounceInterval. Ex: {1, 2, 4, 8, ..., 1024}
ptp clock_mode [e2e/e2e-tc/p2p/p2p-tc]	Configure the clock mode of PTP. - Option “[e2e/e2e-tc/p2p/p2p-tc]” specifies the clock mode which can be End-End Boundary Clock (e2e), End-End Transparent Clock (e2e-tc), Peer-Peer Boundary Clock (p2p), and Peer-Peer Transparent Clock (p2p-tc).
ptp clock_class [<0-255>]	Configure the clock class value of PTP. - Option “[<0-255>]” specifies the PTP’s clock class. Note that Clock Class represents clock’s accuracy level. It is an attribute of an ordinary or boundary clock. It denotes time traceability or frequency distributed by the grandmaster clock.
ptp domain [<0-255>]	Configure the domain value of PTP. - Option “[<0-255>]” specifies domain of PTP.
ptp port enabled [port-list]	Enable PTP feature on switch’s specified port(s).

Command	Description
	- Option “[port-list]” sets PTP feature on the specified port(s) in the port list. Note that ports in the port list can be separated by ","s or "-"s.
ptp port disabled [port-list]	Disable PTP feature on switch’s specified port(s). - Option “[port-list]” disables PTP feature on the specified port(s) in the port list. Note that ports in the port list can be separated by ","s or "-"s.
ptp priority1 [<0-255>]	Configure the priority1 value of PTP. - Option “[<0-255>]” sets clock priority 1 of PTP version 2. The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority.
ptp priority2 [<0-255>]	Configure the priority2 value of PTP. - Option “[<0-255>]” sets clock priority 2 of PTP version 2. The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority.
ptp sync [interval <1-1024>]	Configure the sync interval of PTP. - Option “[interval <1-1024>]” sets the the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network. Note: The value shall be the logarithm to the base 2 of the mean AnnounceInterval. Ex: {1, 2, 4, 8, ..., 1024}
ptp stratum [<0-4>]	Configure the stratum value of PTP. - Option “[<0-4>]” sets the stratum of the clock. The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA).
ptp transport [ethernet/ipv4]	Configure the transport type of PTP. - Option “[ethernet/ipv4]” selects Ethernet (layer 2) multicast transport or layer 3 (UDP/IPv4) multicast transports for PTP (Precision Time Protocol) messages.
ptp utc_offset [<0-32767>]	Configure the UTC Offset value of PTP.

Command	Description
	- Option “[<0-32767>]” sets the Coordinated Universal Time (UTC) offset value.
ptp version [number <1/2>]	Configure the version of PTP. - Option “[number <1/2>]” sets the PTP version number.

1.4.58 POE

Power over Ethernet (PoE) is an optional function for the managed switches which enables the switch to provide power supply to end devices called Powered Device (PD) connected on the other side of the Ethernet ports. This means that the electrical power is delivered along with data over the Ethernet cables. This will be useful for the end devices that are located in the area that has no power supply and the users can save additional wiring for the end devices. To find out whether this function is supported or not by your managed switch, please look for the keyword “PoE” in Atop’s model name. If the switch has “PoE” in its model name, it means that the switch is a Power Sourcing Equipment (PSE) that can provide power output to a Powered Device (PD). Users can configure PoE feature por port(s) on the device using “poe” command and its options as listed in Table 1.59.

Table 1.59 Descriptions of Commands for PoE Setting

Command	Description
show poe status [port-list]	Show PoE status of switch’s specified port(s). - Option “status [port-list]” specifies the port(s) in the list to be shown of their status. Note that port numbers in the port list are separated by ","s or "-"s.
show poe alarm status	Show the PoE’s alarm settings
poe enable	Enable PoE feature
poe disable	Disable PoE feature
poe alarm detect-power enable	Enable PoE’s alarm feature that detect total power exceeding a threshold.
poe alarm detect-power disable	Disable PoE’s alarm feature that detect total power exceeding a threshold.
poe alarm detect-power [<0-9999>]	Configure PoE Detect Total Power alarm limit - Option “[<0-9999>]” set the total power value in Watts which will trigger alarm event. Note that the value ‘0’ means that the alarm event will not trigger.
poe alarm detect-power email-warning enable	Enable PoE’s alarm feature that detects total power exceeding a threshold and sends warning email.
poe alarm detect-power email-warning disable	Disable PoE’s alarm feature that detects total power exceeding a threshold and sends warning e-mail.

poe alarm detect-power led-warning enable	Enable PoE's alarm feature that detects total power exceeding a threshold and turns on warning LED.
poe alarm detect-power led-warning disable	Disable PoE's alarm feature that detects total power exceeding a threshold and turns on warning LED.
poe alarm detect-power relay-warning enable	Enable PoE's alarm feature that detects total power exceeding a threshold and switches on warning relay.
poe alarm detect-power relay-warning disable	Disable PoE's alarm feature that detects total power exceeding a threshold and switches on warning relay.
poe alarm pd-power-on enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on.
poe alarm pd-power-on disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on.
poe alarm pd-power-on email-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and sends warning e-mail.
poe alarm pd-power-on email-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and sends warning e-mail.
poe alarm pd-power-on led-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and turns on warning LED.
poe alarm pd-power-on led-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and turns on warning LED.
poe alarm pd-power-on relay-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and switches on warning relay.
poe alarm pd-power-on relay-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power on and switches on warning relay.
poe alarm pd-power-off enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off.
poe alarm pd-power-off disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off.
poe alarm pd-power-off email-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and sents warning e-mail.
poe alarm pd-power-off email-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and sents warning e-mail.

poe alarm pd-power-off led-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and turns on warning LED.
poe alarm pd-power-off led-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and turns on warning LED.
poe alarm pd-power-off relay-warning enable	Enable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and switches on warning relay.
poe alarm pd-power-off relay-warning disable	Disable PoE's alarm feature that generates alarm when PoE PD (Powered Device) is power off and switches on warning relay.

1.4.59 QINQ

Originally, the 802.1Q standard VLAN only allowed one VLAN tag appended in a packet. But the QinQ feature in EHG7XXX allows two VLAN tags to be appended in a packet. The main purpose of the QinQ is for service providers to place additional VLAN tag as an external network identification and to keep the original customer's VLAN tag if existed. Users can configure VLAN QinQ feature using "qinq" command and its options as shown in Table 1.60.

Table 1.60 Descriptions of Commands for QinQ Setting

Command	Description
show qinq	Show the QinQ setting and information
qinq enable [port-list]	Enable VLAN QinQ feature. - Option "[port-list]" specifies which port(s) in the list or trunk list, e.g. 3, 6-8, Trk2, to enable QinQ feature.
no qinq enable [port-list]	Disable VLAN QinQ feature. - Option "[port-list]" specifies which port(s) in the list or trunk list, e.g. 3, 6-8, Trk2, to disable QinQ feature.
qinq tpid [TPID Value]	Configure VLAN QinQ Tpid feature. - Option "[TPID value]" specifies tag protocol identifier (TPID) value.

1.4.60 QoS

Quality of Service (QoS) is the ability to provide different priority to different applications, users, or data flows. QoS guarantees a certain level of performance to a data flow by using the following metrics: transmitted bit rate, bit error rate, delay, jitter, and probability of packet dropping. QoS guarantees are important if the network capacity is insufficient, especially for application that requires certain bit rate and is delay sensitive. For any network that is best effort, QoS cannot be guaranteed, except that resource is more than sufficient to serve users.

Controlling network traffic needs a set of rules to help classify different types of traffic and define how each of them should be treated as they are being transmitted. This managed switch can inspect both 802.1p Class of Service (CoS) tags and DiffServ tags called Differentiated Services Code Point (DSCP) to provide consistent classification. To configure QoS settings on the managed switch, users can use “qos” command and its options listed in Table 1.61.

Table 1.61 Descriptions of Commands for QoS Setting

Command	Description
show qos type	Show switch’s QoS type setting.
show qos [port-list]	Show switch’s QoS setting by port. - Option “[port-list]” specifies the port(s) in the list which are separated by ","s or "-"s.
qos type [cos-only/cos-and-diffserv]	Configure QoS type as “802.1p CoS” or “Both 802.1p CoS and DiffServ”. - Option “[cos-only/cost-and-diffserv]” is used to select QoS type.
qos priority strict	Configure QoS type as “Strict Priority” mode
qos priority drr [Queue 0 weight<0-2032>] [Queue 1 weight<0-2032>] [Queue 2 weight<0-2032>] [Queue 3 weight<0-2032>] [Queue 4 weight<0-2032>] [Queue 5 weight<0-2032>] [Queue 6 weight<0-2032>] [Queue 7 weight<0-2032>]	Configure QoS type as “Deficit Round Robin” mode and set weight in kbytes value for Queue 0~7. - Option [Queue 0 weight <0-2032>] sets weight in kbytes for Queue 0. - Option [Queue 1 weight <0-2032>] sets weight in kbytes for Queue 1. - Option [Queue 2 weight <0-2032>] sets weight in kbytes for Queue 2. - Option [Queue 3 weight <0-2032>] sets weight in kbytes for Queue 3. - Option [Queue 4 weight <0-2032>] sets weight in kbytes for Queue 4. - Option [Queue 5 weight <0-2032>] sets weight in kbytes for Queue 5. - Option [Queue 6 weight <0-2032>] sets weight in kbytes for Queue 6. - Option [Queue 7 weight <0-2032>] sets weight in kbytes for Queue 7.
qos priority wrr [Queue 0 weight<0-127>] [Queue 1 weight<0-127>] [Queue 2 weight<0-127>] [Queue 3 weight<0-127>] [Queue 4 weight<0-127>] [Queue 5 weight<0-127>] [Queue 6 weight<0-127>] [Queue 7 weight<0-127>]	Configure QoS type as “Weighted Round Robin” mode and set weight in kbytes value for Queue 0~7. - Option [Queue 0 weight <0-127>] sets weight in packets for Queue 0. - Option [Queue 1 weight <0-127>] sets weight in packets for Queue 1. - Option [Queue 2 weight <0-127>] sets weight in packets for Queue 2.

