ISW-24W-4X

Industrial Ethernet Managed Switch

Web Configuration Tool Guide

Part Number: 9037991-00 Rev. AA
Issue: Aug. 2023

[CONTENTS]

1. Introductions

1.1 System Description

The Managed switches deliver high quality, wide operating temperature range, extended power input range, IP-30 design, and advanced VLAN & QoS features. It's ideal for harsh environments and mission critical applications.

The Managed switches provides enterprise-class networking features to fulfill the needs of large network infrastructure and extreme environments.

The Managed switches ease the effort to build a network infrastructure which offers a reliable, well managed and good QoS networking for any business requiring continuous and well-protected services in industrial environments. With the features such as Fast Failover ring protection and QoS, customers can ensure their network is qualified to deliver any real-time and high-quality applications.

1.2 Using the Web Interface

The object of this document "Web Configuration Tool Guide" is to address the web feature, design layout and descript how to use the web interface.

1.2.1 Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

Language script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	16

Google Chrome with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

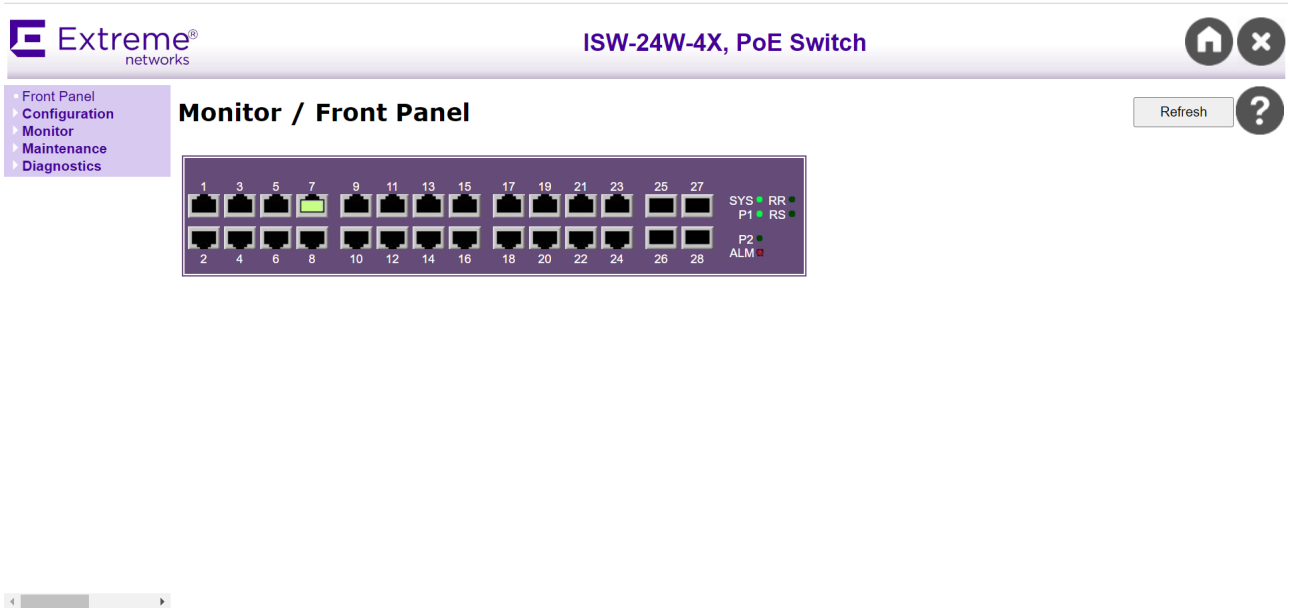
1.2.2 Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

- **Monitor** - Display statistics, status, and contents of memory.
- **Configuration** - Configure the system, interfaces, and filters.
- **Maintenance** - Display system information, download firmware, back up configurations, and modify users.

You can find the detailed information in section 2.2 Tree View.

1.2.3 Title Bar Icons



Help Button

For more information about any screen, click on the Help button on the screen.
Help information is displayed in the same window.

Save Button 

If any unsaved change has been made to the *configuration* (by you during this or a prior session, or by any other administrator using the web interface or the Command Line Interface), a Save icon appears in the title line. To save the running configuration to the startup configuration:

1. Click on the Save icon. The System/Save and Restore screen appears.
2. Click on Submit next to Data Control Action drop-down list on top of System/Save and Restore screen.

1.2.4 Ending a Session

To end a session, close your web browser. This prevents an unauthorized user from accessing the system using your user name and password.

1.3 Using the Online Help

Each screen has a Help button  that invokes a page of information relevant to the particular screen. The Help is displayed in a new window.
Each web page of Configuration/Status/System functions has a corresponding help page.

2. Using the Web

2.1 Login

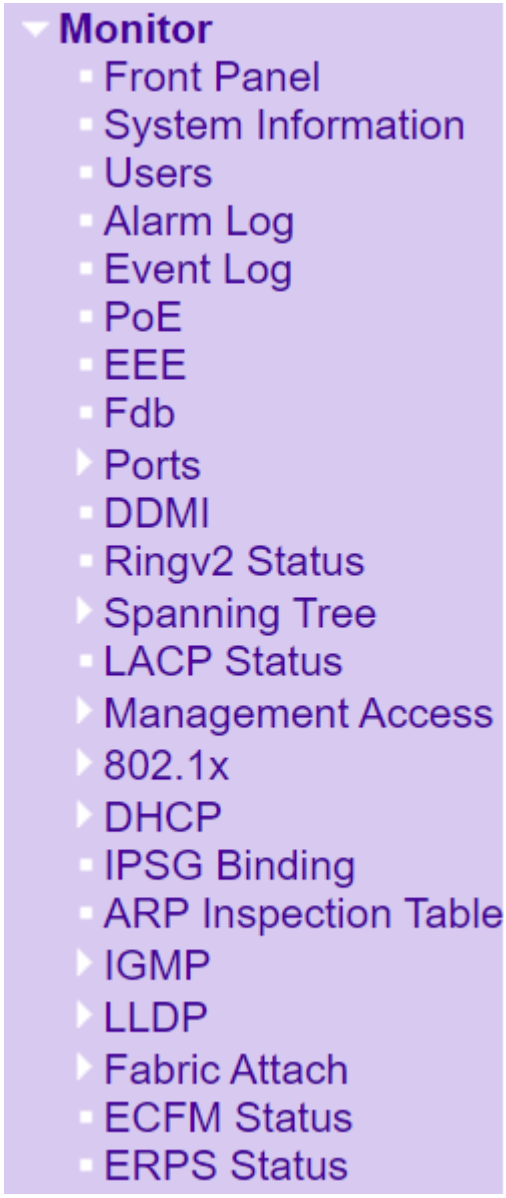
Operation	1. Fill Username and Password 2. Click “Sign in”
Field	Description
Username	Login user name. The maximum length is 32. Default: admin
Password	Login user password. The maximum length is 32. Default: none

2.2 Tree View

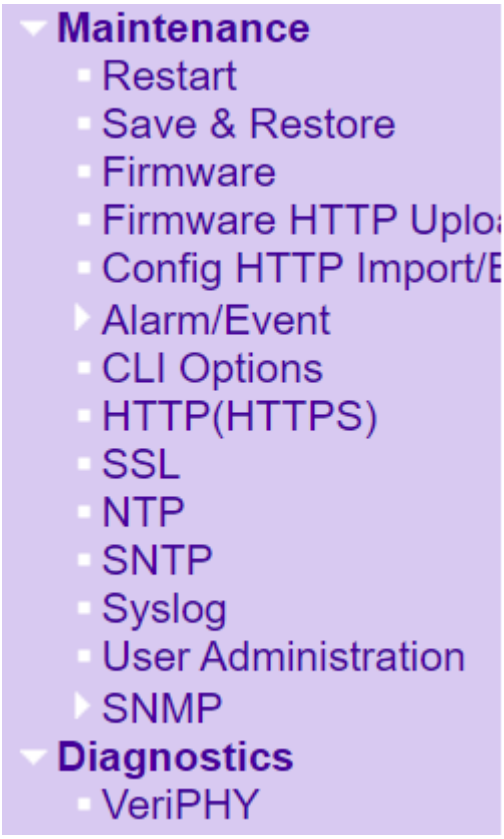
The tree view is a menu of the web. It offers user quickly to get the page for expected data or configuration.

2.2.1 Configuration Menu

2.2.2 Monitor Menu



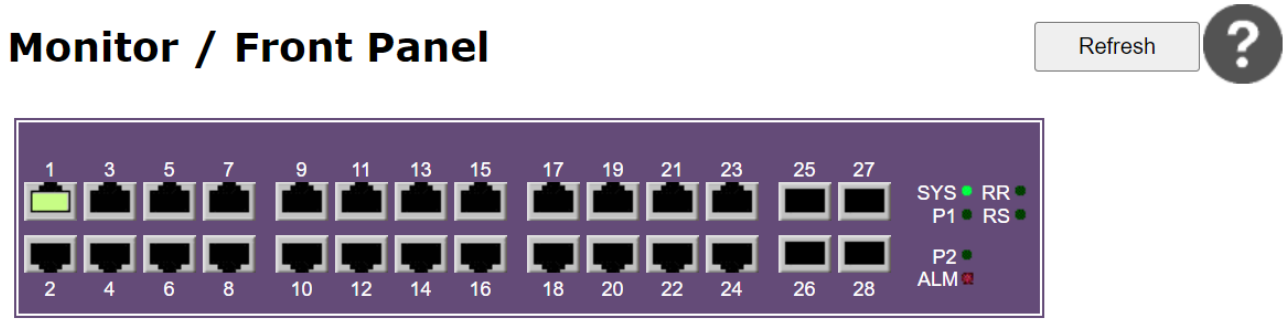
2.2.3 Maintenance/Diagnostics Menu



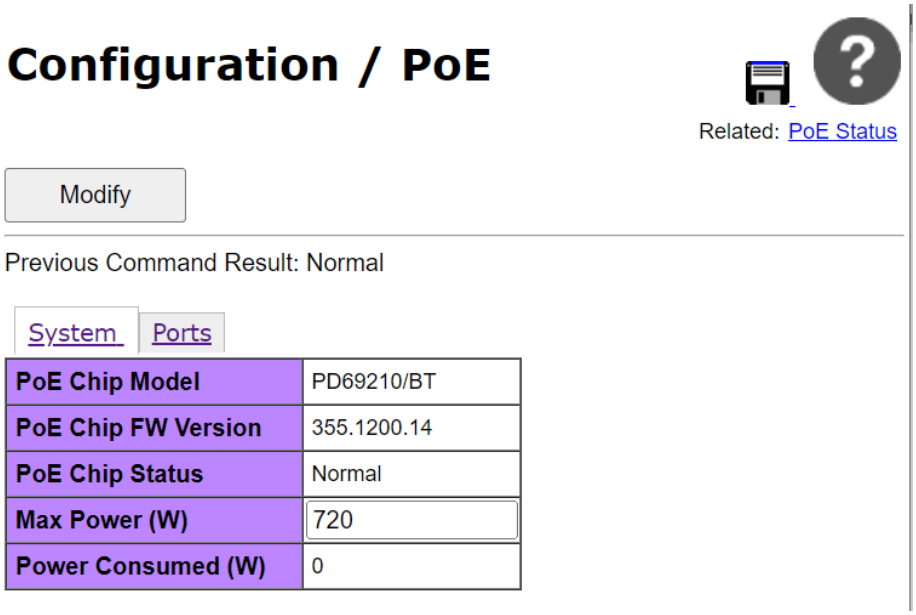
2.3 Configuration

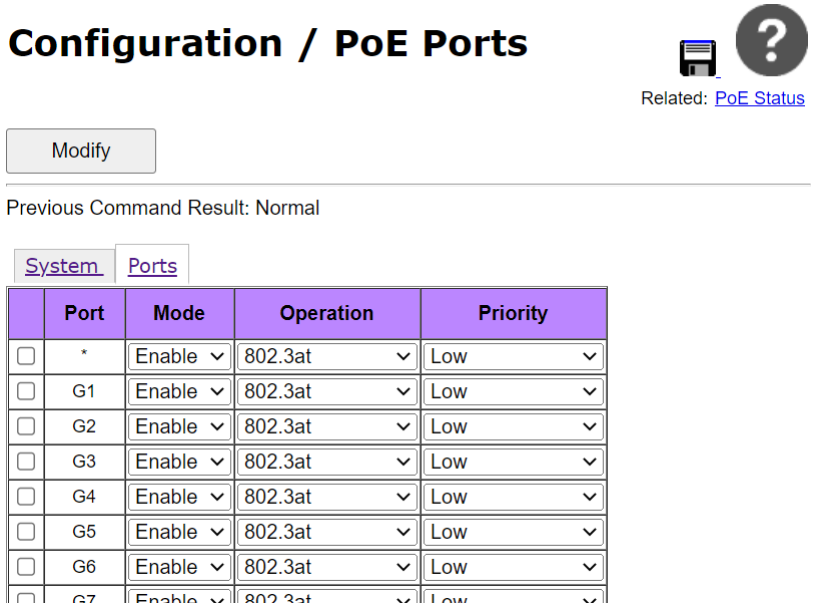
2.3.1 Front Panel

Use the Monitor/Front Panel screen to view the graphic of front panel.
This page will automatically refresh per 3 seconds.



2.3.2 PoE

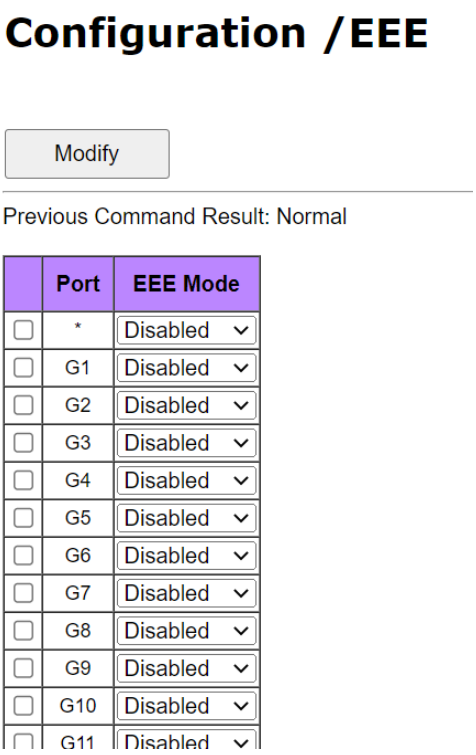




Operation	<u>To configure Max Power:</u> 1. Change Max Power value. 2. Click top "Modify" button to modify the setting. <u>To configure PoE:</u> 1. Select a row of port. 2. Change fields value. 3. Click "Modify" button to modify setting data.
Field	Description
PoE Chip Model	PoE Chip Model Information. (Read-only)
PoE Chip FW Version	PoE Chip Firmware Version. (Read-only)
PoE Chip Status	PoE Chip Status. (Read-only)
Max Power (W)	Max PoE Power limitation overall the system. Unit is Watt. (Range: 0 - 720W, default is 720W).
PoE Power Consumed (W)	Total PoE Power Consumed overall the system. (Read-only)
Port	G1 ~ G24
Mode	PoE Disabled/Enabled on the port.
Operation	PoE operation mode/protocol on the port. - 802.3at : Support PoE capability of performing IEEE-802.3AT protocol - 802.3bt/type3 : Support PoE capability of performing IEEE-802.3BT/Type3

	- 802.3bt/type4 : Support PoE capability of performing IEEE-802.3BT/Type4 - poh : Support PoE capability of performing non-compliant PoH mode
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices require more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

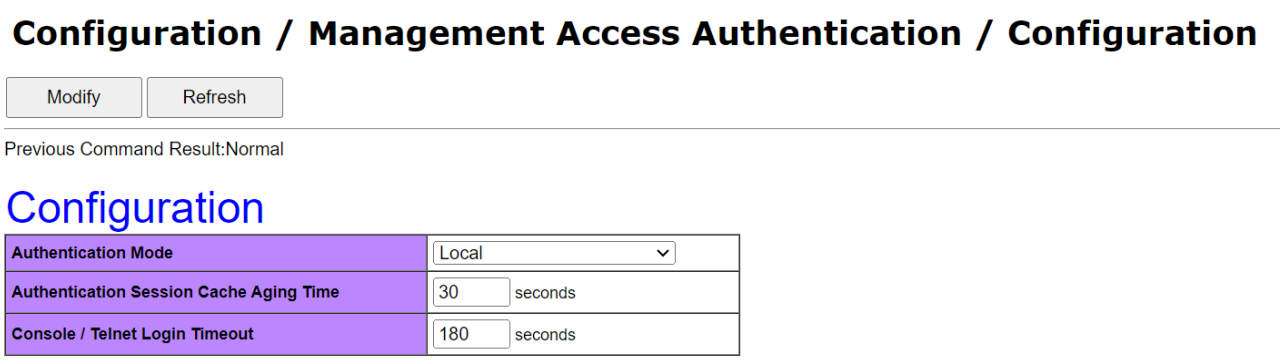
2.3.3 EEE



Operation	Modify: 1. Push "Modify" button to apply new configuration for port(s) configuration. 2. Display "Success" when previous operation is successful. 3. Display "Fail" when previous operation is failure. Refresh: Push "Modify" button to refresh ports status.
Field	Description
Port	Specify the port identifier.