Command	Description
	- Option [Queue 3 weight <0-127>] sets weight in packets for Queue 3. - Option [Queue 4 weight <0-127>] sets weight in packets for Queue 4. - Option [Queue 5 weight <0-127>] sets weight in packets for Queue 5. - Option [Queue 6 weight <0-127>] sets weight in packets for Queue 6. - Option [Queue 7 weight <0-127>] sets weight in packets for Queue 7.

1.4.61 RADIUS-SERVER

RADIUS: The RADIUS is a networking protocol that provides authentication, authorization and accounting (AAA) management for devices to connect and use a network service. Users can configure RADIUS server settings using “radius-server” command and its options as shown in Table 1.62.

Table 1.62 Descriptions of Commands for Radius Server

Command	Description
show radius-server	Show Radius Server settings similar to 802.1X Setting webpage in WebUI.
radius-server host [radius server IP address] [server port <1024-65535>] [accounting port number <1024-65535>]	Configure Radius Server host and port setting. - Option “[radius server IP address]” sets RADIUS server IP address. - Option [server port <1024-65535>] sets RADIUS server’s port number. The range is 1024 ~ 65535. - Option [accounting port number <1024-65535>] sets the accounting port number of the RADIUS server. The range is 1024 ~ 65535.
radius-server key [shared_key]	Configure Radius Server shared key setting. - Option “[shared_key]” sets the shared key or RADIUS Server. It is a shared key between the managed switch and the RADIUS Server. Both ends must be configured to use the same key. Maximum length of 30 characters.
radius-server nas [NAS_ID]	Configure Radius Server NAS identifier setting. - Option “[NAS_ID]” specifies the identifier string for 802.1X Network Access Server (NAS). Maximum length of 30 characters.

1.4.62 RIP

The Industrial L3 managed switch implements a dynamic routing protocol to allow automatically learning and updating of routing table. Dynamic routing protocol can be setup by the users. Routing Information Protocol (RIP) is a distance vector-based routing protocol that can make decision on which interface the L3 managed switch should forward Internet Protocol (IP) packet and can share information about how to route traffic among network devices that use the same routing protocol. RIP sends routing-update messages periodically and when there is a change in network topology. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. RIP can also be used to automatically build up a routing table. To configure RIP on the managed switch using CLI, users can use “rip” command and its options as listed in Table 1.63.

Table 1.63 Descriptions of Commands for RIP Setting

Command	Description
show rip route	Show RIP routing table (Note that the users need to enable ip-routing as shown in Section 1.4.42 first.)
show rip setting	Show RIP settings (Note that the users need to enable ip-routing as shown in Section 1.4.42 first.)
rip enable	Enable RIP feature
no rip enable	Disable RIP feature
rip version [v1/v2]	Configure RIP version. - Option “[v1/v2]” sets the version of RIP.
rip distribution connected enable	Enable RIP’s distribution connected route option. Note that the Distribution option is to set which routing information the RIP will be used to populate its routing table. When the Connected option is selected, the RIP will add the connected routes (subnets directly connected to the EHG7XXX’s interface) to its routing table.
no rip distribution connected enable	Disable RIP’s distribution connected route option.
rip distribution ospf enable	Enable RIP’s distribution with OSPF option.
no rip distribution ospf enable	Disable RIP’s distribution with OSPF option
rip distribution static enable	Enable RIP’s distribution with static route option. Note that when the Static route option is selected, the RIP will add the static routes to its routing table.
no rip distribution static enable	Disable RIP’s distribution with static route option.

1.4.63 STORM-CONTROL

Storm control or storm filter features is available in the managed switch. Storm control prevents traffic on a LAN from being disrupted by ingress traffic of broadcast, multicast, and destination lookup failure (DLF) on a port. Users can set the strom control feature using “strom-control” command as shown in Table 1.64.

Table 1.64 Descriptions of Commands for Storm-Control Setting

Command	Description
show storm-control	Show Storm Control setting
storm-control [broadcast limiting] [multicast limiting] [DLF limiting] [port-list]	Configure storm-control setting per port. - Option “[broadcast limiting]” specifies the type of strom packets to be limited or controlled to be broadcast packets. - Option “[multicast limiting]” specifies the type of strom packets to be limited or controlled to be multicast packets. - Option “[DLF limiting]” specifies the type of strom packets to be limited or controlled to be DLF (Destination Lookup Failure) packets. - Option “[port-list]” specifies port(s) in the list of ports which are separated by ","s or "-"s.

1.4.64 SECURITY

Port Security or static port security feature allows the users to control security on each port of the managed switch and create a table of MAC addresses allowed to access the switch. Users can configure port security using “security” command and its options as listed in Table 1.65.

Table 1.65 Descriptions of Commands for Port Security Setting

Command	Description
security port [port-list]	Enable security port setting per port. - Option “[port-list]” specifies the ports in the port list which are separated by ","s or "-"s.
no security port [port-list]	Disable security port setting per port. - Option “[port-list]” specifies the ports in the port list which are separated by ","s or "-"s.
security static [MAC address] [VLAN ID] [port number]	Configure White-List MAC address rule per VLAN and port number. - Option “[MAC address]” specifies the static MAC address to be added in the

Command	Description
	the white-list that will be allowed to access the managed switch. - Option "[VLAN ID]" specifies the VLAN ID. - Option "[port number]" specifies the port number.
no security static [MAC address] [VLAN ID]	Remove White-List MAC address rule per VLAN. - Option "[MAC address]" specifies the static MAC address to be added in the the white-list that will be allowed to access the managed switch. - Option "[VLAN ID]" specifies the VLAN ID.

1.4.65 SNTP

For automatically date and time setting, the users can enable Simple Network Time Protocol (SNTP) and configure SNTP using "sntp" command and its options as listed in Table 1.66.

Table 1.66 Descriptions of Commands for SNTP Setting

Command	Description
show sntp	Show DUT's SNTP setting
show sntp timezone	Show timezone list
sntp enable	Enable SNTP feature
no sntp enable	Disable SNTP feature
sntp queryperiod [seconds]	Configure SNTP Query Period (in seconds) setting. - Option "[seconds]" specifies the query period of SNTP. This parameter determines how frequently the time is updated from the NTP server. If the end devices require less accuracy, longer query time is more suitable since it will cause less load to the switch. The setting value can be in between 60 – 259200 (72 hours) seconds.
sntp server1 [NTP Server domain/ip]	Configure SNTP Server-1 setting. - Option "[NTP Server domain/ip]" specifies the domain address or IP address of the NTP server.
sntp server2 [NTP Server domain/ip]	Configure SNTP Server-2 setting, - Option "[NTP Server domain/ip]" specifies the domain address or IP address of the NTP server.
sntp timezone [timezone<0-62>]	Configure SNTP time zone area.

Command	Description
	- Option “[timezone<0-62>]” specifies the time zone or user’s current local time. Default time zone is 49.

1.4.66 SYS-TIME

Atop’s industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Users can configure the system time using “sys-time” command and its options as shown in Table 1.67.

Table 1.67 Descriptions of Commands for System Time Setting

Command	Description
show sys-time	Show the currently system time of DUT
sys-time [years] [months] [days] [hours] [minutes] [seconds]	Configure the system time of DUT. - Option “[years]” sets current year. - Option “[months]” sets current month. - Option “[days]” sets current day. - Option “[hours]” sets current hour. - Option “[minutes]” sets current minute. - Option “[seconds]” set current second.

1.4.67 SYSLOG

System Log keeps track of related settings configuration of the device. The actual recorded log event will be shown in Event Log. The users can enable how the log will be saved and/or delivered to other system. The log can be saved to flash memory inside the managed switch and/or it can be sent to a remote log server. The users need to select the log level and provide the IP address of a remote log server and the service log service port. Table 1.68 lists all commands related to SYSLOG that enable users to configure system log.

Table 1.68 Descriptions of Commands for system log setting

Command	Description
show syslog	Show syslog setting and status
syslog log-to-flash	Enable logging events to the flash
no syslog log-to-flash	Disable logging events to the flash
syslog level [level value <0-7>]	Configure log level of system log. - Option “[level value <0-7>]” specifies the log level.
syslog server-enable	Enable logging events to a syslog server
no syslog server-enable	Disable logging events to a syslog server
syslog server-ip [server ip address]	Configure syslog server IP address. - Option “[server ip address]” specifies the log server’s IP address.
syslog server-ip [server ip address] port [port number]	Configure syslog server using port.

Command	Description
	- Option “[server ip address]” specifies the log server’s IP address. - Option “[port number]” specifies port number of the log server.

1.4.68 SMTP

Simple Mail Transfer Protocol (SMTP) is an internet standard for email transmission across IP networks. If there is any warning events, the managed switch can send an alarm message to users by e-mail. The users are allowed to modify E-mail-related settings for sending the system alarms (Link Status, Power Status, and System Log). Users can use “smtp” command and its options listed in Table 1.69 to configure SMTP settings.

Table 1.69 Descriptions of Commands for SMTP Setting

Command	Description
show smtp	Show SMTP settings of DUT
smtp auth [username] [password]	Configure the username/password for accessing SMTP server. - Option “[username]” specifies the username of the SMTP server. - Option “[password]” specifies the password of the SMTP server.
smtp recipient1 [email address]	Configure the 1st recipient E-mail address. - Option “[email address]” specifies e-mail address of the 1st recipient.
smtp recipient2 [email address]	Configure the 2nd recipient E-mail address. - Option “[email address]” specifies e-mail address of the 2nd recipient.
smtp recipient3 [email address]	Configure the 3rd recipient E-mail address. - Option “[email address]” specifies e-mail address of the 3rd recipient.
smtp recipient4 [email address]	Configure the 4th recipient E-mail address. - Option “[email address]” specifies e-mail address of the 4th recipient.
smtp server [server domain/ip address]	Configure the SMTP Server Domain or IP Address. - Option “[server domain/ip address]” specifies the domain name or IP address of the SMTP server.
smtp sender [email address]	Configure the sender E-mail address. - Option “[email address]” specifies e-mail address of the sender.
mtp subject [email subject]	Configure the E-mail subject.

Command	Description
	- Option "[email subject]" specifies e-mail's subject in string with maximum length of 32 characters.
smtp tls	Enable SMTP TLS (Transport Layer Security) setting
no smtp tls	Disable SMTP TLS (Transport Layer Security) setting

1.4.69 SNMP

Simple Network Management Protocol (SNMP) is a protocol for managing devices on IP networks. It exposes management data in the form of variables on the managed systems which describe the system configuration. These variables can then be queried or defined by the users. The SNMP is used by network management system or third-party software to monitor devices such as managed switches in a network to retrieve network status information and to configure network parameters. The Atop's managed switch supports SNMP and can be configured using "snmp" command and its options as listed in Table 1.70.

Table 1.70 Descriptions of Commands for SNMP Setting

Command	Description
show snmp status	Show the SNMP status
show snmp community	Show SNMP user community name and permission
show snmp trap	Show all trap sinks
show snmp usm-user	Show SNMPv3 USM users
snmp enable	Enable SNMP feature
no snmp enable	Disable SNMP feature
snmp community [read-all-only/ read-write-all] [username]	Configure the SNMP community string. - Option "[read-all-only/read-write-all]" specifies the permission type. - Option "[username]" specifies the username or community string of SNMP with maximum length of 16 characters.
no snmp community [username]	Delete SNMP community string rule. - Option "[username]" specifies the community string (username) to be deleted.
snmp trap [ip address] [community string] [port number]	Configure SNMP Trap setting. - Option "[ip address]" specifies the destination IP Address of the Trap server. - Option "[community string]" specifies the community string for authentication. - Option "[port number]" specifies the port number of the Trap server.
snmp trap-mode [inform/trap]	Configure SNMP Trap mode.

Command	Description
	- Option “[inform/trap]” selects the mode of trap either inform or trap.
no snmp trap [ip address] [port number]	Delete SNMP Trap server rule. - Option “[ip address]” specifies the destination IP Address of the Trap server. - Option “[port number]” specifies the port number of the Trap server.
snmp usm-user [admin/user] authnopriv md5 [password]	Configure SNMPv3 authentication setting for Security level AuthNoPriv (need PASSWORD). - Option “[admin/user]” specifies the security level as either admin or user. - Option “[password]” specifies the password for authentication.
snmp usm-user [admin/user] authpriv md5 [password] des [key]	Configure SNMPv3 authentication setting for Security level AuthPriv (need both PASSWORD and encryption KEY). - Option “[admin/user]” specifies the security level as either admin or user. - Option “[password]” specifies the password for authentication - Option “[key]” specifies the DES encryption key.
snmp usm-user [admin/user] noauthpriv	Configure SNMPv3 authentication setting for Security level NoAuthPriv (do not need PASSWORD and encryption KEY). - Option “[admin/user]” specifies the security level as either admin or user.
no snmp usm-user [admin/user]	Delete SNMPv3 authentication setting rule. - Option “[admin/user]” specifies the security level as either admin or user to be deleted.

1.4.70 SSH

The users have option to remotely connect to the managed switch using secure shell (SSH) through any of its port. This section shows how users can configure SSH setting using “ssh” command and its options in Table 1.72.

Table 1.71 Descriptions of Commands for SSH setting

Command	Description
ssh enable	Enable SSH of DUT
no ssh enable	Disable SSH of DUT
ssh key force	Generates new SSH server key and force to replace an existing key.

1.4.71 SPANNING-TREE

IEEE 802.1D Standard spanning tree functionality is supported by Atop's managed switches. The Spanning Tree Protocol (STP) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, Atop's managed switches deploy spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network. Using "spanning-tree" command and its options listed in Table 1.72, user can check the current configuration of spanning tree and make any changes to it.

Table 1.72 Descriptions of Commands for Setting up Spanning Tree

Command	Description
spanning-tree enable	Enable spanning-tree
no spanning-tree enable	Disable spanning-tree
spanning-tree bpdu-guard enable	Enable spanning-tree BPDU (Bridge Protocol Data Unit) Guard
no spanning-tree bpdu-guard enable	Disable spanning-tree BPDU (Bridge Protocol Data Unit) Guard
spanning-tree forward-delay [<4~30>]	Set the amount of forward delay in seconds. Example: spanning-tree forward-delay 20: Set forward delay time to 20 seconds. - Option "[<4-30>]" specifies the forward delay.
spanning-tree hello-time [<1~10>]	Set hello time in seconds. - Option "[<1-10>]" specifies the hello time.
spanning-tree maximum-age [<6~40>]	Set the maximum age of the spanning tree in seconds. - Option "[<6-40>]" specifies the maximum age.
spanning-tree priority [<0~61440>]	Set priority of the spanning tree bridge. - Option "[<0-61440>]" specifies the prority of the spanning tree bridge.
spanning-tree protocol-version [<mstp/rstp/stp>]	Choose protocol version. - Option "[<mstp/rstp/stp>]" specifies the version of spanning tree to be used which can be MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree

Command	Description
	Protocol) or STP (Spanning Tree Protocol).
[no] spanning-tree port edge-port [<port-list>]	Set the port to be edge connection. - Option "[<port-list>]" specifies port number to be set as edge port. - Option "[no]" indicates the removal of the specified port.
[no] spanning-tree port enable-stp [<port-list >]	Enable/Disable spanning-tree for a specific port. - Option "[<port-list>]" specifies port number to be enable for STP. - Option "[no]" indicates the removal or disabling of the specified port.
[no] spanning-tree port enable-bpdu-guard [<port-list>]	Enable/Disable spanning-tree for a specific port. - Option "[<port-list>]" specifies port number to be enable with BDPU-guard. - Option "[no]" indicates the removal or disabling of the specified port.
[no] spanning-tree port non-stp [<port-list>]	Enable or disable spanning tree protocol on this port. - Option "[<port-list>]" specifies port number to be enable with non-stp. - Option "[no]" indicates the removal or disabling of the specified port.
spanning-tree port path-cost [<0 ~ 2E8>] [<port-list>]	Set path cost for a specific port. - Option "[<0-2E8>]" specifies the path's cost. - Option "[<port-list>]" specifies port number.
spanning-tree port priority [<0 ~ 240>] [<port-list>]	Set priority to a specific port. - Option "[<0-240>]" specifies the port's priority. - Option "[<port-list>]" specifies port number.
[no] spanning-tree port point-to-point-mac [<auto | true | false>] [<port-list>]	Set the port to be point to point connection. - Option "[<auto|true|false>]" set the state of point-to-point connection. Auto: Specify point to point link auto detection. True: Set the point-to-point link to true. False: Set the point-to-point link to false. - Option "[<port-list>]" specifies port number. - Option "[no]" indicates the removal or disabling of the specified port.
show spanning-tree	Show spanning-tree information
show spanning-tree port [<port-list>]	Show port information

Command	Description
	- Option “[<port-list>]” specifies the port number to be shown.