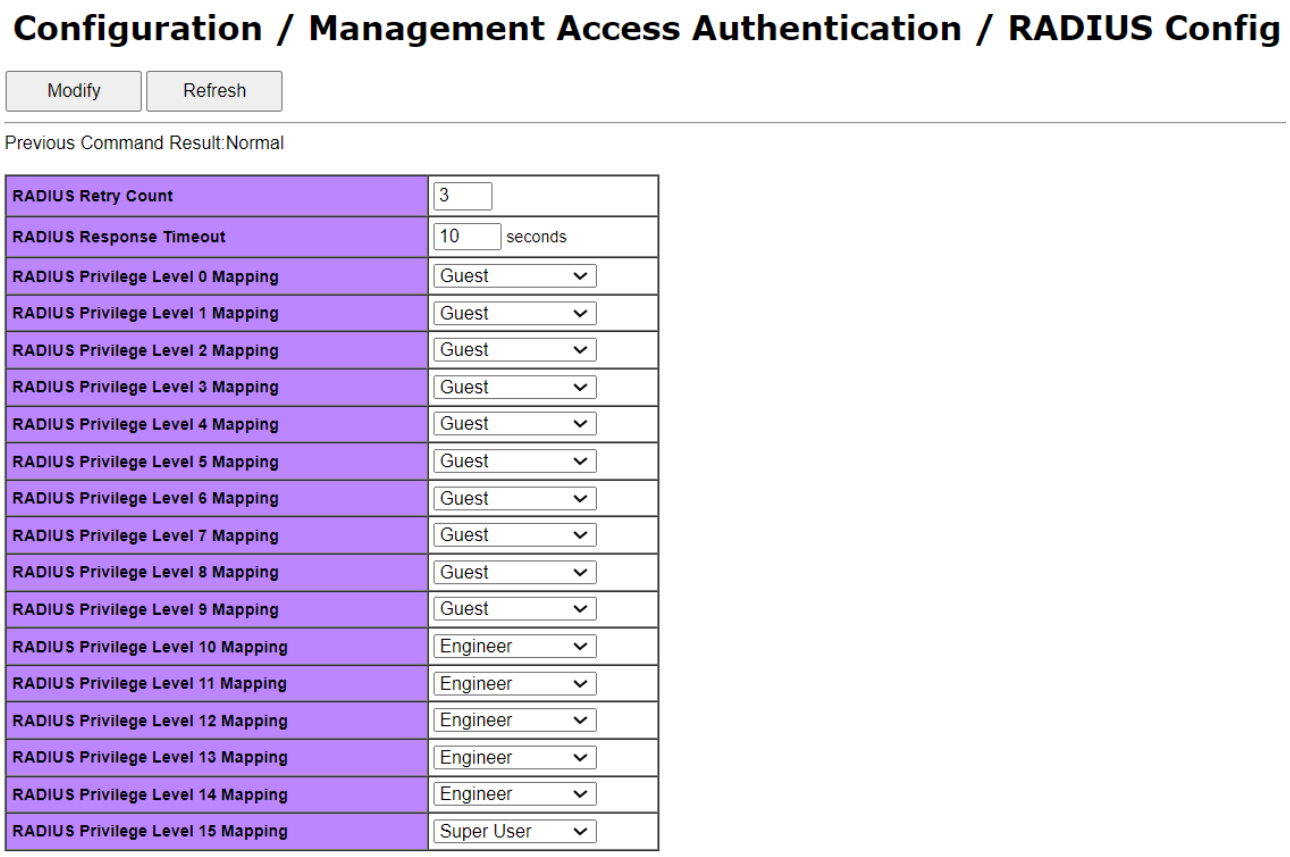
EEE Mode	Perform this port to operate EEE auto negotiation with link-partner. There are : "Enabled" - Enable operating EEE auto-negotiation with link partner. "Disabled" - Disable operating EEE auto-negotiation with link partner. (It is default.)

2.3.4 Management Access Authentication - Configuration



Operation	Modify: 1. Push "Modify" button to apply the changes. 2. Display "Success" when previous operation is successful. 3. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
Authentication Mode	Valid Range: Local RADIUS, Local TACACS+, Local Default value: Local
Authentication Session Cache Aging Time	Valid Range: 10 ~ 600 seconds, default value: 30
Console / Telnet Login Timeout	Valid Range: 30 ~ 600 seconds, default value: 180

2.3.5 Management Access Authentication - RADIUS Config



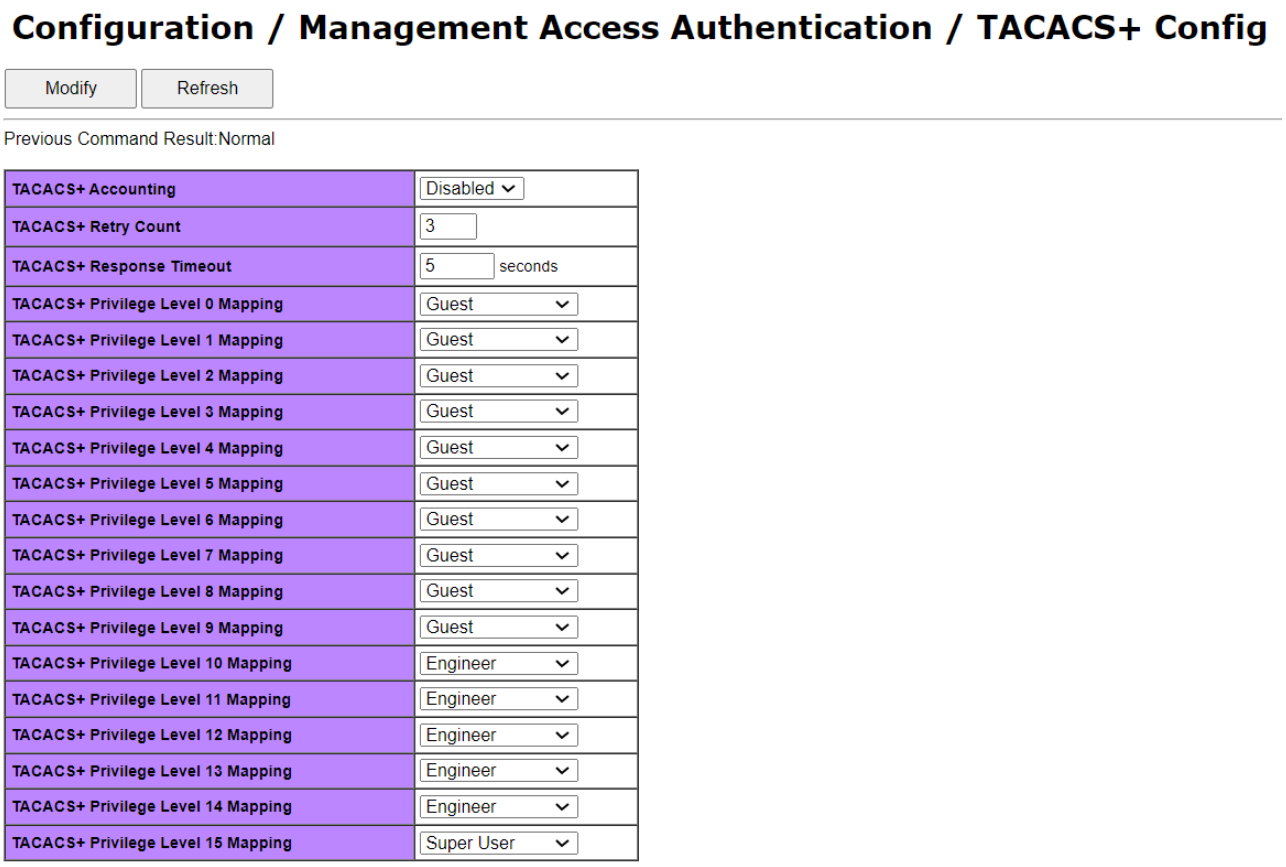
Operation	Modify: 1. Push "Modify" button to apply the changes. 2. Display "Success" when previous operation is successful. 3. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
RADIUS Retry Count	Valid Range: 1 ~ 5, default value: 3
RADIUS Response Timeout	Valid Range: 1 ~ 30 seconds, default value: 10
RADIUS Privilege Level 0 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest

RADIUS Privilege Level 1 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 2 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 3 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 4 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 5 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 6 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 7 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 8 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 9 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
RADIUS Privilege Level 10 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
RADIUS Privilege Level 11 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
RADIUS Privilege Level 12 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
RADIUS Privilege Level 13 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
RADIUS Privilege Level 14 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
RADIUS Privilege Level 15 Mapping	Valid Range: Super User, Engineer and Guest, default value: Super User

2.3.6 Management Access Authentication - RADIUS Server

Operation	New Server: 1. Push "New Server" button to edit the new server configuration. 2. Push "Delete" button to remove the new server configuration. 3. Up to 4 servers can be created. Modify: 1. Push "Modify" button to apply the changes. 2. Display "Success" when previous operation is successful. 3. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
IPv4 Address	RADIUS Server IPv4 Address
Port	RADIUS Server Authentication UDP port number, Valid Range: 1 ~ 65535, default is 1812.
Secret	RADIUS Server Authentication Key, Valid Range: 1 ~ 16 characters

2.3.7 Management Access Authentication - TACACS+ Config



Operation	Modify: 1. Push "Modify" button to apply the changes. 2. Display "Success" when previous operation succeeds. 3. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
TACACS+ Accounting	Valid Range: Disabled / Enabled, default value: Disabled
TACACS+ Retry Count	Valid Range: 1 ~ 5, default value: 3
TACACS+ Response Timeout	Valid Range: 1 ~ 300 seconds, default value: 5
TACACS+ Privilege Level 0	Valid Range: Super User, Engineer and Guest, default value: Guest

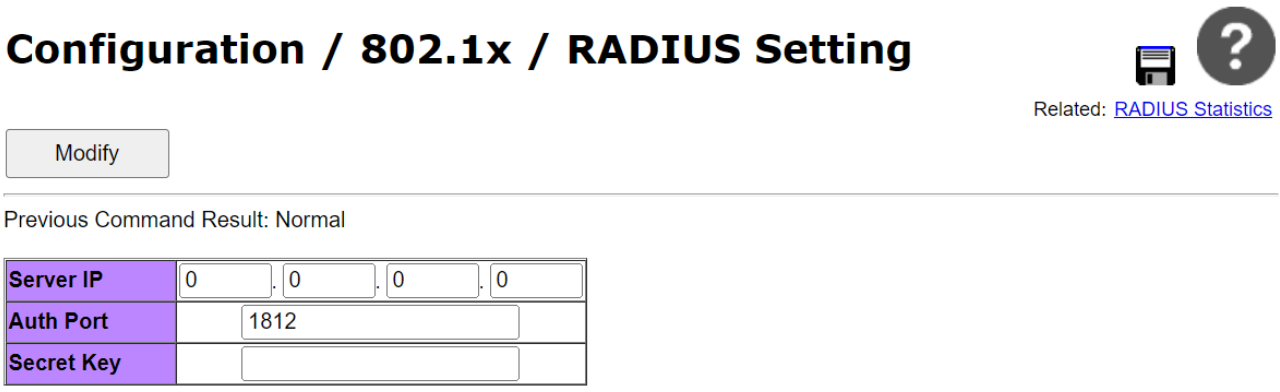
Mapping	
TACACS+ Privilege Level 0 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 1 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 2 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 3 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 4 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 5 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 6 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 7 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 8 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 9 Mapping	Valid Range: Super User, Engineer and Guest, default value: Guest
TACACS+ Privilege Level 10 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
TACACS+ Privilege Level 11 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
TACACS+ Privilege Level 12 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
TACACS+ Privilege Level 13 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
TACACS+ Privilege Level 14 Mapping	Valid Range: Super User, Engineer and Guest, default value: Engineer
TACACS+ Privilege Level	Valid Range: Super User, Engineer and Guest, default value: Super User

15 Mapping	

2.3.8 Management Access Authentication - TACACS+ Server

Operation	New Server: 1. Push "New Server" button to edit the new server configuration. 2. Push "Delete" button to remove the new server configuration. 3. Up to 4 servers can be created. 4. Each summit can add only one entry at one time. Modify: 1. Push "Modify" button to apply the changes. 2. Display "Success" when previous operation succeeds. 3. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
IPv4 Address	TACACS+ Server IPv4 Address
Port	TACACS+ Server Authentication TCP port number, Valid Range: 1 ~ 65535, default is 49.
Secret	TACACS+ Server Authentication Key, Valid Range: 0 ~ 32 characters

2.3.9 802.1x Authentication - RADIUS Setting



Operation	Modify: 1. Modify Server IP, Authentication Port and Secret Key fields. 2. Click "Modify" button to apply change.
Field	Description
Server IP	The IP address of RADIUS server. Allow IPv4 address. 0.0.0.0 means disable RADIUS. Default is 0.0.0.0.
Auth Port	The UDP port of RADIUS server for authentication. Range 1~65535. Default is 1812.
Secret Key	The key to be used between RADIUS server and Authenticator. Range 0~16 chars. Default is empty string.

2.3.10 802.1x Authentication - PAE Port Authentication

Configuration / 802.1x / System Authentication

Modify

Previous Command Result: Normal

System Ports

System AuthControl	Disabled

Configuration / 802.1x / PAE Port Authentication

Related: PAE Port Status EAPOL Statistics

Modify

Previous Command Result: Normal

System Ports

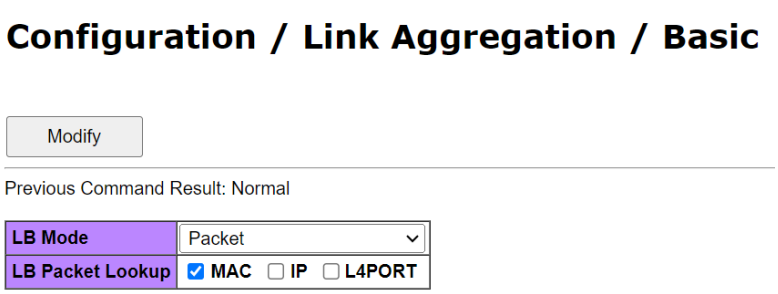
	Port	Auth Control	ReAuth Enabled	ReAuth Period(sec)	Sense Period(sec)	Quiet Period(sec)	Tx Period(sec)	Supp. Timeout(sec)	Server Timeout(sec)	Max Request
☐	*	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G1	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G2	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G3	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G4	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G5	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G6	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G7	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G8	Force Authorized	Disabled	3600	10	60	30	30	30	2
☐	G9	Force Authorized	Disabled	3600	10	60	30	30	30	2

Operation	Modify System Auth. Control: 1. Select System Auth. Control. 2. Click "Modify" button to apply change. Modify PAE Port Authentication: 1. Update below fields. 2. Check up the port(s) to be changed. Click "Modify" button to modify PAE Port Authentication options.
Field	Description
System AuthControl	Enable/Disable system 802.1x authentication function. Default value is Disabled.
Port	PAE port: 1 ~ MAX Number of Port.

Auth Control	Specify the authentication control behavior for the port. There are: "Force Unauthorized" - Specify the port is required to be held in the Unauthorized state. "Force Authorized" - Specify the port is required to be held in the Authorized state. "Auto" - Specify the port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server. "Sense" - Specify the port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server, If sense period expired, then go to MAC Based Authentication. "MAC Based" - Specify the port is set to the Authorized or Unauthorized state based on Supplicant's MAC Address
ReAuth Enabled	Defines whether regular reauthentication will take place on this Port. A value of 'Enabled' enables reauthentication; 'Disabled' disables reauthentication.
ReAuth Period(sec)	Defines a nonzero number of seconds between periodic reauthentication of the Supplicant. The default value is 3600s; it can be set by management to any value in the range from 1 to 3600s.
Sense Period(sec)	The initialization value used for the senseWhile timer. Its default value is 10 seconds; it can be set by management to any value in the range from 10 to 255 seconds.
Quiet Period(sec)	The initialization value used for the quietWhile timer (specified in IEEE-802.1x-8.5.2.1). Its default value is 60 seconds; it can be set by management to any value in the range from 1 to 255 seconds.
Tx Period(sec)	The initialization value used for the txWhen timer (specified in IEEE-802.1x-8.5.2.1). Its default value is 30 seconds; it can be set by management to any value in the range from 1 to 255 seconds.
Supp. Timeout(sec)	The initialization value used for the aWhile timer when timing out the Supplicant. Its default value is 30 seconds; it can be set by management to any value in the range from 1 to 255 seconds.

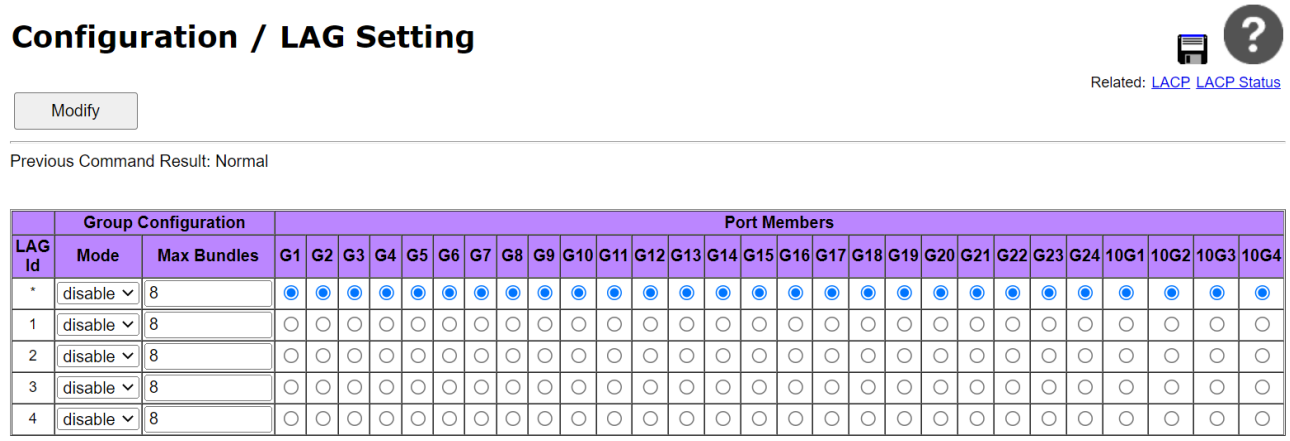
Server Timeout(sec)	The initialization value used for the aWhile timer when timing out the Authentication Server. Its default value is 30 seconds; it can be set by management to any value in the range from 1 to 255 seconds.
Max Request	The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session. Its default value is 2; it can be set by management to any value in the range from 1 to 10.