1.4.72 STATIC-ROUTING

Static routing is a form of routing based on IP address at OSI Layer 3 that occurs when a router uses a manually configured routing entry to forward packet. The users can define the routes by themselves by specifying what is the next hop (or the next router) based on IP address that the Layer 3 switch will forward data packet for a specific subnet. Note that to allow IPv4 Static Routing to operate properly, please enable the IP Routing function as described in Section 1.4.42 first. To configure static routing, users can use “static-routing” command and its options shown in Table 1.73.

Table 1.73 Descriptions of Commands for Static-Routing

Command	Description
show static-routing	Show Static Routing settings
static-routing add [name] [destination ip address] [subnet mask] [gateway ip address] [metric<0-65535>]	Add Static Routing entries. - Option “[name]” specifies added static routing entry’s name. - Option “[destination ip address]” specifies destination IP address of the static routing entry. - Option “[subnet mask]” specifies subnet mask of the static routing entry. - Option “[gateway ip address]” specifies gateway IP address of the static routing entry. - Option “[metric <0-65535>]” specifies route metric of the static routing entry.
no static-routing [name]	Delete Static Routing entry. - Option “[name]” specifies the entry’s name to be removed.

1.4.73 SFLOW

sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector., users can use “static-routing” command and its options shown in Table 1.73.

Table 1.74 Descriptions of Commands for sFlow

Command	Description
show sflow setting	Show sFlow settings

Command	Description
sflow enable	Enable sflow feature
sflow receiver_set [ip address][UDP port<1-65535>][size<200-1468>]	Configure sFlow receiver setting - Option "[ip address]" specifies IP address of sFlow receiver. - Option "[UDP port<1-65535>]" specifies UDP port number of sFlow receiver. - Option "[size<200-1468>]" specifies maximum number of data bytes that can be sent in a single sample datagram
sflow port counter_enable [port list]	Enable the status of counter polling on specific port(s). - Option "[port list]" specifies the port belongs to sflow port such as 3, 6-8
sflow port sampler_enable [port list]	Enable the status of flow sampling on specific port(s). - Option "[port list]" specifies the port belongs to sflow port such as 3, 6-8
sflow port setting [port list][interval<0-3600>][rate<0-4096>][header<14-200>]	Configure sflow port setting. (Max header, Sampleing rate, Counter Interval) - Option "[port list]" specifies the port belongs to sflow port such as 3, 6-8 - Option "[interval<0-3600>]" specifies the counter interval - Option "[rate<0-4096>]" specifies the sampler N packets of 1 - Option "[header<14-200>]" specifies the Max. Header of sampler (default:128)
no sflow enable	Disable sflow feature

1.4.74 TIMEOUT

This section shows how users can configure CLI's timeout setting using "timeout" command as shown in Table 1.76.

Table 1.75 Descriptions of Commands for CLI's timeout setting

Command	Description
show timeout	Show CLI's timeout setting
timeout [interval <30-3600>]	Configure CLI timeout in seconds - Option "[interval <30-3600>]" specifies the timeout duration in seconds.

1.4.75 TEMPERATURE

The managed switch keeps records of user and system temperature logs. There are summary statistics and distribution of temperature information for each log. The highest temperature, the lowest temperature and the average temperature are reported in degree Celsius. Additionally,

there is a recorded time which shows the time since the temperature log were recorded. Users can display either system temperature logs or user temperature logs and can reset the user log using the commands listed in Table 1.76.

Table 1.76 Descriptions of Commands for temperature information

Command	Description
show temperature system-log	Show system temperature log of DUT
show temperature user-log	Show user temperature log of DUT
temperature reset user-log	Reset user temperature log of DUT

1.4.76 TRUNK

The managed switch supports Link Trunking, which allows one or more links to be combined together as a group of links to form a single logical link with larger capacity. The advantage of this function is that it gives the users more flexibility while setting up network connections. The bandwidth of a logical link can be doubled or tripled. In addition, if one of links in the group is disconnected, the remaining trunked ports can share the traffic within the trunk group. This function creates redundancy for the links, which also implies a higher reliability for network communication. Users can configure trunk settings using “trunk” command and its options as listed in Table 1.77.

Table 1.77 Descriptions of Commands for Trunking

Command	Description
show trunk	Show Trunking setting
trunk add [trunk group<1-8>] lacp [port-list] [LACP active port-list]	Add Trunking rule with LACP (Link Aggregation Control Protocol) enabled. - Option “[trunk group <1-8>]” specifies the trunk group number to be added. - Option “[port-list] specifies LACP ports in the port list which are separated by ","s or "-"s. - Option “[LACP active port-list]” specifies LACP active ports in the port list which are separated by ","s or "-"s.
trunk add [trunk group<1-8>] no-lacp [port-list]	Add Trunking rule without lacp enabled and use default hash type. - Option “[trunk group <1-8>]” specifies the trunk group number to be added. - Option “[port-list] specifies ports without LACP in the port list which are separated by ","s or "-"s.
trunk add [trunk group<1-8>] [lacp/no-lacp] hash [type] [port-list]	Add Trunking rule without lacp enabled and modified hash type. - Option “[trunk group <1-8>]” specifies the trunk group number to be added.

Command	Description
	- Option “[lacp/no-lacp]” specifies that the trunking does not enable LACP. - Option “[type]” specifies the hash type which can be: dst-ip, dst-mac, src-ip, src-mac, src/dst-ip, src/dst-mac. - Option “[port-list]” specifies ports in the port list which are separated by ","s or "-"s.
no trunk [trunk group<1-8>]	Delete Trunking rule - Option “[trunk group <1-8>]” specifies the trunk group number to be removed.

1.4.77 TELNET

The managed switch allows users to access it through Telnet application. Then, the users can use the CLI of Telnet to configure the managed switch. To enable or disable Telnet access, users can use “telnet” commands as shown in Table 1.78.

Table 1.78 Descriptions of Commands for telnet setting

Command	Description
telnet enable	Enable telnet of DUT
no telnet enable	Disable telnet of DUT

1.4.78 TRACEROUTE

Through the CLI, the users can issue the traceroute command which is a network diagnostic tool as shown in Table 1.79.

Table 1.79 Descriptions of Commands for Traceroute

Command	Description
traceroute [host/ip address]	Traceroute between the switch and a given Host/IP. - Option “[host/ip address]” specifies the destination host name or IP address to be traced for its route in the network.

1.4.79 UDLD

The UniDirectional Link Detection (UDLD) protocol is a protocol that can be used to prevent Layer-2 switching loops in the network. The network loop problem usually occurs in Spanning Tree network topology and when there is unidirectional link failure (miswiring or malfunction of the network interface). UDLD is a data link layer (Layer-2) protocol that keeps track of physical layer configuration (fiber or copper). It helps detect switching loops and disables one-way connections. UDLD protocol requires that two neighboring switches have to exchange UDLD packets on the corresponding ports on each switch to detect the unidirectional link. UDLD packets are transmitted periodically (hello interval) to its neighbor switches on LAN ports that

has UDLD protocol enabled. If the UDLD packets are not echoed back or no acknowledgement within a specific time, the port will be shut down and flagged as unidirectional link. Users can configure the UDLD protocol using the “udld” command and its options as listed in Table 1.80.

Table 1.80 Descriptions of Commands for UDLD Setting

Command	Description
show udld vlan [VLAN ID<1-4094>]	Show the UDLD VLAN settings. - Option “vlan [VLAN ID <1-4094>]” specifies the VLAN ID that UDLD protocol is enabled.
udld enable	Enable UDLD feature
udld disable	Disable UDLD feature
udld vlan [vlan id<1-4094>] port [port-list<e.g. 3,6-8>]	Configure UDLD VLAN based port setting - Option “[VLAN ID <1-4094>]” specifies the VLAN ID that UDLD protocol is enabled. - Option “[port-list]” specifies port number with UDLD VLAN, e.g. 3, 6-8.
udld hello-interval [interval<5-100>]	Configure UDLD Hello Interval value. - Option “[inverval <5-100>]” sets the hello interval.
no udld hello-interval	Configure UDLD Hello Interval back to default value
udld recovery-interval [interval<30-86400>]	Configure UDLD Recovery Interval value. - Option “[interval <30-86400>]” specifies the recover interval for UDLD.
no udld recovery-interval	Configure UDLD Recovery Interval back to default value
udld reset	Reset UDLD which port should be shutdown by UDLD

1.4.80 U-RING

U-Ring (Unicast Ring) is another ring protocol available in the managed switch. The U-Ring could provide redundancy connection between two EHG7XXX industrial managed switches which are not directly connected by physical wires but by two additional network devices on each switch. Users can configure U-Ring settings by using “u-ring” command and its options as listed in Table 1.81.

Table 1.81 Descriptions of Commands for U-Ring Settings

Command	Description
show u-ring	Show u-ring status and settings
u-ring enable	Enable u-ring feature
no u-ring enable	Disable u-ring feature
u-ring master	Configure DUT as ring master
no u-ring master	Disable DUT as ring master

u-ring ringport [1st ring port] [2nd ring port]	Configure u-ring 1st/2nd port setting. - Option "[1st ring port] [2nd ring port]" specifies the 1st and 2nd ring ports.
u-ring heartbeat_expire [time<100-10000>]	Configure the Heartbeat Expire Time(ms) of u-ring - Option "[time <100-10000>]" specifies heartbeat expire time in milliseconds.