2.3.11 Link Aggregation – Basic



Operation	Modify: 1. Push "Modify" button to apply changes. 2. Display "Success" when changes are successfully applied. 3. Display "Fail" when changes are failed to be applied.
Field	Description
LB Mode	Configure the hash algorithm to do load balance for the link aggregation. There are: Packet: Hash based on packet header information. It can configure which layer of information is included in Hash generation. Please refer to description of "LB Packet lookup" field. This is default setting. Port: Hash based on the ingress interface, which can be either a port or a link aggregation.
LB Packet Lookup	Configure which layer of packet header information is included in Hash generation. These setting is only available when LB mode is packet-based. There are : MAC: To enable inclusion of Layer 2 information in Hash generation for IP packets. IP: To enable inclusion of information from Layers 3 in Hash generation. L4Port: To enable inclusion of TCP/UDP ports in Hash generation.

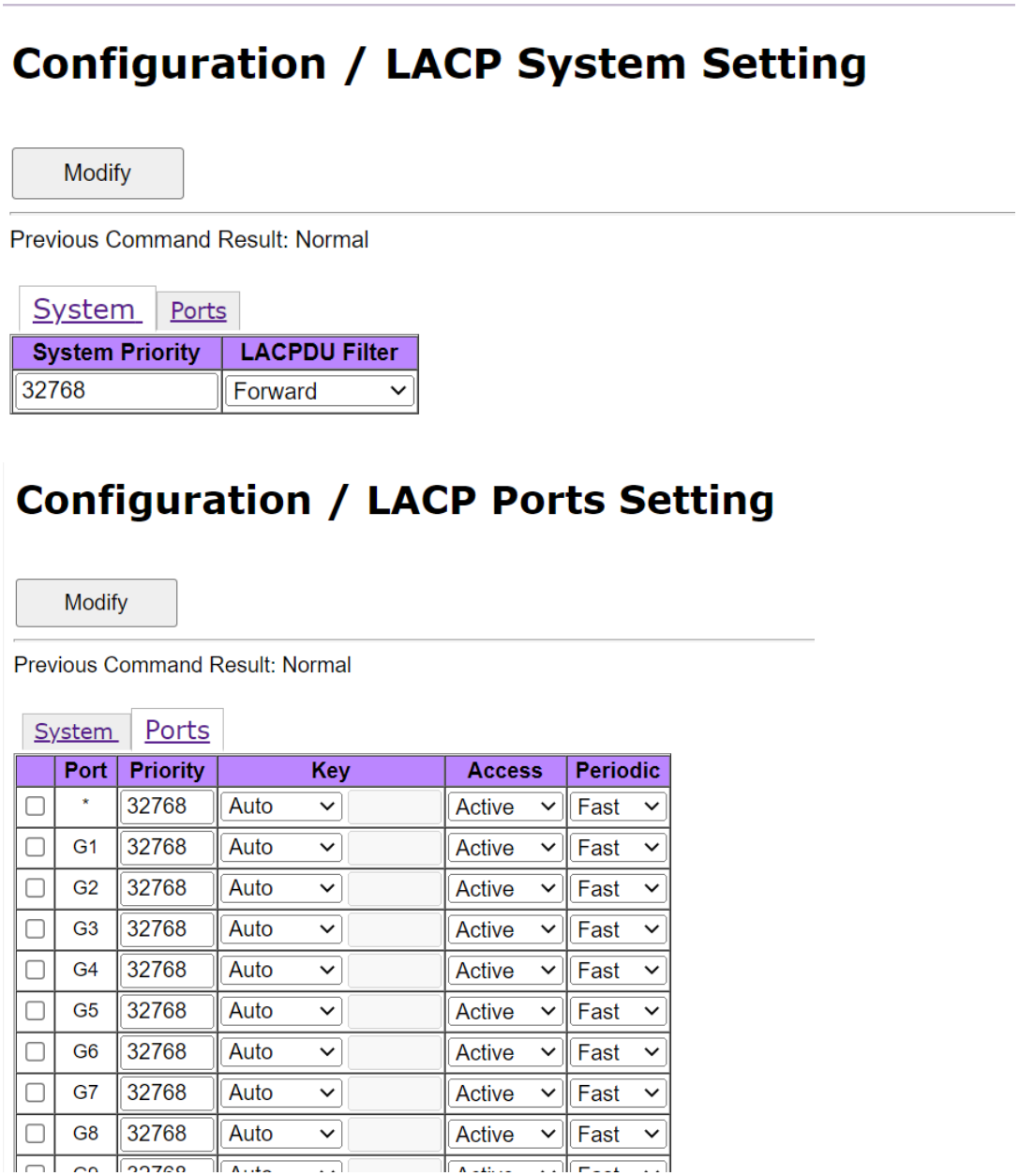
2.3.12 Link Aggregation – LAG setting



	Group Configuration		Port Members																										
LAG Id	Mode	Max Bundles	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	10G1	10G2	10G3	10G4
*	disable	8	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
1	disable	8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	disable	8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	disable	8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	disable	8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Operation	Modify: 1. Select one LAG for setting. 2. Click Modify button.
Field	Description
LAG ID	Inform one number to identify this Link Aggregation group.
Mode	Specify the method to operate Link Aggregation for this LAG. There are : "disable" - This LAG is not available now. "static" - This LAG operates aggregation depending on static bundling of manually configured ports. "lacp" - This LAG operates aggregation depending on dynamic bundling of LACP process.
Max Bundles	Specify the max bundled members for this LAG. This value limits the "active" bundling numbers, not numbers joined to the LAG. Valid range is from 1 to 8. Default is 8.
Port Members	Specify the port join to the LAG. Each port is allowed to join to one LAG only.

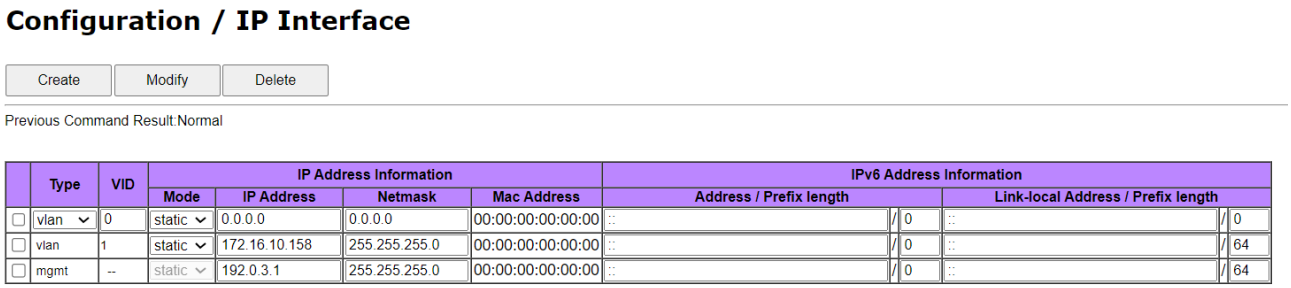
2.3.13 Link Aggregation – LACP Setting



Operation	Push "Modify" button to apply changes. Display "Success" when changes are successfully applied. Display "Fail" when changes are failed to be applied.
Field	Description
System Priority	Specify the system priority for LACP process. Valid range is from 1 to 65535. Default is 32768.
LACPDU Filter	Specify LACPDU filter behavior. There are :

	"Disable" - Bypass incoming LACP PDUs. "Forward" - Receive LACP PDUs on LACP Port and bypass it on the non-LACP port. (default). "Soft-Drop" - Receive LACP PDUs on LACP Port and discard it on the non-LACP port. "Hard-Drop" - Always drop incoming LACP PDUs.
Port	Specify the port identifier.
Priority	Specify one number to identify the priority for this LACP port. Valid range is from 1 to 65535. Default is 32768.
Key	Specify key generated method for this LACP port. There are : "Auto" - key value is dynamic generated according to port speed. (It is default.) "Specific" - key value is static configured number in range of 1 to 65535.
Access	Specify access mode for this LACP port. There are : "Active" - this LACP port always generates LACP-PDU to do negotiation with partner. (It is default.) "Passive" - this LACP port will do nothing until it receives LACP-PDU from the partner.
Periodic	Specify transmissions mode of LACP-PDU for this LACP port. There are : "Fast" - the number of seconds between periodic transmissions is using Short Timeouts of 1 second. (It is default.) "Slow" - the number of seconds between periodic transmissions is using Long Timeouts of 30 seconds.

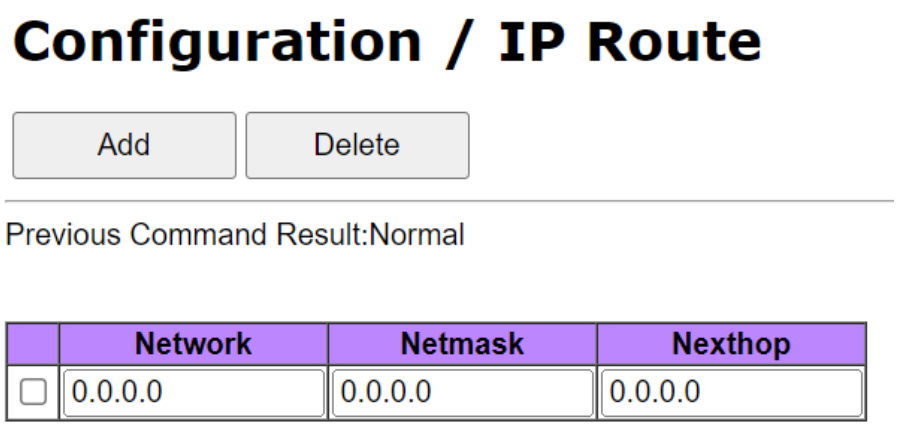
2.3.14 IP Interface



Operation	Modify: Choose the check-box of IP interfaces that are modified and then push "Modify" button to apply these changes. Display "Success" when changes are successfully applied. Display "Fail" when changes are failed to be applied. Create: Input valid value in first row fields and then push "Create" button to create one IP interface. Display "Success" when new IP interface is successfully created. Display "Fail" when new IP interface is failed to be created. Delete: Choose the check-box of IP interfaces that are deleted and then push "Delete" button to delete these ones. Display "Success" when selected IP interfaces are successfully deleted. Display "Fail" when selected IP interfaces are not completely deleted.
Field	Description
Type	Specify the type associated to this IP interface. There are : "vlan" - this IP interface is only available on specific VLAN. "mgmt" - this IP interface is only available on physical management port.

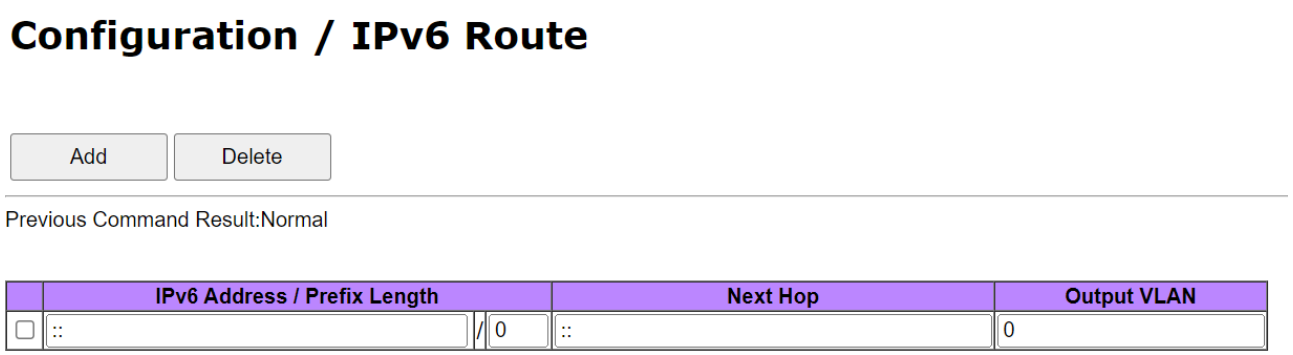
VID	Specify the VLAN that IP interface operates on. In case of "Creating", input one VLAN number in range of 2 to 4094. In others case, this field is read-only. This field is only available while type is "vlan".
Mode	Specify IP address assignment for this interface. There are : "static" - IP address is static configured. "dhcp" - IP address is assigned by DHCP CLIENT process. When interface type is "mgmt", it only accepts static IP setting.
IP Address	When mode is 'static', this field supports manual setting in format of dotted decimal notion. When mode is 'dhcp', this field is read-only. It is dynamic assigned by DHCP CLIENT process.
IP Netmask	When mode is 'static', this field supports manual setting in format of dotted decimal notion. When mode is 'dhcp', this field is read-only. It is dynamic assigned by DHCP CLIENT process.
Mac Address	This is read-only filed, informed the MAC address of this IP interface. This address is assigned by internal mechanism at stage of creating IP interface.
IPv6 Address/Prefix length	This field supports IPv6 unicast address setting in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 2001::123:c456:1001/64. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.
IPv6 Link-local Address/Prefix length	This field supports IPv6 link-local address setting in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::223:2ff:fe00:184d/64. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. By default, automatically construct an IPv6 link-local address in the EUI-64 format.

2.3.15 IP Route



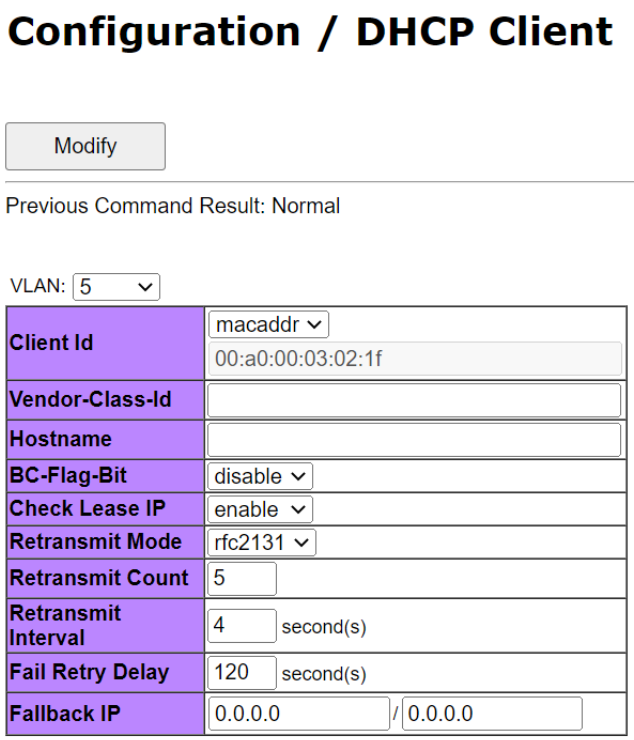
Operation	Delete: Choose the check-box of routes that are deleted and then push "Delete" button to delete these ones. Display "Success" when selected routes are successfully deleted. Display "Fail" when selected routes are not completely deleted. Create: Input valid value in first row fields and then push "Create" button to create one new route. Display "Success" when new route is successfully created. Display "Fail" when new route is failed to be created.
Field	Description
Network	Specify the network address of the route. It only accepts unicast IP address string identified in dotted decimal format (ex: w.x.y.z).
Netmask	Specify the netmask address of the route . It only accepts the sting in dotted decimal format (ex: w.x.y.z).
Nexthop	Specify nexthop address for this route. It only accepts unicast IP address string identified in dotted decimal format (ex: w.x.y.z).

2.3.16 IPv6 Route



Operation	Delete: Choose the check-box of routes that are deleted and then push "Delete" button to delete these ones. Display "Success" when selected routes are successfully deleted. Display "Fail" when selected routes are not completely deleted. Create: Input valid value in first row fields and then push "Create" button to create one new route. Display "Success" when new route is successfully created. Display "Fail" when new route is failed to be created.
Field	Description
IPv6 Address / Prefix Length	Specify the destination address of the route. The first field supports IPv6 unicast address setting in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). The second field is network prefix length in range of 1 to 128.
Next hop	Specify nexthop address for this route. It supports IPv6 unicast address setting in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). It must be valid address of one hop that exist on any reachable network.
Output VLAN	Specify egress interface of the routing traffic associated to this route. When this filed is undefined, the VLAN interface that can reach nexthop will be default egress VLAN interface.