1.4.81 VLAN

A Virtual Local Area Network (VLAN) is a group of devices that can be located anywhere on a network, but all devices in the group are logically connected together. In other words, VLAN allows end stations to be grouped together even if they are not located on the same network switch. With a traditional network, users usually spend a lot of time on devices relocations, but a VLAN reconfiguration can be performed entirely through software. Also, VLAN provides extra security because devices within a VLAN group can only communicate with other devices in the same group. For the same reason, VLAN can help to control network traffic. Traditional network broadcasts data to all devices, no matter whether they need it or not. By allowing a member to receive data only from other members in the same VLAN group, VLAN avoids broadcasting and increases traffic efficiency. To configure VLAN settins on the manged switch, users can use "vlan" command and its options as listed in Table 1.82.

Table 1.82 Descriptions of Commands for VLAN Settings

Command	Description
show vlan	Show Static and Dynamic VLAN Table (All VLAN entries)
show vlan [vlan id<1-4094>]	Show Static and Dynamic VLAN Table (Specified VLAN) - Option "[vlan id <1-4094>]" specifies VLAN ID to be shown.
show vlan ip address [vlan id<1-4094>]	Show IPv4 address of Specified VLAN - Option "[vlan id <1-4094>]" specifies VLAN ID to be shown.
show vlan ipv6 address [vlan id<1-4094>]	Show IPv6 address of Specified VLAN - Option "[vlan id <1-4094>]" specifies VLAN ID to be shown.
show vlan ip-subnet-based	Show the current IP Subnet Based VLAN
show vlan management	Show the current VLAN Management VLAN ID
show vlan mac-based	Show the current MAC Based VLAN
show vlan portBased	Show the current VLAN group and member
show vlan pvid [port-list]	Show the Port configured VLAN ID of Specified VLAN. - Option "[port-list]" specifies ports in the port list or trunk list such as 3, 6-8, Trk2.
show vlan protocol-based [group-table/port-table]	Show the current Protocol Based VLAN group table.

Command	Description
	- Option “[group-table/port-table]” selects either group table or port table.
show vlan static	Show static VLAN table
show vlan spanning-tree	Show per VLAN per port spanning tree information
vlan add [vlan id<1-4094>] [name] [member port list] [tagged port list]	Add or edit VLAN rule. - Option “[vlan id <1-4094>]” specifies VLAN ID to be added. - Option “[name]” specifies the VLAN’s name. - Option “[member port list]” specifies the port or trunk number that belongs to member port such as 3, 6-8, Trk2. - Option “[tagged port list]” specifies the tagged port or trunk number such as 3, 6-8, Trk2.
vlan ip address [vlan id<1-4094>] [ip address]	Configure IPv4 address of specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “[ip address]” specifies the IP address to be configured.
vlan ip address [vlan id<1-4094>] dhcp enable	Enable DHCP to the specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “dhcp enable” is used to enable DHCP.
no vlan ip address [vlan id<1-4094>] dhcp enable	Disable DHCP to the specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “no” is to disable of DHCP.
vlan ipv6 address [vlan id<1-4094>] autoconfig enable	Enable IPv6 autoconfig to specified VLAN - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured.
no vlan ipv6 address [vlan id<1-4094>] autoconfig enable	Disable IPv6 autoconfig to specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “no” is to disable the IPv6 autoconfiguration.
vlan ipv6 address [vlan id<1-4094>] dhcp enable	Enable IPv6 DHCP to the specified VLAN - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured.
no vlan ipv6 address [vlan id<1-4094>] dhcp enable	Disable IPv6 DHCP to the specified VLAN - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “no” is to disable the IPv6 DHCP.

Command	Description
vlan ipv6 address [vlan id<1-4094>] manual enable	Enable IPv6 address manual setting to specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured..
no vlan ipv6 address [vlan id<1-4094>] manual enable	Disable IPv6 address manual setting to specified VLAN. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “no” is used to disable IPv6 address manual setting.
vlan ipv6 address [vlan id<1-4094>] [address_with_prefix]	Configure the IPv6 address with Prefix length to specified VLAN - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option [address_with_prefix] specified IPv6 address with prefix length.
vlan ip-subnet-based add [ip address] [prefix_length<0-64>] [VLAN ID<1-4094>]	Add IP-Subnet-Based VLAN Setting rule. - Option “[ip address]” specifies IP address to be added. - Option “[prefix_length <0-64>] specifies length of prefix. - Option “[VLAN ID <1-4094>]” specifies VLAN ID to be configured.
vlan ip-subnet-based delete [ip address]	Delete an IP-Subnet-Based Vlan rule. - Option “[ip address]” specifies IP address to be deleted.
vlan ip-subnet-based clear	Clear all IP-Subnet-Based VLAN rule
vlan management [vlan id<1-4094>]	Modify the Management VID of DUT - Option “[VLAN ID <1-4094>]” specifies VLAN ID to be configured.
vlan mac-based add [MAC address] [vlan id<1-4094>]	Add MAC-Based Vlan Setting rule - Option “[MAC address]” specifies the MAC address to be added. - Option “[VLAN ID <1-4094>]” specifies VLAN ID to be configured.
vlan mac-based delete [MAC address]	Delete a MAC-Based Vlan Setting rule - Option “[MAC address]” specifies the MAC address to be deleted.
vlan mac-based clear	Clear all MAC-Based VLAN rule
vlan portBased add [VLAN group id] [port-list]	Add VLAN Port-based group configuration rule - Option “[VLAN group id]” specified VLAN group ID to be added. - Option “[port-list]” specifies port number in the Member port list of VLAN Port-based group such as 3 or 6-8.

Command	Description
vlan portBased delete [VLAN group id]	Delete a VLAN Port-based group configuration rule. - Option “[VLAN group id]” specified VLAN group ID to be deleted.
vlan portBased clear	Clear all VLAN Port-based group configuration rule
vlan pvid [port-list] [vlan id<1-4094>]	Configure Port configured VLAN ID. - Option “[port-list]” specifies port number in port list or trunk number in trunk list such as 3, 6-8, or Trk2. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured.
vlan protocol-based group-table add [ethernet/llc/snap] [frame type] [group id<1-2147483646>]	Add Protocol-Based VLAN group-table Setting rule. - Option “[ethernet/llc/snap]” specifies protocol frame type which can be Ethernet, LLC, or SNAP. - Option [frame type] specifies frame type value. - Option [group id <1-2147483646>] specifies group ID.
no vlan protocol-based group-table add [ethernet/llc/snap] [frame type]	Delete a Protocol-Based VLAN group-table Setting rule. - Option “[ethernet/llc/snap]” specifies protocol fraem type which can be Ethernet, LLC, or SNAP. - Option [frame type] specifies frame type value.
vlan protocol-based port-table add [group id<1-2147483646>] [vlan id<1-4094>]	Add Protocol-Based VLAN port-table setting rule - Option “[group id <1-2147483646>]” specifies group ID to be added. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured.
vlan protocol-based port-table delete [group id<1-2147483646>]	Delete a Protocol-Based VLAN port-table setting rule. - Option “[group id <1-2147483646>]” specifies group ID to be deleted.
vlan protocol-based port-table add [group id<1-2147483646>] [vlan id<1-4094>] [port-list]	Add Protocol-Based VLAN port-table setting rule include specified ports - Option “[group id <1-2147483646>]” specifies group ID to be added. - Option “[vlan id <1-4094>]” specifies VLAN ID to be configured. - Option “[port-list]” specifies port number in the port list or trunk number in the trunk list such as 3, 6-8, Trk2.

Command	Description
vlan protocol-based port-table delete [group id<1-2147483646>] [port-list]	Delete a Protocol-Based VLAN port-table setting rule include specified ports - Option "[group id <1-2147483646>]" specifies group ID to be deleted.

1.4.82 VRRP

Virtual Router Redundancy Protocol (VRRP) (RFC 3768) enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any moment, one of the VRRP routing platforms is the master (active) and the others are backups. If the master router fails, one of the backup routers will become the new master router. The master router provides a virtual default routing platform and enables traffic on the LAN to be routed without relying on a signle routing platform. Using VRRP, a backup router can take over a failed default (master) router within a few seconds. This is performed automatically with the minimum required VRRP traffic and without any interaction with the hosts. Users can configure VRRP (Virtual Router Redundancy Protocol) using "vrrp" command and its options as listed in Table 1.83.

Table 1.83 Descriptions of Commands for Setting up VRRP

Command	Description
vrrp	Enable VRRP
no vrrp	Disable VRRP
vrrp add vrid [<1-255>] vlan [<1-4094>] state [<Master/Backup>] pre-empt [<0/1>] priority [<1-254>] advt [<1-255>] auth [<None/Pass>] [code<code>]	Add a new VRRP instance with vrrp-id, VLAN, state, preempt, priority, advertisement interval, and authentication details such as type (NONE|PASS) and code (in case type is PASS). - Option "[<1-255>]" specified virtual router ID. - Option "[<1-4094>]" specifies VLAN ID. - Option "[<Master/Backup>]" specifies virtual router state as either master or backup. - Option "[<0/1>]" specifies pre-emption. This option allows a backup router to preempt a master router. - Option "[<1-254>]" specifies priority. It is an 8-bit number indicating the priority value of the configured virtual router. The higher values represent the higher priority. VRRP routers configured as backup router must use priority values between 1 to 254. The default priority value for VRRP routers backing up a virtual router is 150. The priority value 255 is the highest priority. The priority value of 0 means that the master router does not want to participate.

Command	Description
	- Option "[<1-255>]" specifies the Advertisement interval which is the time inverval in seconds. The default value is 10 second. It is also 8-bit number which means the interval can be between 1 to 255 seconds - Option "[<None/Pass>] specifies the authentication type. The PASS or Password Authentication Type means that the VRRP will use 8 characters of plain text as Authentication Code. - Option "[code<code>]" specifies the authentication code which is a string of 8 bytes. If the string is shorter than 8 bytes, the remaining space must be cleared to zero.
no vrrp vrid [<1-255>]	Delete existing VRRP instance - Option "[<1-255>]" specifies the virtual router ID to be deleted.
no vrrp vrid all	Delete all existing VRRP instances
vrrp vrid [<1-255>] state [<Master/Backup>]	Set the VRRP state for existing vrrp-id MASTER or BACKUP. - Option "[<1-255>]" specifies the virtual router ID. - Option "[<Master/Backup>]" set the state of specified virtual router to either MASTER or Backup.
vrrp vrid [<1-255>] vif [<AA:BB:CC:DD>]	Set a Virtual IP to the existing vrrp-id - Option "[<1-255>]" specifies the virtual router ID. - Option "[<AA:BB:CC:DD>]" specifies the virtual IP address.
no vrrp vrid [<1-255>] vif [<AA:BB:CC:DD>]	Delete an existing virtual IP from existing vrrp-id - Option "[<1-255>]" specifies the virtual router ID. - Option "[<AA:BB:CC:DD>]" specifies the virtual IP address.
vrrp vrid [<1-255>] pre-empt	Enable a preemption mode for an existing vrrp-id - Option "[<1-255>]" specifies the virtual router ID.
no vrrp vrid [<1-255>] pre-empt	Disable a preemption mode for an existing vrrp-id - Option "[<1-255>]" specifies the virtual router ID.
vrrp vrid [<1-255>] priority [<1-254>]	Set the Priority 0-255 for an existing vrrp-id, 255 is the highest priority. 0 means master doesn't want to participate. - Option "[<1-255>]" specifies the virtual router ID.

Command	Description
	- Option “[<1-254>]” specifies the priority for the virtual router.
no vrrp vrid [<1-255>] priority	Set the Priority to default value (100) for an existing vrrp-id. - Option “[<1-255>]” specifies the virtual router ID.
vrrp vrid [<1-255>] advt [<1-255>]	Set the VRRP packet Advertisement Interval timer. - Option “[<1-255>]” specifies the virtual router ID. - Option “[<1-255>]” specifies the Advertisement interval.
vrrp vrid [<1-255>] auth [<None/Pass>] [pass-code]	Set the interface authentication type as NONE or PASS for an existing vrrp-id. If set it to PASS, enter pass-code. - Option “[<1-255>]” specifies the virtual router ID. - Option “[<None/Pass>] specifies the authentication type. - Option “[pass-code]” specifies the authentication code which is a string of 8 bytes.
show vrrp vrid [<1-255>]	Display the information of all existing virtual routers, if no vrid is entered. Otherwise, if vrid is entered, display the information of that virtual router. - Option “[1-255>]” specifies the virtual router ID.
show vrrp vrid [<1-255>] state	Display the state of existing vrrp-id - Option “[1-255>]” specifies the virtual router ID.
vrrp restart	Restart vrrp
show vrrp status	Show VRRP Status

2 Configuring with a Telnet Console

An alternative configuration method is the Telnet method and it is described in this chapter.

2.1 Telnet

Telnet is a remote terminal software to login to any remote telnet servers. It is typically installed in most of the operating systems. In order to use it, users open a command line terminal (e.g., cmd.exe for Windows Operating System).

2.2 Telnet Log-in

After the command line terminal is opened, type in “telnet 10.0.50.1” as shown in Figure 2.1. Note that telnet command needs to follow by IP address or domain name. In this example, the default IP address is 10.0.50.1. If users change the switch IP address, the IP address to log-in should be changed to match the new switch’s IP address.

Figure 2.1 Telnet Command

2.3 Command Line Interface for Telnet

After input the telnet command line, the switch's interface is displayed as shown in Figure 2.2.

```
Username: admin
Password:
switch#
```

Figure 2.2 Log-in Screen using Telnet

Users will see the welcome screen to the switch interface. From Chapter 1, configuring through telnet is similar to configuring through the serial console. Users are automatically logged into the privileged mode. The configuration commands are also similar to the serial console methods. (Please refer to Chapter 1 for more information on configuration).

2.4 Commands in the Privileged Mode

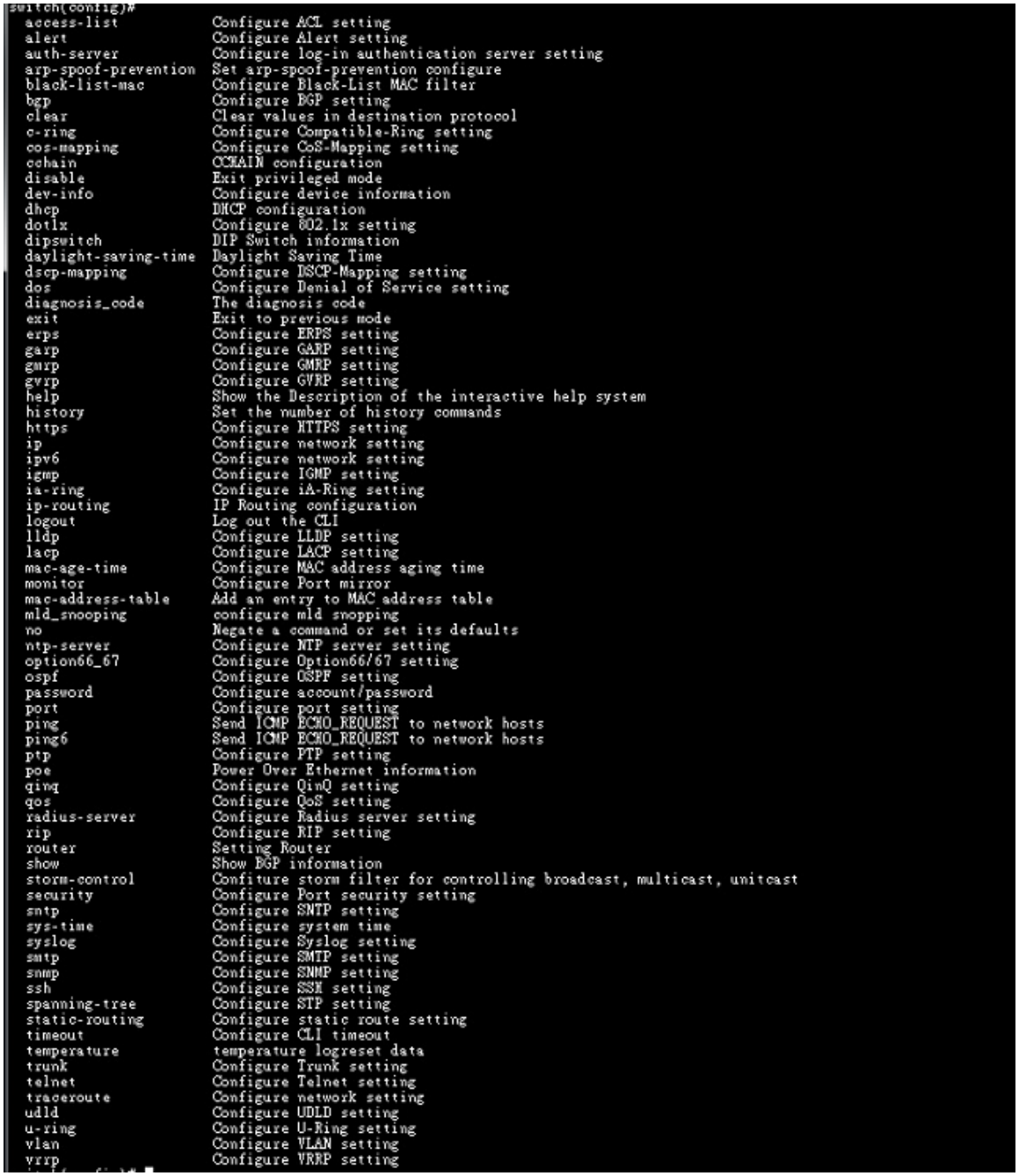
When users do not know the commands to use for the command line configuration, users type in "?" and the commands are displayed on screen as shown in Figure 2.3.

```
Username: admin
Password:
switch#
  configure  Enter configuration mode
  copy       Copy from one file to another
  disable    Exit privileged mode
  exit       Exit to previous mode
  erase      Erase start-up configuration
  help       Show the Description of the interactive help system
  history    Set the number of history commands
  logout     Log out the CLI
  no         Negate a command or set its defaults
  ping       Send ICMP ECHO_REQUEST to network hosts
  reload     Halt and perform a cold restart
  show       Show BGP information
  update     Update firmware
switch#
```