2.3.17 DHCP Client



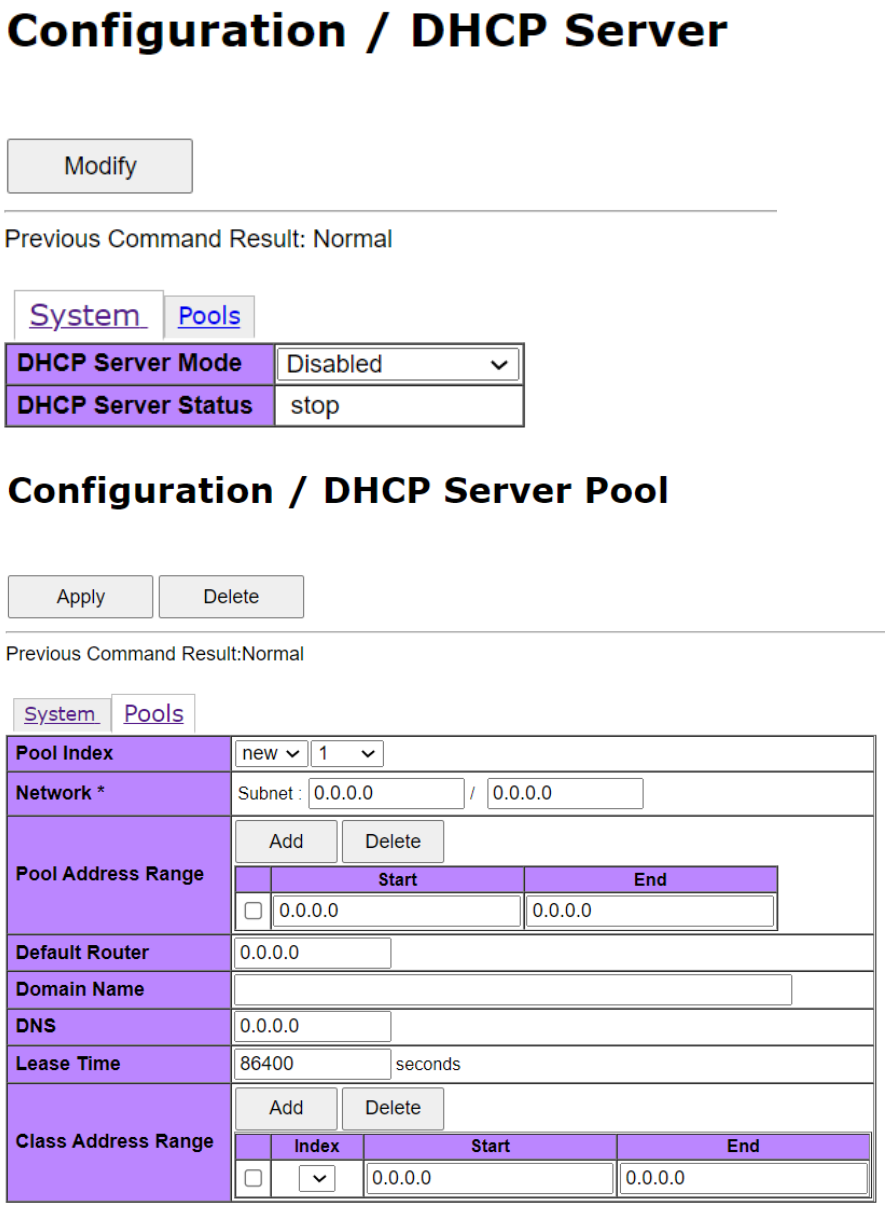
Operation	Push "Modify" button to apply new configuration for a DHCP client. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
VLAN	Identify the VLAN operated DHCP in drop-down list. When one VLAN is selected, valid DHCP client configuration form is generated for user setting.

Client Id	This field is used by DHCP clients to specify their unique identifier. It treats as code of "61" in the options field of the DHCP message. In common the client identifier consists of type-value pairs similar to the 'htype'/'chaddr' fields. It supports three different modes for user specifying the identifier. There are : "macaddr" - it consists of a hardware type and hardware address. In this case the type is one of the ARP hardware types defined in STD2 [RFC 1700]. The MAC address of the VLAN interface will be used as a reference for this hardware address. "ascii" - it also consists of the type and identifier value. In this case the type of "0" is used and one contains identifier string other than a hardware address. Any printable character of ASCII table is accepted, that maximum length is 32 characters. "hex" - it consists of multiple hexadecimal octets. In this case user determinate value of the type and identifier string. User should input 2 hexadecimal pairs of octet(s) that up to 64 hexadecimal numbers (or 32 hexadecimal octets).
Vendor-Class-Id	This field is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. It treats as code of "60" in the options field of the DHCP message. When the field is empty, this option will not be attached on DHCP message. It supports maximum length is 32 characters.
Hostname	This field is used to specify the name of the DHCP client. It treats as code of "12" in the options field of the DHCP message. While the filed is empty or no change by default, this name string is similar to local device name. User can configure different name string other than device name, which maximum length is 64 characters.

BC-Flag-Bit	Specify "BROADCAST" bit of the flag field of the DCHP message. Sometimes DHCP client cannot accept IP unicast datagrams before leased IP address is not available on local device. This will cause the client always reject unicast datagram of DHCP response message. Then the client cannot get leased IP address since it rejects lease message. In this case user can select "enabled" option for setting this bit in DHCP request message to inform DHCP server that always send broadcast datagram. By default, "disabled" is selected in this field.
Check Lease IP	Inform DHCP client detecting that lease IP address is already in use in the network. There are : "enabled" - DHCP client will do ARP announcement for detecting duplicated IP address. If receives Gratuitous ARP or any ARP message informed this IP, it will send a DHCPDECLINE message to the server and restarts the process. By default, this option is used for doing this detecting mechanism. "disabled" - DHCP client use the leased IP address without any detecting.
Retransmit Mode	Inform DHCP client retransmission mechanism. There are : "rfc2131" - the DHCP client always retransmit the DHCPREQUEST according to the retransmission algorithm described in section 4.4.5 of RFC2131. "user" - user determine the interval and number for retransmitting the DHCPREQUEST.
Retransmit Count	Specify the numbers to retransmit how many DHCPREQUEST if no response message receives. This filed is only available when Retransmit Mode is "user". The accepted range is "0 ~ 5".
Retransmit Interval	Specify the timeout to retransmit DHCPREQUEST if no response message receives. This filed is only available when Retransmit Mode is "user". The accepted range is "4 ~ 64" in unit of second. The value of "4" is used by default.
Fail Retry Delay	Specify the delay time for restarting initialization process when last initialization process fails. The accepted range is "10 ~ 600" in unit of second. The value of "120" is used by default.

Fallback IP	Inform one "fallback" mechanism to doing temporal IP assignment on DHCP client when leased IP address in not available. This mechanism is only available when both fields of IP address and netmask are valid. Only accept the address in format of dotted decimal notion. (ex: w.x.y.z)

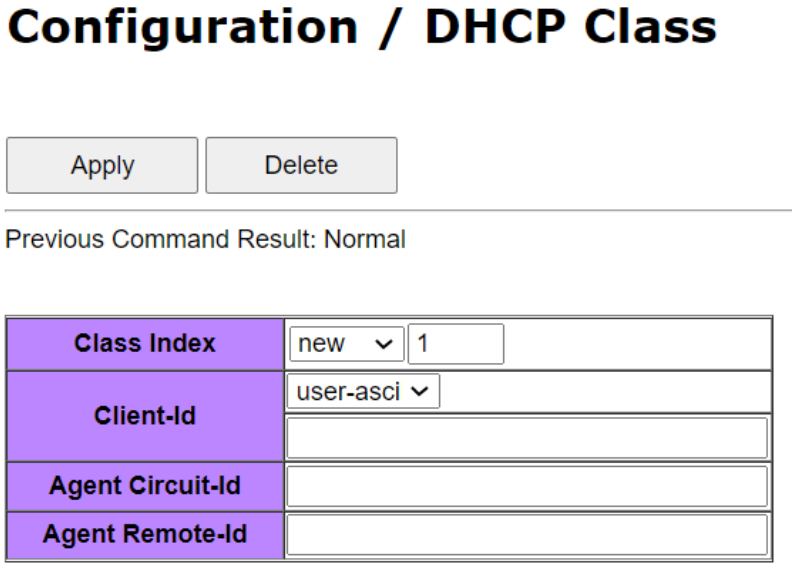
2.3.18 DHCP Server



Operation	Modify: Push "Modify" function to apply new configuration. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Apply: This button support "Creating" and "Modifying" function to configure the DHCP server pool. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failed. Delete: This button support "Deleting" function to delete the DHCP server pool. Choose the check-box of entry that are deleted and push "Delete" button to delete selected entries. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failed.
Field	Description
DHCP Server Mode	Support enabled of performing DHCP server on the local device. "Enabled" - DHCP server is enabled to perform on local device. "Disabled" - DHCP server is disabled to perform on local device
DHCP Server Status	Inform what status DHCP server is operating on. There are: Stop: DHCP server is unavailable now. It occurs when DHCP server mode is "disabled". Running: DHCP server is available now. It occurs when DHCP server mode is "enabled" and it can do normal DHCP-lease handshaking with client(s). Restarting: DHCP server is restarting now. It will stop DHCP-lease handshaking and reload all relevant database. It occurs when DHCP server mode is "enabled" and some DHCP configuration changes. Idle: DHCP server is idle now. DHCP server is shutdown temporally. It occurs when DHCP server mode is "enabled" and some internal error cause DHCP server work abnormal. And local DHCP server will stop operating until the error is solved.

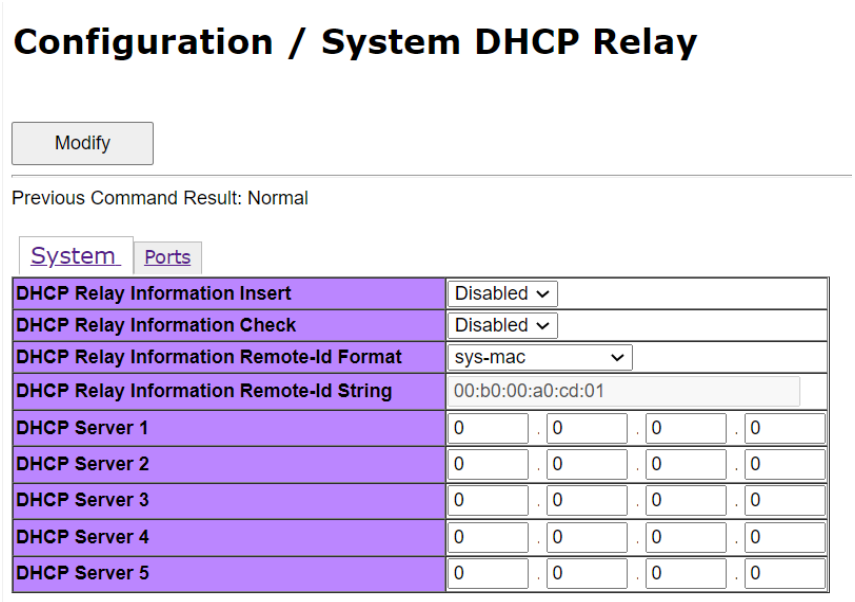
Network*	Network address and netmask. It should match IP address subnet of an existing specific VLAN interface.
Address Range (*)	It indicates available range of address for DHCP client. There are maximum 5 sets for multiple address range. To specify both start-IP and end-IP to allocate the address range. To specify only start-IP to allocate one address. Maximum DHCP Pool size is 1024 overall the system.
Default Router	Default-router in this network.
Domain Name	Domain name of this network. Max. length is 64 characters.
DNS	DNS server of this network.
Lease Time	Define the lease time for IP Address lease. (Range: 60 - 31536000 seconds, default is 86400 seconds)
Class Address	To allocate one or multiple IP address for the class.

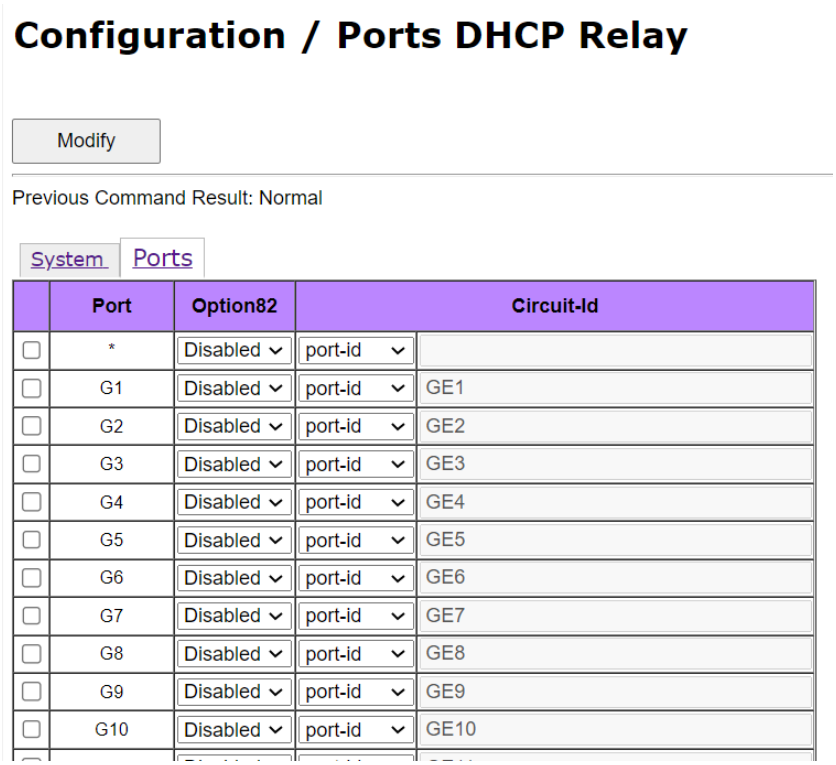
2.3.19 DHCP Class



Operation	Apply: This button support "Add" and "Modify" function to configure the DHCP class entry. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Delete: This button support "Delete" function to delete the DHCP class entry. Choose the check-box of entry that is deleted and push "Delete" button to delete this one. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Class Index	The number for identifying the index of this DHCP class entry. In case of "Creating", choose "new" option in a drop-down list with valid options. When this option is selected, one empty form is generated for user setting new DHCP class entry. In case of "Modifying" or "Deleting", choose id number in a drop-down list with valid options. One valid form is generated for user modifying or deleting this DHCP class entry.
Client-Id	Configure value of client identifier, that encapsulated in value field of optoin61. It provides three options to configure value of client identifier in different format. There are : "user-ascii" - It accepts all printable character of ASCII table, that range is from 1 to 32 . "hwaddr" - It accepts the common format of ethernet address. (Ex: 00:11:22:33:44:55) "user-hex" - It accepts hexadecimal octets, that range is from 1 to 32 in unit of 2 numbers.
Agent Circuit-Id	Configure value of agent circuit string, that encapsulated in 1st sub-option field of option82. It accepts any printable character of ASCII table, that range is from 1 to 32.
Agent Remote-Id	Configure value of agent remote string, that encapsulated in 2nd sub-option field of option82. It accepts any printable character of ASCII table, that range is from 1 to 32.

2.3.20 DHCP Relay

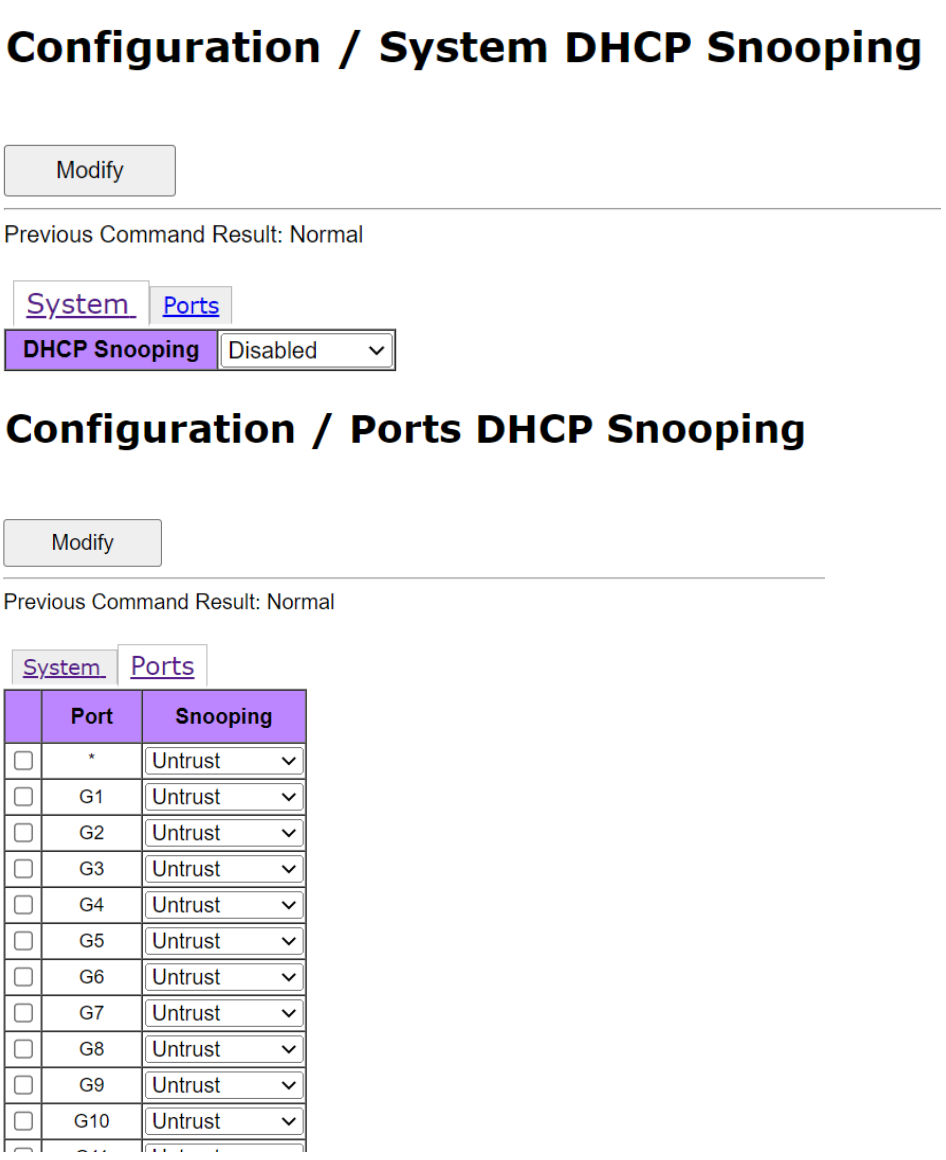




Operation	Push "Modify" button to apply new configuration when some fields' value change. Display "Success" when the changes are successfully applied. Display "Fail" when the changes are failed to applied.
Field	Description

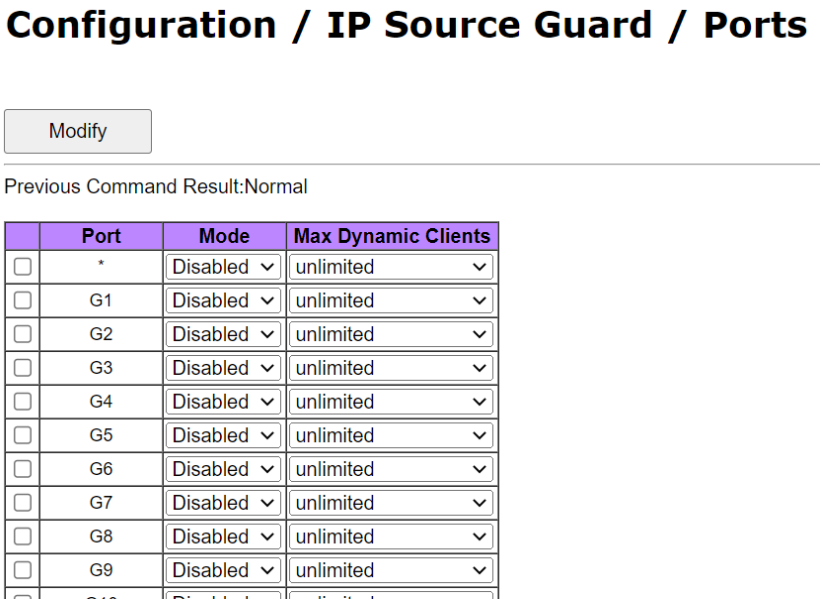
DHCP Relay Information Check	Enabled - Always check relay information of DHCP-Reply messages. Disable - Ignore relay information of DHCP-Reply messages.
DHCP Relay Information Insert	"Enabled" - When DHCP-request message is received on port where is enabled to append option82 field, it always appends remote-id of option82 field to this message. "Disable" - do not append anything.
DHCP Relay Information Remote-Id Format	Specify the remote-id is auto-generated based on specific rule or configured by user. "sys-mac" - use system mac-address as remote-id. "hostname" - use host-name string as remote-id. "ascii" - user can configure any printable ASCII characters in range of 1 to 32.
DHCP Relay Information Remote-Id String	When Remote-Id Format is "ascii", user can configure any printable ASCII characters in range of 1 to 32. When Remote-Id Format is others, the value of this field is auot-generated and it is read-only.
DHCP Server	Specify the DHCP relaying target for DHCP-request message. There are maximum of 5 remote DHCP servers.
Port	Port number.
Option82	Enable or Disable Option82 on the port. If disable option82, option61 would be used if DHCP client supports option61.
Circuit ID	This string could be specified by user or auto-generated (see description above). It is added to DHCP packet sent by DHCP client and then packet would be relayed to server side. When relay of port is disabled, this ID would be set to empty. Max length of character: 32.

2.3.21 DHCP Snooping



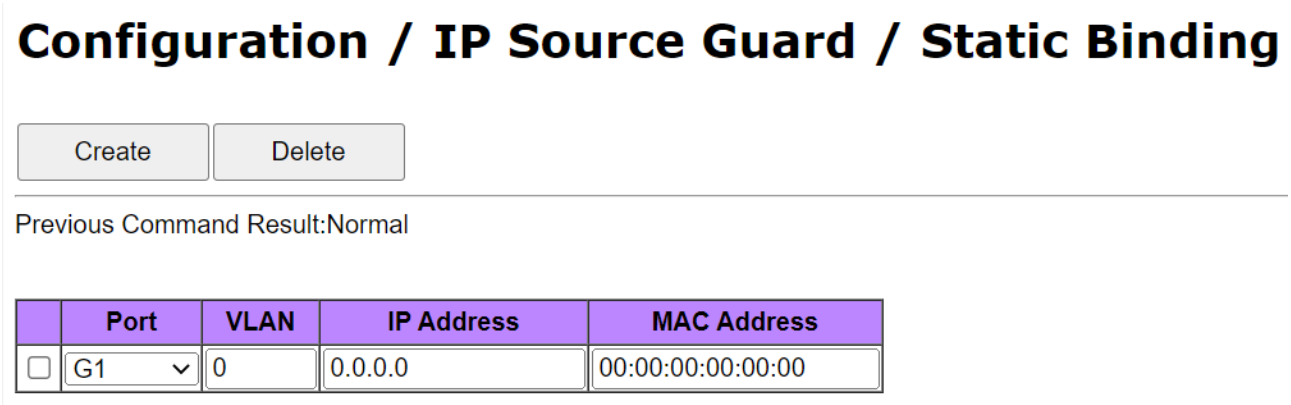
Operation	Modify: To Modify the DHCP Snooping configuration on the port.
Field	Description
DHCP Snooping	Control system's DHCP snooping Enabled or Disabled.
Port	Port number.
Snooping	Snooping Mode Trust: Configures the port as trusted source of the DHCP messages. Untrust: Configures the port as untrusted source of the DHCP messages.

2.3.22 IP Source Guard - Ports



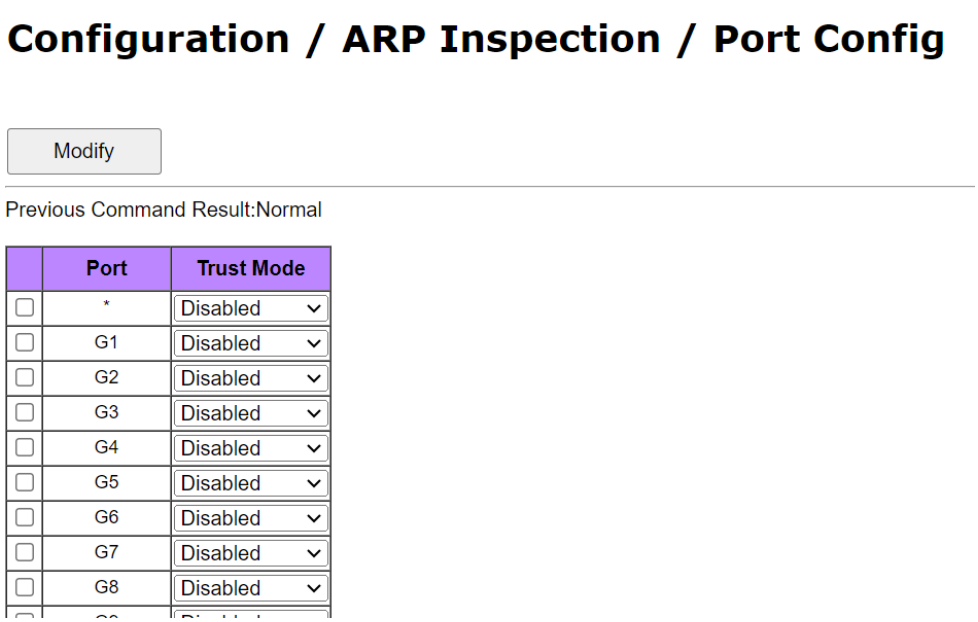
Operation	Modify: Push "Modify" button to apply new configuration for port(s) configuration. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Port	Specify the port identifier.
Mode	Perform this port to operate IP validation for the ingress packet. There are : "Enabled" - Enable operating IP validation. "Disabled" - Disable operating IP validation. (It is default.)
Max Dynamic Clients	This control the how many hosts allow to join IP validation table. The valid value is in range of 0 to 5. The default is unlimited that means port-based limitation is same with system-based.

2.3.23 IP Source Guard - Static Binding



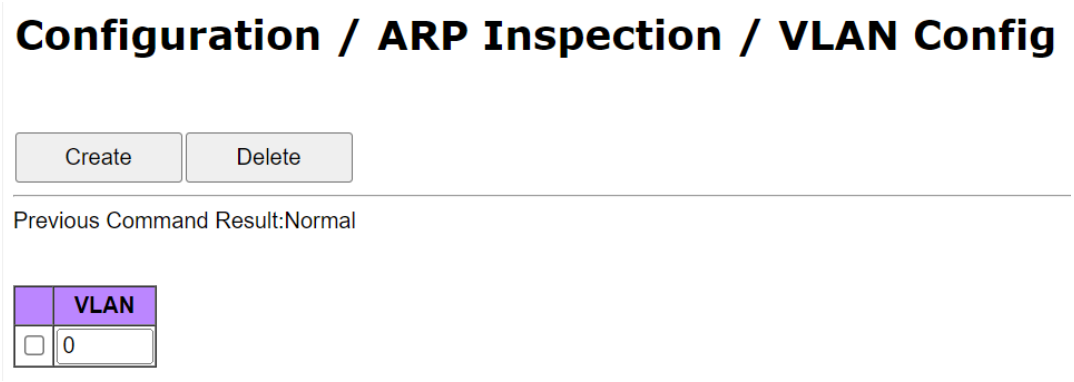
Operation	Create: Push "Create" button to create new binding entry. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Delete: Push "Delete" button to delete one or more static entries. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Port	Port for the static allowed entry.
VLAN	VLAN for the static allowed entry.
IP Address	Allowed IP address for the static binding entry. This field supports manual setting in format of dotted decimal notion. (ex: 192.168.100.1).
MAC Address	Allowed MAC address for the static binding entry. This field supports manual setting in format of colon hexadecimal notion. (ex: 00:11:22:33:44:55).

2.3.24 ARP Inspection – Port Config



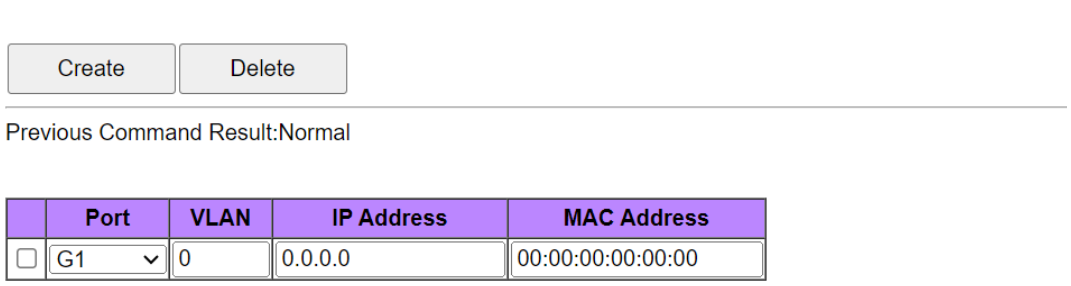
Operation	Modify: Push "Modify" button to apply new configuration for port(s) configuration. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Port	Specify the port identifier.
Trust Mode	Perform this port to operate ARP inspection for the ingress ARP. There are : "Enabled" - Disable ARP inspection operating since port is trusted. "Disabled" - Enable ARP inspection operating since port is not trusted. (It is default.) Note: It also need to consider if ARP inspection is enabled on ingress VLAN.

2.3.25 ARP Inspection – VLAN Config



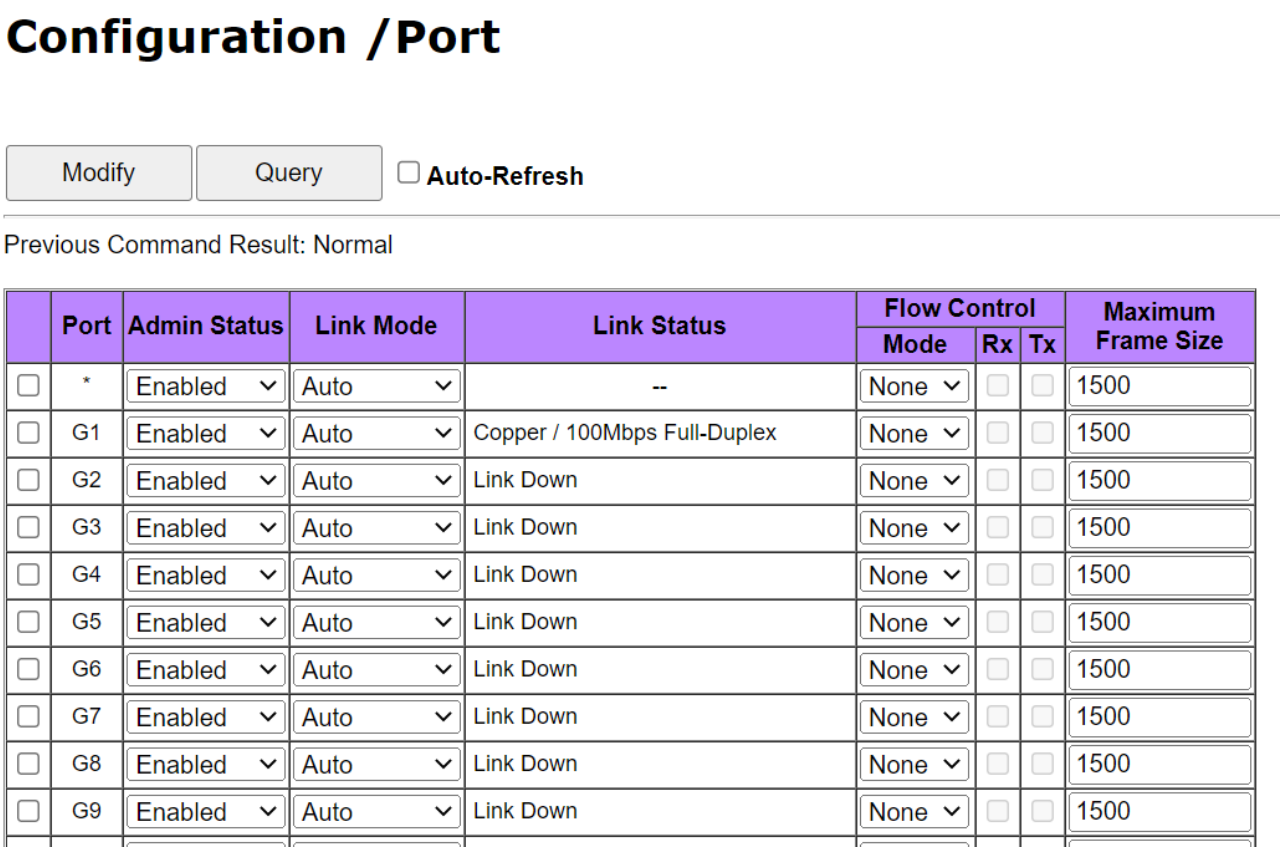
Operation	Create: Push "Create" button to enable ARP inspection for specific VLAN. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Delete: Push "Delete" button to disable one or more VLAN ARP inspection operating. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
VLAN	VLAN for operating ARP inspection.

2.3.26 ARP Inspection – Static Entry



Operation	Create: Push "Create" button to enable ARP inspection for specific VLAN. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Delete: Push "Delete" button to disable one or more VLAN ARP inspection operating. Display "Success" when previous operation succeed. Display "Fail" when previous operation is failure.
Field	Description
Port	Port for the static entry.
VLAN	VLAN for the static entry.
IP Address	Allowed IP address for the static entry. This field supports manual setting in format of dotted decimal notion. (ex: 192.168.100.1).
MAC Address	Allowed MAC address for the static entry. This field supports manual setting in format of colon hexadecimal notion. (ex: 00:11:22:33:44:55).

2.3.27 Port Configuration – Port

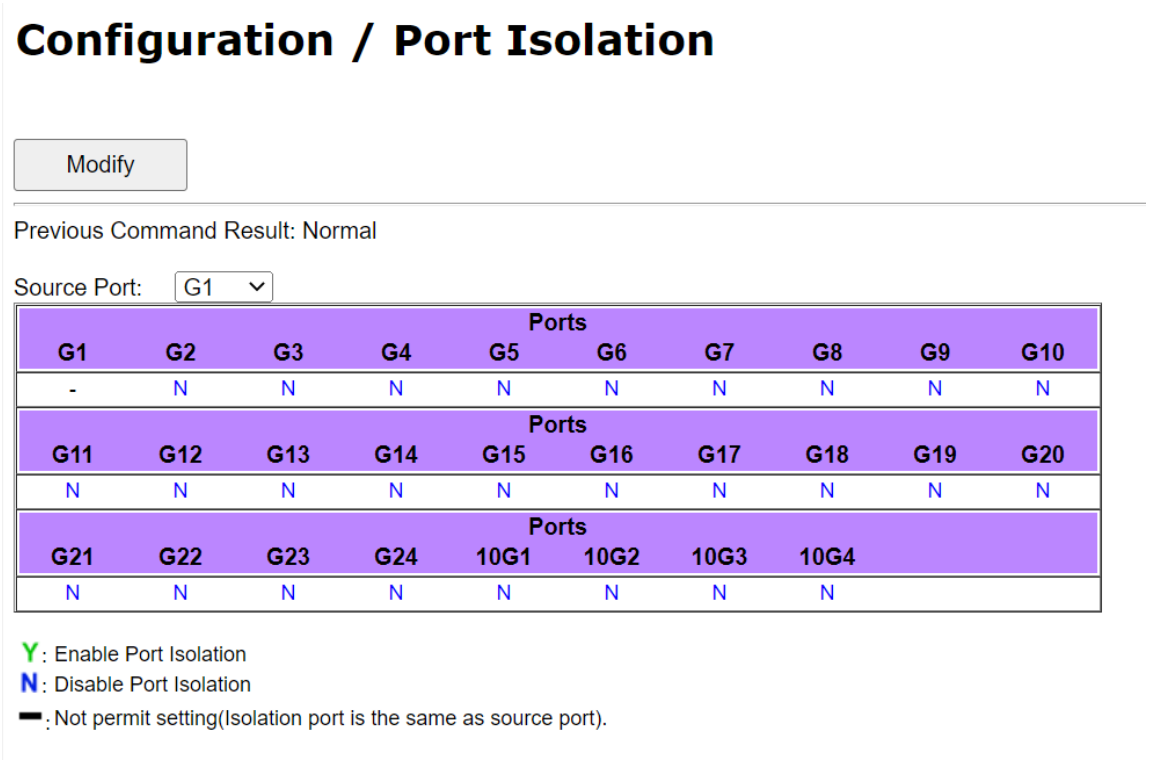


Operation	Modify: Push "Modify" button to apply new configuration for port(s) configuration. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Refresh: Push "Modify" button to refresh ports status.
Field	Description
Port	Specify the port identifier.
Admin Status	Perform this port as active or temporal shutdown. There are : "Enabled" - Port is active and operates auto-negotiation with link partner. (It is default.) "Disabled" - Port is shutdown and any communication is forbidden.