Figure 2.3 Commands in the Privileged Mode

2.5 Commands in the Configuration Mode

When users type in “?” in configuration mode, a long list of commands is displayed on screen as shown in Figure 2.4. Table 2.1 shows all commands that can be used to configure the switch in the configuration mode.



```
switch(config)#
  access-list          Configure ACL setting
  alert                Configure Alert setting
  auth-server          Configure log-in authentication server setting
  arp-spoof-prevention Set arp-spoof-prevention configure
  black-list-mac       Configure Black-List MAC filter
  bgp                  Configure BGP setting
  clear                Clear values in destination protocol
  c-ring               Configure Compatible-Ring setting
  cos-mapping          Configure CoS-Mapping setting
  cchain               CCHAIN configuration
  disable              Exit privileged mode
  dev-info             Configure device information
  dhcp                 DHCP configuration
  dot1x                Configure 802.1x setting
  dipswitch            DIP Switch information
  daylight-saving-time Daylight Saving Time
  dscp-mapping         Configure DSCP-Mapping setting
  dos                  Configure Denial of Service setting
  diagnosis_code       The diagnosis code
  exit                 Exit to previous mode
  erps                 Configure ERPS setting
  garp                 Configure GARP setting
  gmrp                 Configure GMRP setting
  gvrp                 Configure GVRP setting
  help                 Show the Description of the interactive help system
  history              Set the number of history commands
  https                Configure HTTPS setting
  ip                   Configure network setting
  ipv6                 Configure network setting
  igmp                 Configure IGMP setting
  ia-ring              Configure iA-Ring setting
  ip-routing           IP Routing configuration
  logout               Log out the CLI
  lldp                 Configure LLDP setting
  lacp                 Configure LACP setting
  mac-age-time         Configure MAC address aging time
  monitor              Configure Port mirror
  mac-address-table    Add an entry to MAC address table
  mld_snooping         configure mld snopping
  no                   Negate a command or set its defaults
  ntp-server           Configure NTP server setting
  option66_67          Configure Option66/67 setting
  ospf                 Configure OSPF setting
  password             Configure account/password
  port                 Configure port setting
  ping                 Send ICMP ECHO_REQUEST to network hosts
  ping6                Send ICMP ECHO_REQUEST to network hosts
  ptp                  Configure PTP setting
  poe                  Power Over Ethernet information
  qinq                 Configure QinQ setting
  qos                  Configure QoS setting
  radius-server        Configure Radius server setting
  rip                  Configure RIP setting
  router               Setting Router
  show                 Show BGP information
  storm-control        Confiture storm filter for controlling broadcast, multicast, unitcast
  security             Configure Port security setting
  sntp                 Configure SNTP setting
  sys-time             Configure system time
  syslog               Configure Syslog setting
  smtp                 Configure SMTP setting
  snmp                 Configure SNMP setting
  ssh                  Configure SSH setting
  spanning-tree        Configure STP setting
  static-routing       Configure static route setting
  timeout              Configure CLI timeout
  temperature          temperature logreset data
  trunk                Configure Trunk setting
  telnet               Configure Telnet setting
  traceroute           Configure network setting
  udld                 Configure UDLD setting
  u-ring               Configure U-Ring setting
  vlan                 Configure VLAN setting
  vrrp                 Configure VRRP setting
```

Figure 2.4 Commands in the Configuration Mode

Table 2.1 Commands in the Configuration Mode

Command	Descriptions
access-list	Configure ACL setting

Command	Descriptions
alert	Configure Alert setting
auth-server	Configure log-in authentication server setting
arp-spoof-prevention	Set arp-spoof-prevention configure
black-list-mac	Configure Black-List MAC filter
bgp	Configure BGP setting
clear	Clear values in destination protocol
c-ring	Configure Compatible-Ring setting
cos-mapping	Configure CoS-Mapping setting
cchain	CCHAIN configuration
disable	Exit privileged mode
dev-info	Configure device information
dhcp	DHCP configuration
dot1x	Configure 802.1x setting
dipswitch	DIP Switch information
daylight-saving-time	Daylight Saving Time
dscp-mapping	Configure DSCP-Mapping setting
dos	Configure Denial of Service setting
diagnosis_code	The diagnosis code
exit	Exit to previous mode
erps	Configure ERPS setting
garp	Configure GARP setting
gmrp	Configure GMRP setting
gvrp	Configure GVRP setting
help	Show the Description of the interactive help system
history	Set the number of history commands
https	Configure HTTPS setting
ip	Configure network setting
ipv6	Configure network setting
igmp	Configure IGMP setting
ia-ring	Configure iA-Ring setting
ip-routing	IP Routing configuration
logout	Log out the CLI
lldp	Configure LLDP setting
lacp	Configure LACP setting
mac-age-time	Configure MAC address aging time
monitor	Configure Port mirror
mac-address-table	Add an entry to MAC address table
mld_snooping	configure mld snopping
no	Negate a command or set its defaults
ntp-server	Configure NTP server setting
option66_67	Configure Option66/67 setting
ospf	Configure OSPF setting
password	Configure account/password
port	Configure port setting

Command	Descriptions
ping	Send ICMP ECHO_REQUEST to network hosts
ping6	Send ICMP ECHO_REQUEST to network hosts
ptp	Configure PTP setting
poe	Power Over Ethernet information
qinq	Configure QinQ setting
qos	Configure QoS setting
radius-server	Configure Radius server setting
rip	Configure RIP setting
router	Setting Router
show	Show BGP information
storm-control	Configure storm filter for controlling broadcast, multicast, unitcast
security	Configure Port security setting
sntp	Configure SNTP setting
sys-time	Configure system time
syslog	Configure Syslog setting
smtp	Configure SMTP setting

Note: Please see Chapter 1 for the details of switch configuration.

3 Configuring with a SSH Console

An alternative configuration method is the SSH method and it is described in this chapter.

3.1 SSH

SSH is a remote terminal software to login to any remote SSH servers. It is typically installed in most of the operating systems. In order to use it, users open a command line terminal (e.g., cmd.exe for Windows Operating System).

3.2 SSH Log-in

Users may download SSH client for Windows such as PuTTY and enter the IP address of the managed switch to login. A dialog window for entering User name and Password may appear after entering the IP address as shown in Figure 3.1. Note that SSH command needs to follow by IP address or domain name. In this example, the default IP address is 10.0.50.1. If users change the switch IP address, the IP address to log-in should be changed to match the new switch IP address.

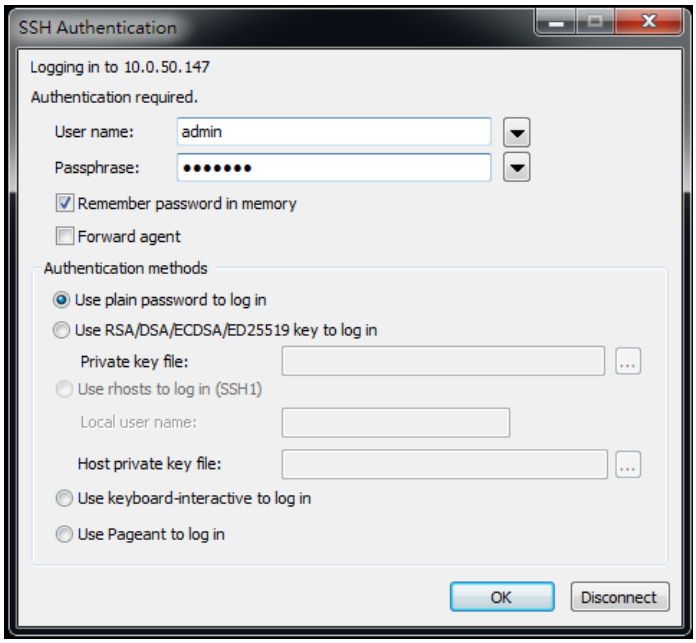


Figure 3.1 SSH Login Command

3.3 Command Line Interface for SSH

After successfully login using SSH, the switch's interface is displayed as shown in Figure 3.2.

Figure 3.2 Log-in Screen using SSH

From Chapter 1, configuring through SSH is similar to configuring through the serial console. Users are automatically logged into the privileged mode. The configuration commands are also similar to the serial console methods. (Please refer to Chapter 1 for more information on configuration).