Link Mode	Specify what speed the port communicates with link partner. There are : "Auto Mode" - It always do auto-negotiation with link-partner to discovery the real link speed. The result of negotiation is shown in Link-Status filed. "Force Mode" - Specify the port operating on the fixed speed without any negotiation. For Fast-Ethernet port, there are options, include 10M/Half, 10M/Full, 100M/Half and 100M/Full. For Gigabit-Ethernet port, there are options, include 10M/Half, 10M/Full, 100M/Half, 100M/Full and 1000M/Full. Each option specifies both speed and duplex mode. For example, option of '100M/Full' indicates speed of 100Mbps with full-duplex mode.
Link Status	Specify the current link speed operating on the port. There are : G1 ~ G24 "Link Down" - Port is inactive. It could be physical link break or manually disabled. "10Mbps Half-Duplex" - Port is operating on speed of 10Mbps with half-duplex mode. "10Mbps Full-Duplex" - Port is operating on speed of 10Mbps with full-duplex mode. "100Mbps Half-Duplex" - Port is operating on speed of 100Mbps with half-duplex mode. "100Mbps Full-Duplex" - Port is operating on speed of 100Mbps with full-duplex mode. "1000Mbps Full-Duplex" - Port is operating on speed of 1000Mbps with full-duplex mode. 10G1 ~ 10G4 "Link Down" - Port is inactive. It could be physical link break or manually disabled. "1G Full-Duplex" - Port is operating on speed of 1G with full-duplex mode. "2.5G Full-Duplex" - Port is operating on speed of 2.5G with full-duplex mode. "10G Full-Duplex" - Port is operating on speed of 10G with full-duplex mode.

Flow Control	Specify how the flow-control operates on this port. There are three parameters for informing current flow-control state on this port. There are : "Mode" - This field is used to specify how to control flow-control on this port, include: None - No flow-control operates on this port. Force - Provide manual control for unique or both directions. Auto - Perform flow-control auto negotiation with link-partner. The flow-control operation is depending on result of negotiation, the defined in Table28B-4 of IEEE-802.3-Annex.28B. Both bits of 'PAUSE' and 'ASM_DIR' are advertised for the procedure of pause resolution. "Rx" - Inform the flow-control operating on rx-direction for this port. When mode is 'None', this field is disabled. When mode is 'Force', user can configure this parameter to determine if operates flow-control on rx-direction. It means receiving of 'PAUSE' frame(s) is accepted or forbidden on this port. When mode is 'Auto', this field is read-only for informing the result of negotiation with link-partner. "Tx" - Inform the flow-control operating on tx-direction for this port. When mode is 'None', this field is disabled. When mode is 'Force', user can configure this parameter to determine if operates flow-control on tx-direction. It means transmission of 'PAUSE' frame(s) is accepted or forbidden on this port. When mode is 'Auto', this field is read-only for informing the result of negotiation with link-partner.
Maximum Frame Size	The maximum frame size received on this port, including 4 bytes CRC. This value must be even. When odd number is specified, it will be tuned up to even number automatically. That valid size is in range of 64 to 10240, which unit is byte. The default is 1500.

2.3.28 Port Configuration – Port Isolation



Configuration / Port Isolation

Modify

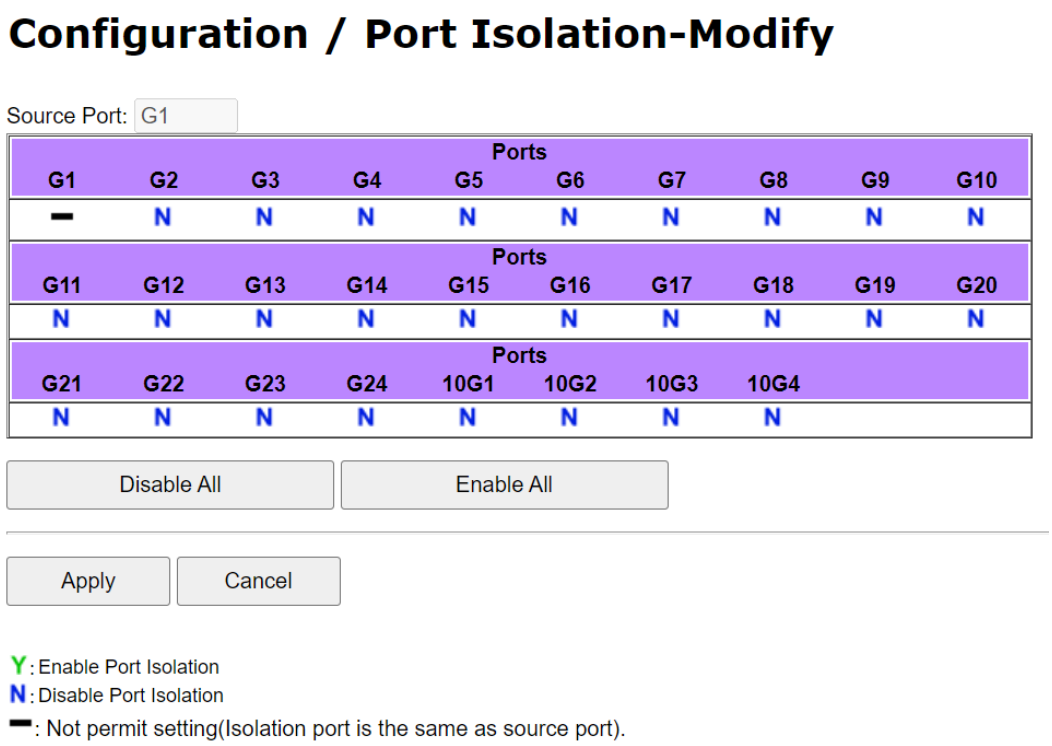
Previous Command Result: Normal

Source Port: G1

Ports									
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
-	N	N	N	N	N	N	N	N	N
Ports									
G11	G12	G13	G14	G15	G16	G17	G18	G19	G20
N	N	N	N	N	N	N	N	N	N
Ports									
G21	G22	G23	G24	10G1	10G2	10G3	10G4		
N	N	N	N	N	N	N	N		

Y: Enable Port Isolation
N: Disable Port Isolation
-: Not permit setting(Isolation port is the same as source port).

Port Isolation-Modify



Configuration / Port Isolation-Modify

Source Port: G1

Ports									
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10
-	N	N	N	N	N	N	N	N	N
Ports									
G11	G12	G13	G14	G15	G16	G17	G18	G19	G20
N	N	N	N	N	N	N	N	N	N
Ports									
G21	G22	G23	G24	10G1	10G2	10G3	10G4		
N	N	N	N	N	N	N	N		

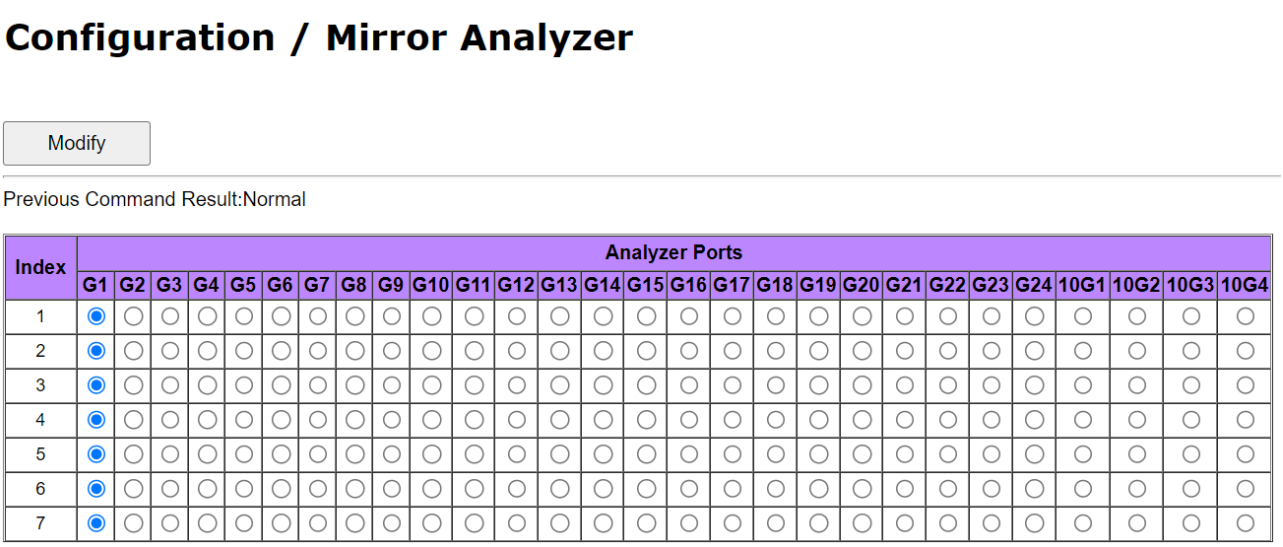
Disable All | Enable All

Apply | Cancel

Y: Enable Port Isolation
N: Disable Port Isolation
-: Not permit setting(Isolation port is the same as source port).

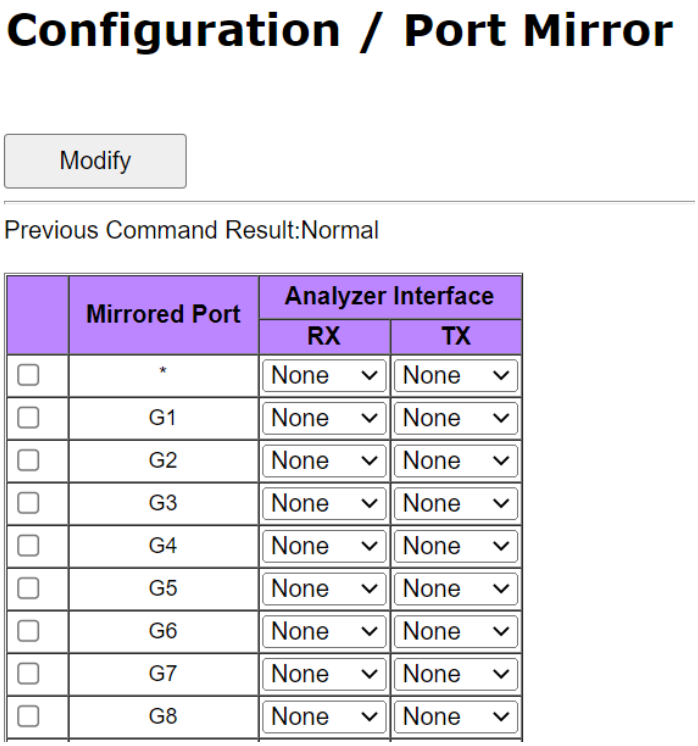
Operation	Modify: Click “Modify” button to open modification page. Port Isolation - Modify: 1. Click “Disable All”, ”Enable All” or click on (Y/N/-) to change isolation setting by port. 2. Click “Apply” to apply change or Press “Cancel” to cancel and go back to main page of Isolation.
Field	Description
Source Port	Port range: G1 ~ G24, 10G1 ~ 10G4.
Isolation Port	Range: Y/ N/ -. Y:Isolation is true N:Isolation is false -:Not permit setting (Isolation port is the same as source port)
Disable All	Disable Isolation to all ports
Enable All	Enable Isolation to all ports

2.3.29 Traffic Mirroring – Analyzer



Operation	Push "Modify" button to apply new configuration when some fields' value change. Display "Success" when the changes are successfully applied. Display "Fail" when the changes are failed to applied.
Field	Description
Index	The index to identify the number of one analyzer interface.
Analyzer Ports	Configure one physical port as output port of analyzer interface.

2.3.30 Traffic Mirroring – Ports



Operation	Push "Modify" button to apply new configuration when some fields' value change. Display "Success" when the changes are successfully applied. Display "Fail" when the changes are failed to applied.
Field	Description
Index	The index to identify the number of one analyzer interface. There are 7 analyzer interfaces for mirrored port binding on unique direction. Or binding 'none' on one direction of the port to disable mirroring.
Mirrored Ports	Provides per-port traffic mirroring on both RX and TX direction. It can bind different analyzer interface on RX and TX direction, or just disable one direction mirroring. (Note: The analyzer port must be different from the mirrored port.)

2.3.31 RingV2

Configuration / RingV2

Modify

Previous Command Result: Normal

Index	Group Id	Mode	Role	Transmission	Ring Port(s)		Auto Ring			
					Node1	Node2	Priority	Interval (100ms)	Skew Interval (100ms)	Preempt
1	1	Disabled	Ring(Slave)		G1	G2	0	50	50	Enabled
2	2	Disabled	Ring(Slave)		G3	G4	0	50	50	Enabled
3	3	Disabled	Chain (Member)		G1	G2	-	-	-	-
4	4	Disabled	Coupling(Backup)	All	G5		-	-	-	-
5	5	Disabled	Coupling(Backup)	All	G6		-	-	-	-
6	6	Disabled	Coupling(Backup)	All	G7		-	-	-	-
7	7	Disabled	Coupling(Backup)	All	G8		-	-	-	-
8	8	Disabled	Coupling(Backup)	All	G9		-	-	-	-

Operation	To Modify RingV2: 1. Set or select the following fields. 2. Click "Modify" button to modify data.
Field	Description
Index	The group index. It indicates this ring group that the index of all ring groups.
Group ID	The group identifier that is used to make all devices on the ring topology to identify receiving ring frame belonged to which ring group. This could avoid confusing among multiple ring groups on the network. This group identifier must be unique on the device. By default, group identifier is same with group index. User can configure this parameter in range of 1 to 128.

Mode	Enable Ring on the specific group. Please notes following rules. They could cause the failure situation happens. (1)Ring group can not coexist with chain group. When one ring or chain group is enabled, another type group will fail to enable. (2)Coupling group can not coexist with chain group. When one coupling or chain group is enabled, another type group will fail to enable. (3)Coupling group must run within ring group. When at least valid ring group is running, or it will fail to enable coupling group. If no any ring group is running, all running coupling group(s) will be automatically removed. (4)Ring group port must be unique. It is forbidden that port is configured as node1 and node2 of the group or shared by different groups. (5)Ringv2 and STP can not coexist. When one is enabled, another is failed to enable.
Role	Configure the Ring group on this switch as specific role. ## Ring Group ## It is normal ring topology. The ring topology is composed of one master and at least one slave. There are 3 role types, include: Ring-Master: It is responsible of loop protection function. There are 2 ring ports, one is normal port and it is in forwarding state; another one is protected port and it is in blocking for doing loop protection when ring topology is normal. When ring topology is failure, protect port's state will transit to forward. Ring-Slave: All devices except to master on the ring topology are slave. It has 2 ring ports; both are normal port and in forwarding state. Ring-Auto: It supports dynamically ring-master election. - When ring topology is in normal state, the ring device which owns highest priority will win the election to be the auto-master. The others which lost the election will be auto-slave. - When ring topology is failure, the device is always auto-slave since signal failure happens, all ring ports should be forwarding. ## Coupling group ## It can connect to non-ringv2 aware device.

	The coupling topology is composed of one coupling-primary and one coupling-backup. There are 2 role types, include: Coupling-Primary: It is primary role of coupling topology. It only has one coupling port connected to non-ringv2 aware device, this port is in forwarding state. Coupling-Backup: It is backup role of coupling topology. It also has one coupling port connected to non-ringv2 aware device. When primary role is normal, the coupling port is in blocking state. When primary role is failure or primary device is failure, the coupling port will transit to forward state. ## Dual-Homing ## It maintains 2 ports connected to 2 non-ringv2 aware devices, one port is normal port and in forwarding state and another is backup port and in blocking state. When normal port is failure, backup port will transit to forward. ## Chain Group ## The chain is like half-ring, there are 2 chain devices it connected to non-ringv2 aware devices. There are 3 role types, include: Chain-Head: The device that directly connects to non-ringv2 aware device is called chain-head or chain-tail. The chain-head maintain one normal port that connect to non-ringv2 aware device and another port connect to ringv2 aware device (called chain-member). The chain-tail maintain one backup port that connect to non-ringv2 aware device and another port connect to ringv2 aware device (called chain-member). Chain-Tail: Check description of Chain-head. There are some situations that backup port could transit to forward. a.The normal port of chain-head is failure or the chain-head device is failure. b.The normal port of chain-member is failure or some chain-member device(s) are failure. c.The normal port of chain-tail is failure. Chain-Member: All devices of chain topology, except to Chain-Head and Chain-Tail, are Chain-Member. It maintains 2 normal ports and both are in forwarding state. ## Balancing Chain Group ##

	The balancing chain is enhanced chain. It could achieve purpose of traffic balancing on chain topology. There are 4 role types, include: Balancing Chain Central Block: Balancing-Chain-Central-Block is responsible of doing traffic balancing. It maintains 2 chain ports; When balancing chain topology is normal, one is normal port and in forwarding port, another is backup port and in blocking state. When balancing chain topology is failure, the backup port's state will transit to forward. Balancing Chain Terminal 1/2: The balancing chain device also support capability of connecting to non-ringv2 aware device. The device that connects to non-ringv2 aware device is called Balancing-Chain-Terminal. There are 2 devices directly connected to non-ringv2 aware devices, one is called Balancing-Chain-Terminal-1 and another is called Balancing-Chain-Terminal-2. Both terminal devices also maintain 2 normal ports and both are in forwarding state. Balancing Chain Member: All devices of balancing chain topology, except to Balancing-Chain-Central-Block and Balancing-Chain-Terminal-1/2, are Balancing-Chain-Member. It maintains 2 normal ports and both are in forwarding state.
Transmission	Control diag packet transmission direction. Please notes following rules. They could cause the failure situation happens. (1)When Coupling ring port connect to ring structure . Transmission should be set to 'Inside'. (2)When Coupling ring port connect to any structure except ring. Transmission should be set to 'Outside'. (3)When Coupling ring port connect to ring structure and others structure at the same time. Transmission should be set to 'All'.

Ring Port(s)	Selecting ring port(s). Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring/chain CANNOT be the same. # When role is ring/master: One ring port is forward port and another is blocking port. The block port is redundant port; it is blocking port in normal state. # When role is ring/slave: Both ring ports are forward port. # When role is coupling/primary: Only need one ring port named primary port. # When role is coupling/backup: Only need one ring port named backup port. This backup port is redundant port; it is blocking port in normal state. # When role is dual-homing: One ring port is primary port and another is backup port. This backup port is redundant port; it is blocking port in normal state. # When role is chain/head: One ring port is member port and another is head port. Both ring ports are forwarding port in normal state. # When role is chain/tail: One ring port is member port and another is tail port. The tail port is redundant port; it is blocking port in normal state. # When role is chain/member: Both ring ports are member port. Both ring ports are forwarding port in normal state. # When role is balancing-chain/central-block: One ring port is member port and another is blocking port. The block port is redundant port; it is blocking port in normal state. # When role is balancing-chain/terminal-1/2: One ring port is member port and another is terminal port. Both ring ports are forwarding port in normal state. # When role is balancing-chain/member: Both ring ports are member port. Both ring ports are forwarding port in normal state.

Priority	This field is only available while ring-auto is setting on the ring group. It is used to decide which ring device will win the election of auto-master. The higher value means higher priority than other ring devices. When both ring devices have same priority, the MAC address of the devices will be referenced. Also, the MAC address is higher means higher priority.
Interval	This field is only available while ring-auto role is setting on the ring group. When ring-auto is configured, the ring device always generates periodic ring-discovery message and flood to ring-topology to join the election of auto-master. The periodic time is assigned by this parameter. This parameter can be setting in range of <1-600>, which unit is 100ms. The default value is 50.
Skew Interval	This field is only available while ring-auto is setting on the ring group. After ring device lost the election of auto-master, it records brief information of current auto-master, include device's address, priority and aging time. The aging time is refreshed per receiving ring-discovery of auto-master. If the aging time is not be refreshed and expired, the ring device which lost last election may process election again since auto-master may be dead and need one new auto-master. Per aging time of auto-master is calculated by following formula : aging time = discovery-interval + skew-interval. This parameter can be setting in range of <5-600>, which unit is 100ms. The default value is 50.
Preempt	This field is only available while ring-auto is setting on the ring group. When it is disabled, it means ring device which is elected to be auto-master can not be preempted till it is down. When it is enabled, it means ring device which is elected to be auto-master can be preempted by the device with higher priority.

2.3.32 LLDP

Configuration / LLDP

Modify

Previous Command Result: Normal

LLDP Parameters

Tx Interval	5	seconds
Tx Hold	4	times
Tx Reinit	2	seconds
Tx Delay	1	seconds

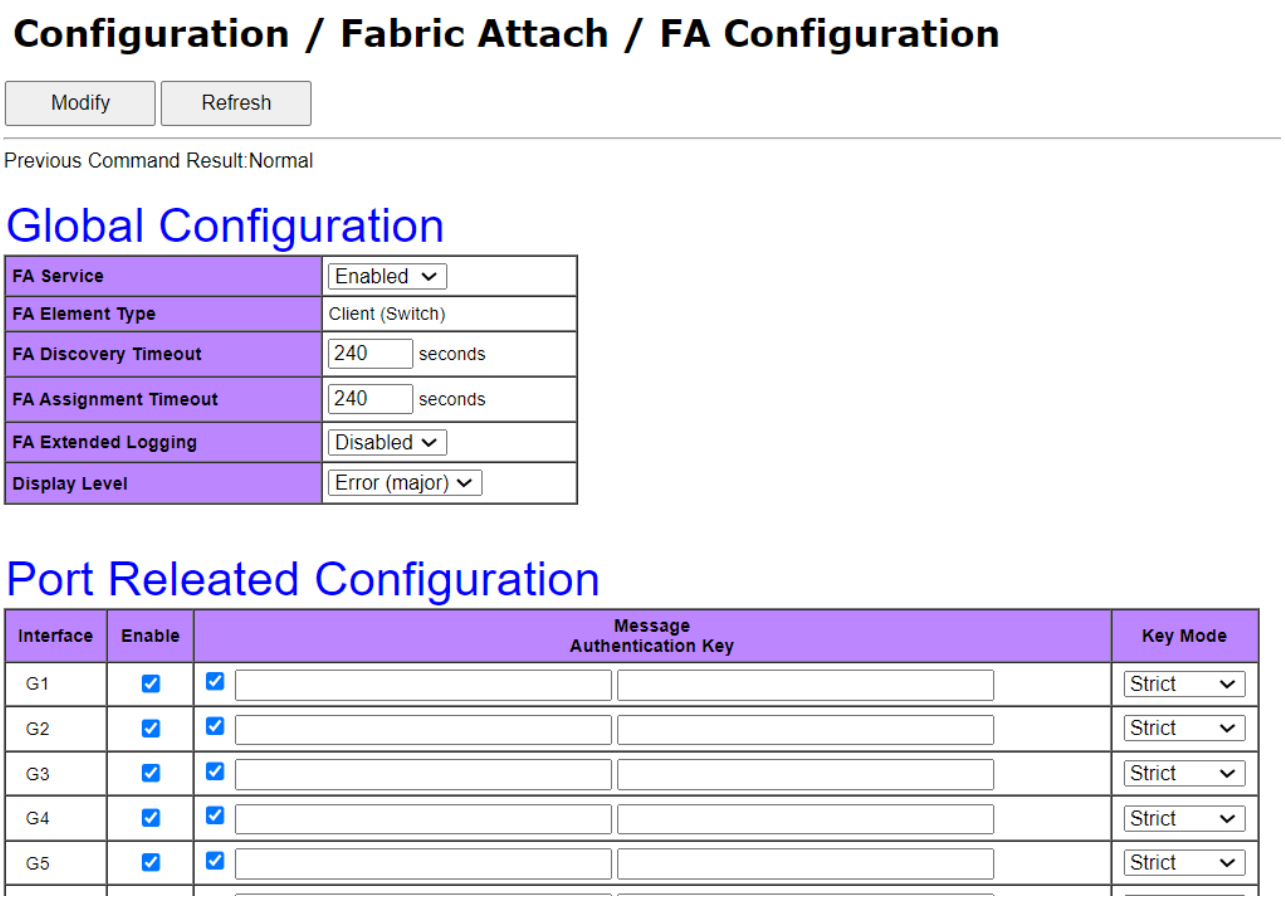
LLDP Port Configuration

	Port	Mode
☐	G1	Disabled
☐	G2	Disabled
☐	G3	Disabled
☐	G4	Disabled
☐	G5	Disabled
☐	G6	Disabled

Operation	<u>To modify LLDP Parameters:</u> 1.Modify the following fields: 2.Click "Modify" button to apply change. <u>To modify LLDP Port Configuration:</u> 1.Select Port check box. 2.Select Mode Disabled/ Enabled. 3.Click "Modify" button to apply change.
Field	Description
Tx Interval	The interval at which LLDP frames are transmitted on behalf of this LLDP agent. Range: 5 - 32768 seconds, Default value = 5 seconds.
Tx Hold	The time-to-live value expressed as a multiple of the TxInterval object. Range: 2 - 10 times, Default value = 4 times.
Tx Reinit	The TxReinit indicates the delay (in units of seconds) from when PortConfigAdminStatus object of a particular port becomes 'disabled' until re-initialization will be attempted. Range: 1 - 10 seconds, Default value = 2 seconds.

Tx Delay	The TxDelay indicates the delay (in units of seconds) between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. Range: 1 - 8192 seconds, Default value = 1 seconds.
Port	LLDP Port: Port-1 - MAX Number of Port.
Mode	Enable/Disable LLDP mode. Default value is Disabled.

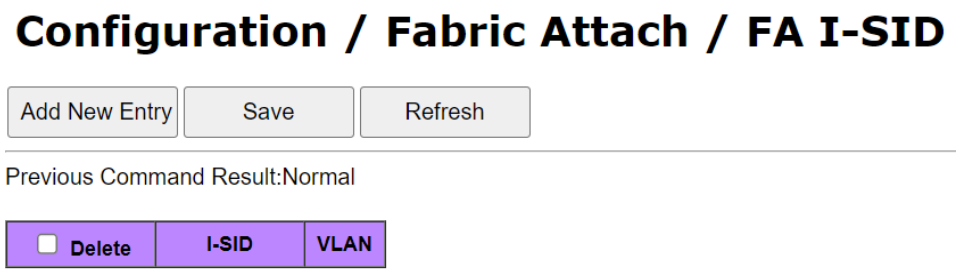
2.3.33 Fabric Attach - FA Configuration



Operation	Modify: Push "Modify" button to apply the changes. Display "Success" when previous operation succeed. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
FA Service	Valid Range: Disabled, Enabled, default value: Enabled
FA Element Type	Read-Only
FA Discovery Timeout	Valid Range: 45 ~ 480 seconds, default value: 240
FA Assignment Timeout	Valid Range: 45 ~ 480 seconds, default value: 240

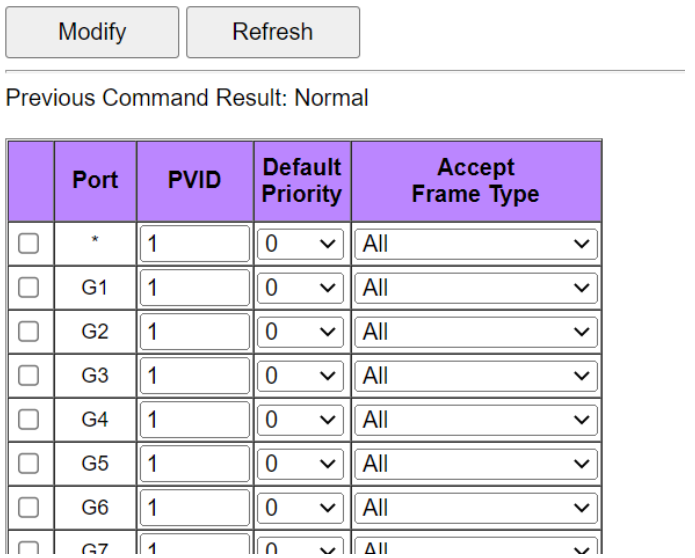
FA Extended Logging	Valid Range: Disabled, Enabled, default value: Disabled
Display Level	Valid Range: Error (major) / Error (minor) / Warning / Notice / Information, default value: Error (major)
Interface	The name of the interface
Enable	Uncheck the box for Disabled, check to box for Enabled, default value: Checked
Message Authentication Key	Check the checkbox to enable message authentication, the key is 0 ~ 32 characters, please input the same key in the confirm text box
Key Mode	Valid Range: Strict, Standard, default value: Strict

2.3.34 Fabric Attach - FA I-SID



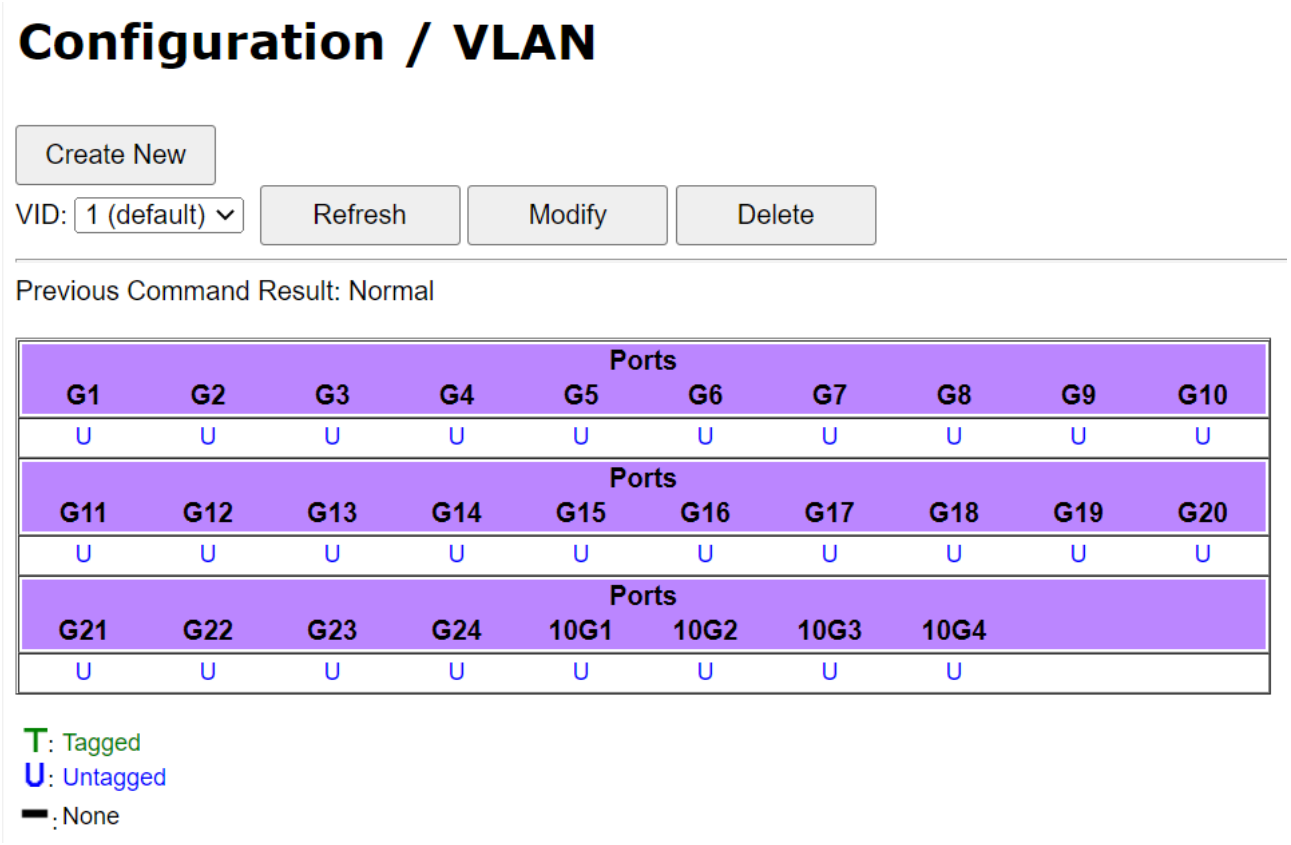
Operation	Add New Entry: Push "Add New Entry" button to edit the new entry. Push "Delete" button to remove the new entry. Up to 94 entries can be created. Each submit can add only one entry at one time. Save: Push "Save" button to apply the changes. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Refresh: Push "Refresh" button to refresh the page.
Field	Description
I-SID	I-SID of the mapping, Valid Range: 1 ~ 16777214
VLAN	VLAN ID of the mapping, Valid Range: 1 ~ 4094

2.3.35 VLAN Configuration - Ports



Operation	To Modify a Port: 1. Enter or select the following fields 2. Click "Modify" button to update.
Field	Description
Port	This parameter is a bridge port number.
PVID	Value:1~4094. Default value is 1.
Default Priority	Default Priority value: 0~7. Default is 0.
Accept Frame Type	Range: All/ OnlyVlanTagged/ Only Untagged. Default is All.

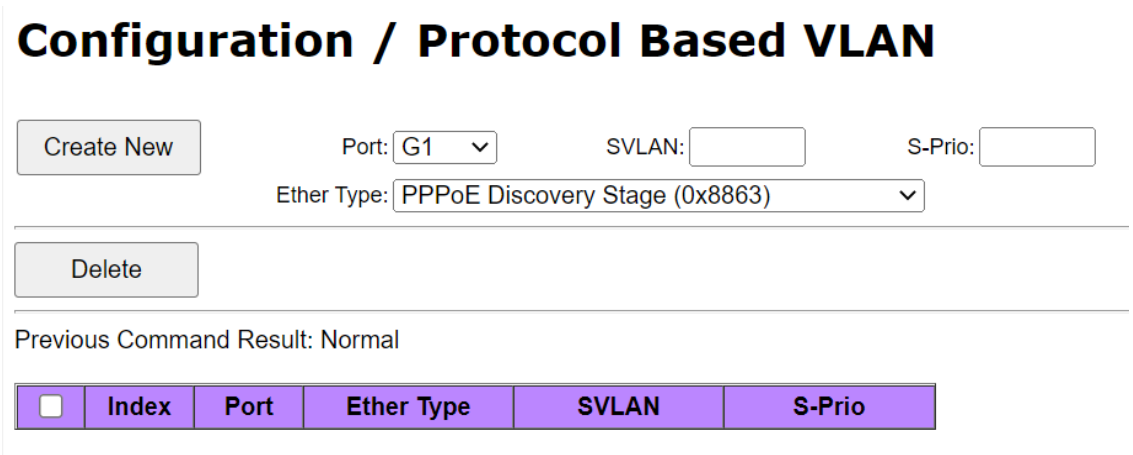
2.3.36 VLAN Configuration - VLAN



Operation	<u>Create New:</u> 1. Click “Create New” button to create a new VLAN with VLAN name. 2. Set VID and Name. 3. Select Member Port with Tagged or Untagged, or unselect (dash). 4. Click “Apply” button to create, or click “Cancel” button to cancel. <u>Modify:</u> 1. Click “Modify” button to open “Modify” page. 2. Modify Name or member port. 3. Click “Apply” button to modify, click “Cancel” button to cancel. <u>Delete:</u> 1. Choice VLANs checkbox to select.