3.4 Commands in the Privileged Mode

When users do not know the commands to use for the command line configuration, users can type in "?" and the commands are displayed on screen as shown in Figure 3.3.

```
switch#
  configure  Enter configuration mode
  copy       Copy from one file to another
  disable    Exit privileged mode
  exit       Exit to previous mode
  erase      Erase start-up configuration
  help       Show the Description of the interactive help system
  history    Set the number of history commands
  logout     Log out the CLI
  no         Negate a command or set its defaults
  ping       Send ICMP ECHO_REQUEST to network hosts
  reload     Halt and perform a cold restart
  show       Show BGP information
  update     Update firmware
switch#
```

Figure 3.3 Commands in the Privileged Mode

3.5 Commands in the Configuration Mode

When users type in “?” in configuration mode, a long list of commands is displayed on screen as shown in Figure 3.4. Table 3.1

```
switch(config)#
  access-list          Configure ACL setting
  alert                Configure Alert setting
  auth-server          Configure log-in authentication server setting
  arp-spoof-prevention Set arp-spoof-prevention configure
  black-list-mac       Configure Black-List MAC filter
  bgp                  Configure BGP setting
  clear                Clear values in destination protocol
  c-ring               Configure Compatible-Ring setting
  cos-mapping          Configure CoS-Mapping setting
  cchain               CCHAIN configuration
  disable              Exit privileged mode
  dev-info             Configure device information
  dhcp                 DHCP configuration
  dot1x                Configure 802.1x setting
  dipswitch            DIP Switch information
  daylight-saving-time Daylight Saving Time
  dscp-mapping         Configure DSCP-Mapping setting
  dos                  Configure Denial of Service setting
  diagnosis_code       The diagnosis code
  exit                 Exit to previous mode
  erps                 Configure ERPS setting
  garp                 Configure GARP setting
  gmrp                 Configure GMRP setting
  gvrp                 Configure GVRP setting
  help                 Show the Description of the interactive help system
  history              Set the number of history commands
  https                Configure HTTPS setting
  ip                   Configure network setting
  ipv6                 Configure network setting
  igmp                 Configure IGMP setting
  ia-ring              Configure iA-Ring setting
  ip-routing           IP Routing configuration
  logout               Log out the CLI
  lldp                 Configure LLDP setting
  lacp                 Configure LACP setting
  mac-age-time         Configure MAC address aging time
  monitor              Configure Port mirror
  mac-address-table    Add an entry to MAC address table
  mld_snooping         configure mld snopping
  no                   Negate a command or set its defaults
  ntp-server           Configure NTP server setting
  option66_67          Configure Option66/67 setting
  ospf                 Configure OSPF setting
  password             Configure account/password
  port                 Configure port setting
  ping                 Send ICMP ECHO_REQUEST to network hosts
  ping6                Send ICMP ECHO_REQUEST to network hosts
  ptp                  Configure PTP setting
  poe                  Power Over Ethernet information
  qinq                 Configure QinQ setting
  qos                  Configure QoS setting
  radius-server        Configure Radius server setting
  rip                  Configure RIP setting
  router               Setting Router
  show                 Show BGP information
  storm-control        Confiture storm filter for controlling broadcast, multicast, unitcast
  security             Configure Port security setting
  sntp                 Configure SNTP setting
  sys-time             Configure system time
  syslog               Configure Syslog setting
  smtp                 Configure SMTP setting
  snmp                 Configure SNMP setting
  ssh                  Configure SSH setting
  spanning-tree        Configure STP setting
  static-routing       Configure static route setting
  timeout              Configure CLI timeout
  temperature          temperature logreset data
  trunk                Configure Trunk setting
  telnet               Configure Telnet setting
  traceroute           Configure network setting
  udld                 Configure UDLD setting
  u-ring               Configure U-Ring setting
  vlan                 Configure VLAN setting
  vrrp                 Configure VRRP setting
```

Figure 2.4 shows all commands that can be used to configure the switch in the configuration mode.

```
switch(config)#
  access-list          Configure ACL setting
  alert                Configure Alert setting
  auth-server          Configure log-in authentication server setting
  arp-spoof-prevention Set arp-spoof-prevention configure
  black-list-mac       Configure Black-List MAC filter
  bgp                  Configure BGP setting
  clear                Clear values in destination protocol
  c-ring               Configure Compatible-Ring setting
  cos-mapping          Configure CoS-Mapping setting
  cchain               CCHAIN configuration
  disable              Exit privileged mode
  dev-info             Configure device information
  dhcp                 DHCP configuration
  dotlx                Configure 802.1x setting
  dipswitch            DIP Switch information
  daylight-saving-time Daylight Saving Time
  dscp-mapping         Configure DSCP-Mapping setting
  dos                  Configure Denial of Service setting
  diagnosis_code       The diagnosis code
  exit                 Exit to previous mode
  erps                 Configure ERPS setting
  garp                 Configure GARP setting
  gmrp                 Configure GMRP setting
  gvrp                 Configure GVRP setting
  help                 Show the Description of the interactive help system
  history              Set the number of history commands
  https                Configure HTTPS setting
  ip                   Configure network setting
  ipv6                 Configure network setting
  igmp                 Configure IGMP setting
  ia-ring              Configure iA-Ring setting
  ip-routing           IP Routing configuration
  logout               Log out the CLI
  lldp                 Configure LLDP setting
  lacp                 Configure LACP setting
  mac-age-time         Configure MAC address aging time
  monitor              Configure Port mirror
  mac-address-table    Add an entry to MAC address table
  mld_snooping         configure mld snopping
  no                   Negate a command or set its defaults
  ntp-server           Configure NTP server setting
  option66_67          Configure Option66/67 setting
  ospf                 Configure OSPF setting
  password             Configure account/password
  port                 Configure port setting
  ping                 Send ICMP ECHO_REQUEST to network hosts
  ping6                Send ICMP ECHO_REQUEST to network hosts
  ptp                  Configure PTP setting
  poe                  Power Over Ethernet information
  qinq                 Configure QinQ setting
  qos                  Configure QoS setting
  radius-server        Configure Radius server setting
  rip                  Configure RIP setting
  router               Setting Router
  show                 Show BGP information
  storm-control        Confiture storm filter for controlling broadcast, multicast, unitcast
  security             Configure Port security setting
  sntp                 Configure SNTP setting
  sys-time             Configure system time
  syslog               Configure Syslog setting
  smtp                 Configure SMTP setting
  snmp                 Configure SNMP setting
  ssh                  Configure SSH setting
  spanning-tree        Configure STP setting
  static-routing       Configure static route setting
  timeout              Configure CLI timeout
  temperature          temperature logreset data
  trunk                Configure Trunk setting
  telnet               Configure Telnet setting
  traceroute           Configure network setting
  udld                 Configure UDLD setting
  u-ring               Configure U-Ring setting
  vlan                 Configure VLAN setting
  vrrp                 Configure VRRP setting
```

Figure 3.4 Commands in the Configuration Mode

Table 3.1 Commands in the Configuration Mode

Command	Descriptions
access-list	Configure ACL setting
alert	Configure Alert setting
auth-server	Configure log-in authentication server setting
arp-spoof-prevention	Set arp-spoof-prevention configure
black-list-mac	Configure Black-List MAC filter
bgp	Configure BGP setting

Command	Descriptions
clear	Clear values in destination protocol
c-ring	Configure Compatible-Ring setting
cos-mapping	Configure CoS-Mapping setting
cchain	CCHAIN configuration
disable	Exit privileged mode
dev-info	Configure device information
dhcp	DHCP configuration
dot1x	Configure 802.1x setting
dipswitch	DIP Switch information
daylight-saving-time	Daylight Saving Time
dscp-mapping	Configure DSCP-Mapping setting
dos	Configure Denial of Service setting
diagnosis_code	The diagnosis code
exit	Exit to previous mode
erps	Configure ERPS setting
garp	Configure GARP setting
gmrp	Configure GMRP setting
gvrp	Configure GVRP setting
help	Show the Description of the interactive help system
history	Set the number of history commands
https	Configure HTTPS setting
ip	Configure network setting
ipv6	Configure network setting
igmp	Configure IGMP setting
ia-ring	Configure iA-Ring setting
ip-routing	IP Routing configuration
logout	Log out the CLI
lldp	Configure LLDP setting
lacp	Configure LACP setting
mac-age-time	Configure MAC address aging time
monitor	Configure Port mirror
mac-address-table	Add an entry to MAC address table
mld_snooping	configure mld snopping
no	Negate a command or set its defaults
ntp-server	Configure NTP server setting
option66_67	Configure Option66/67 setting
ospf	Configure OSPF setting
password	Configure account/password
port	Configure port setting
ping	Send ICMP ECHO_REQUEST to network hosts
ping6	Send ICMP ECHO_REQUEST to network hosts
ptp	Configure PTP setting
poe	Power Over Ethernet information
qinq	Configure QinQ setting

Command	Descriptions
qos	Configure QoS setting
radius-server	Configure Radius server setting
rip	Configure RIP setting
router	Setting Router
show	Show BGP information
storm-control	Configure storm filter for controlling broadcast, multicast, unitcast
security	Configure Port security setting
sntp	Configure SNTP setting
sys-time	Configure system time
syslog	Configure Syslog setting
smtp	Configure SMTP setting

Note: Please see Chapter 1 for the details of switch configuration.

Atop Technologies, Inc.

www.atoponline.com

TAIWAN HEADQUARTER and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231