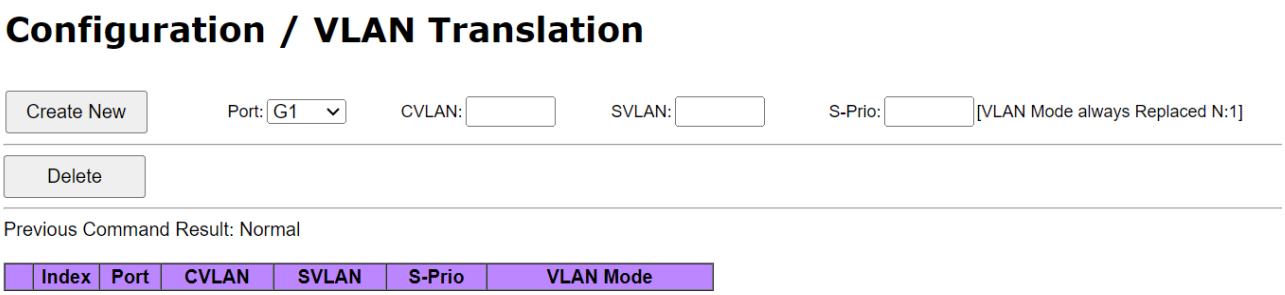
	2. Click “Delete” to delete selected VLAN(s). Refresh: 1. Click “Refresh” button to get current data.
Field	Description
VID	Value: 1~4094. Default value is 1.
Name	Range:0~32 characters
Tagged	Range: T/ U/ －. T: Tagged U: Untagged －: None (not join this VLAN)
Set All Ports to None	Set all ports to None (no port joins this VLAN) －
Set All Ports to Tagged	Set all ports join the VLAN as Tagged. T
Set All Ports to Untagged	Set all ports join the VLAN as Untagged. U

2.3.37 Protocol-Based VLAN



Operation	Create New: 1. Click "Create New" button to Create New page. 2. Set Port and Ether Type, input SVLAN and S-Prio. 3. Click Create New button. (Max entry: 10.) Delete: 1. Select Index with check box. 2. Click "Delete" button to delete selected data.
Field	Description
Index	Index 1~20.
Port	Protocol-base VLAN config port number, Port range:G1 ~ G24, 10G1 ~ 10G4.
Ether Type	Select Ether Type: 1. PPPoE Discovery Stage (0x8863). 2. PPPoE Session Stage (0x8864). 3. Internet Protocol (0x0800). 4. Address Resolution Protocol (ARP) (0x0806). 5. Others (input ether type), Range 0000~FFFF.
SVLAN	Service VLAN ID, Range 1 ~ 4094
S-Prio	CoS of SVLAN: Range 0~7, 8:reserve ingress priority

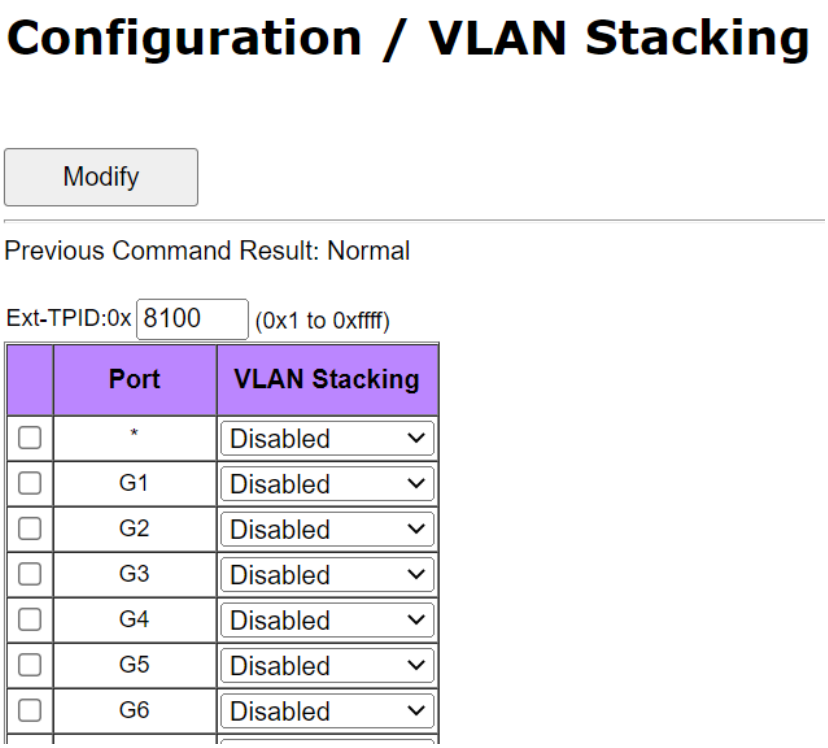
2.3.38 VLAN Translation



Operation	Create:

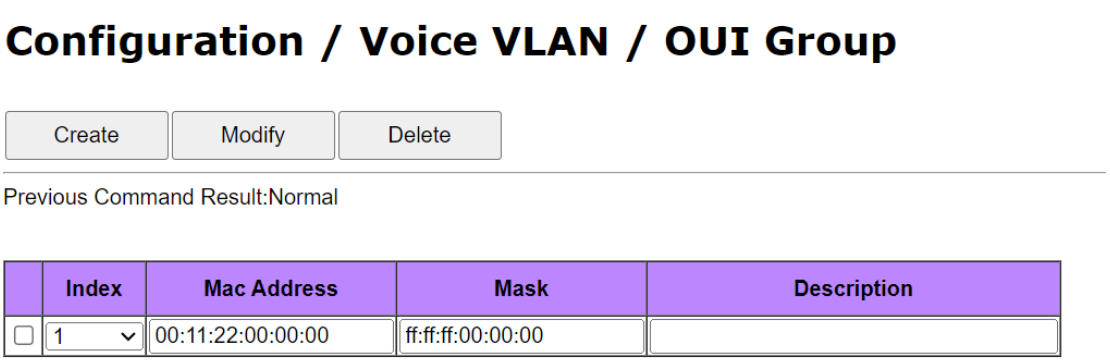
	1. Select Port, fill CVLAN, C-Prio, SVLAN and S-Prio. 2. Click "Create New" button to create new entry. Click Delete button to delete selected entry(s).
Field	Description
Index	Index 1~20, max entry: 20.
Port	VLAN translation port number: Port range:G1 ~ G24, 10G1 ~ 10G4.
CVLAN	Customer VLAN ID: Range: 1 ~ 4094
SVLAN	Service VLAN ID: Range: 1 ~ 4094
S-Prio	CoS of SVLAN: Range 0~7, 8:reserve ingress priority
VLAN Mode	Currently only supports: Replaced N to 1.

2.3.39 VLAN Stacking



Operation	Modify: 1. Select Port check box 2. Select Stacking Disabled/ Enabled, click "Modify" button to apply change.
Field	Description
Ext-TPID (Hex)	The range is from 1~FFFF (0x1 to 0xffff) Default is 0x8100
VLAN Stacking Port	Port: G1 ~ G24, 10G1 ~ 10G4.
VLAN Stacking	Enable/Disable VLAN Stacking (QinQ) mode. Default value is disable.

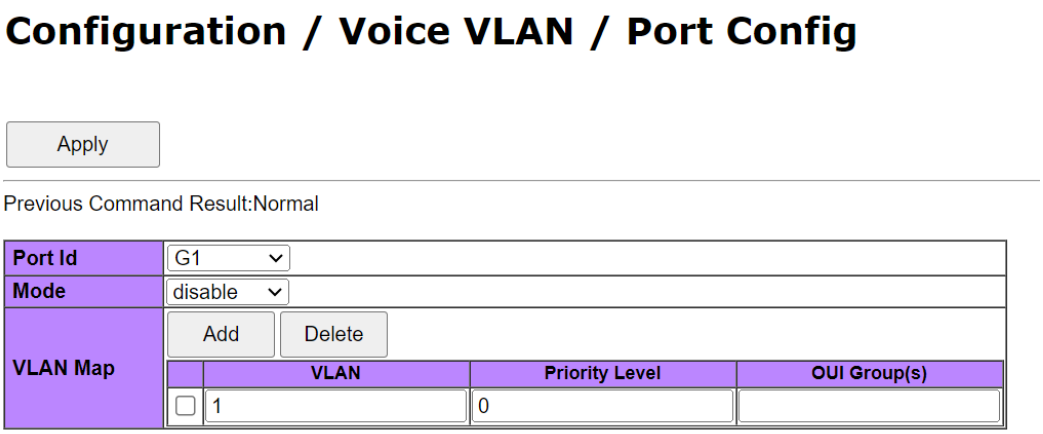
2.3.40 Voice VLAN – OUI Group



Operation	Create New: Input valid value in first row fields and then push "Create" button to create one OUI address group. Display "Success" when new OUI address group is successfully created. Display "Fail" when new OUI address group is failed to be created. Modify: Choose the check-box of OUI address groups that are modified and then push "Modify" button to apply these changes. Display "Success" when changes are successfully applied. Display "Fail" when changes are failed to be applied. Delete: Choose the check-box of OUI address group that are deleted and then push "Delete" button to delete these ones. Display "Success" when selected OUI address groups are successfully deleted. Display "Fail" when selected OUI address groups are not completely deleted.
Field	Description
Index	Specify the index for identifying a OUI address group. In case of "Creating", select one unused index for new group. In others case, this field is read-only.
MAC Address	Specify MAC address for this OUI address group. This field only supports the setting in format of colon hexadecimal notion. (ex: 00:11:22:33:44:55).

Mask	Specifies the valid length of the OUI address by using a mask in the format of colon hexadecimal notion. (ex: ff:ff:ff:00:00:00).
Description	Specify the OUI address description, a string of 0 to 32 characters.

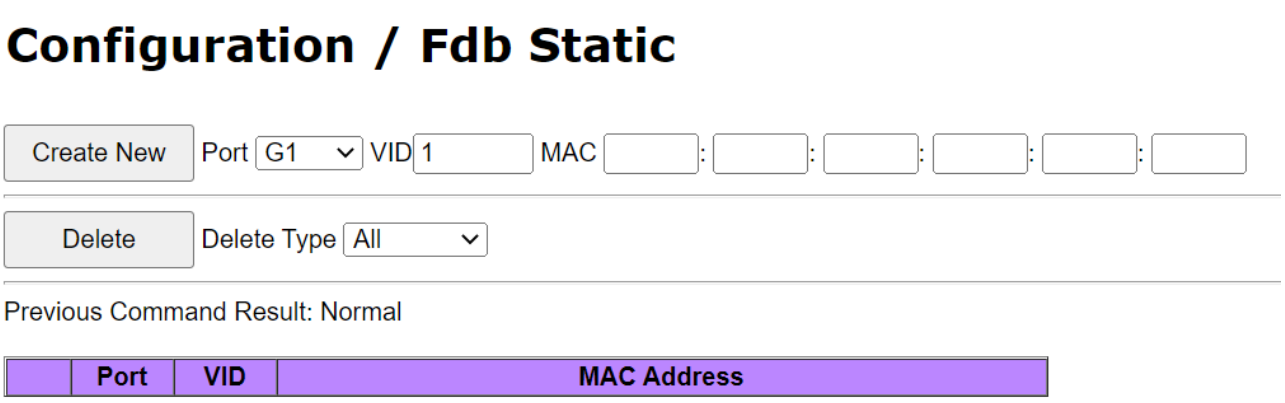
2.3.41 Voice VLAN – Port Config



Operation	Apply: This always apply current setting to replace old existed configuration.
Field	Description
Port Id	The simple description to identify one port. Select one port in a drop-down list to set voice configuration of this port.
Mode	Configure this parameter to indicate voice VLAN lookup behavior. There are : Disable - Disable voice VLAN operation on this port. Mac - Enable MAC address-based voice VLAN lookup for all voice traffic received on the port. This suppose voice traffic is untagged and it always use OUI address to differentiate voice and data traffic. When source MAC address of received voice traffic is identified by OUI address table, both specific VLAN and priority are attached on traffic. Others data traffic will follow normal VLAN lookup behavior (ex: Port-Based VLAN). Vlan - Enable VLAN based voice VLAN lookup. This suppose voice traffic is VLAN-tagged. When voice traffic is identified by VLAN map table, it will be remarked by

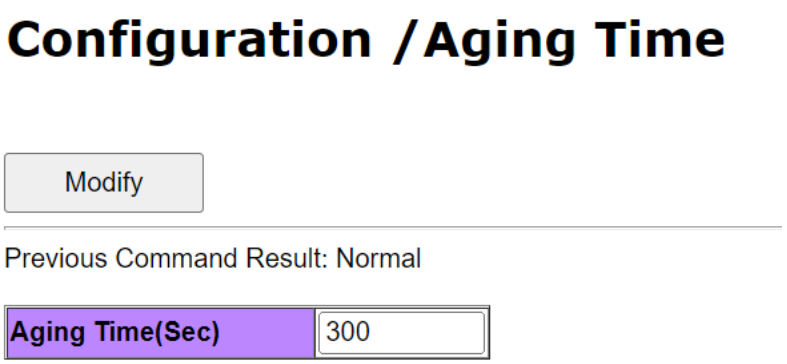
	higher priority level.
VLAN Map	Specify the VLAN what voice traffic is mapped to. Each port supports maximum 4 VLAN number to identify different voice traffic. Each VLAN support 3 parameters to do this identification. There are: VLAN - The VLAN that voice traffic is mapped to. Priority - The priority level what voice traffic is remarked. OUI Groups - Specify what OUI address is referring to identify the voice traffic. This field is only available when mode is "Mac".

2.3.42 MAC Learning & Forwarding – Fdb Static



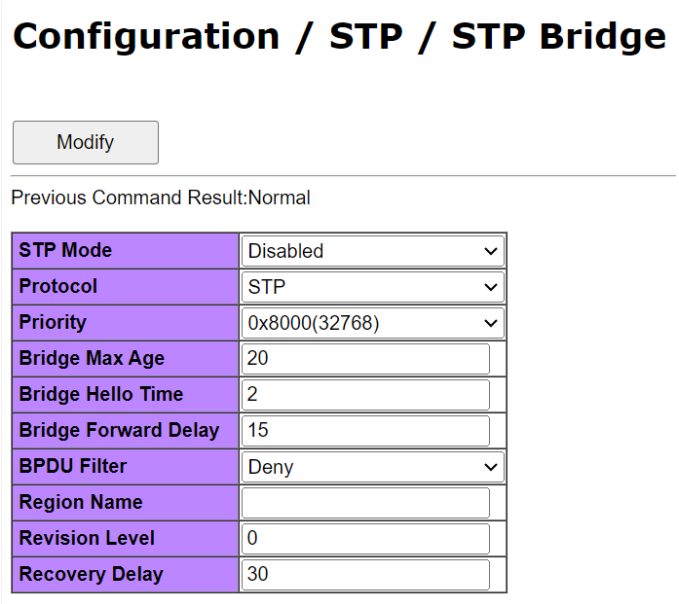
Operation	Create New: 1. Setting Port, VID and MAC Address 2. Click “Create New” to create a new data Delete: 1. Select a delete type “All/Port/VID/Selected” 2. If delete type is “Port”, then select a port from list. 3. If delete type is “VID”, then input a VID. 4. If delete type is “Selected”, then select row(s) to be deleted. 5. Click “Delete” button to delete.
Field	Description
Port	Port: G1 ~ G24, 10G1 ~ 10G4.
VID	Range: 1~4094. Default value is 1.
MAC Address	Format XX:XX:XX:XX:XX:XX

2.3.43 MAC Learning & Forwarding – Aging Time



Operation	Modify: 1. Modify the configuration 2. Click “Modify” button to apply the change
Field	Description
Aging Time(Sec)	Range: 10~600, Default is 300 seconds.

2.3.44 STP Bridge



Operation	Modify: 1. Select “Config” page. 2. Modify the configuration. 3. Clicks “Modify” button to apply change.
Field	Description
STP Mode	Control the STP operation for system level. There are : "Enabled" - Enable STP operation. "Disabled" - Disable STP operation. This is default option.
Protocol	Specify the STP is operating on which version, include STP, RSTP and MSTP.
Priority	Specify the priority of spanning tree. This is only used when protocol is operating on STP, RSTP or CIST case. For MSTI case, per instance will maintain another unique priority. The range is from 0 to 61440 in step of 4096. The default is 32768.
Bridge Max Age	Specify the maximum age of received protocol information before it is discarded. It is used when the Bridge is the Root or is attempting to become the Root. The range is from 6 to 40 in unit of one second. The default is 20.

Bridge Hello Time	Specify the value of the Hello Time parameter when the Bridge is the Root or is attempting to become the Root. This parameter is the time interval between transmissions of Topology Change Notification BPDUs towards the root when the Bridge is attempting to notify the Designated Bridge on the LAN to which its Root Port is attached of a topology change. The range is from 1 to 10 in unit of one second. The default is 2.
Bridge Forward Delay	Specify the time spent by a port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received Configuration Messages indicate a topology change. The range is from 4 to 30 in unit of one second. The default is 15.
BPDU Filter	Specify the behavior of received BPDU when STP is disabled. There are : "Deny" - It always discard received BPDU. This is default setting. "Flooding" - It always flood received BPDU to all bridge ports except to received port.
Region Name	Specify Region Name used by MSTP stack. The range is from 0 to 32 in unit of a character. This field default value is empty.
Revision Level	Specify Revision Level used by MSTP stack. The range is from 0 to 65535. This default is 0.
Recovery Delay	Specify the time that stay in "Err-Disable" state since received BPDU on BPDU-Guard enabled port. The range is from 30 to 86400 in unit of one second. This default is 30.

2.3.45 STP Port

Configuration / STP / STP Ports

Modify

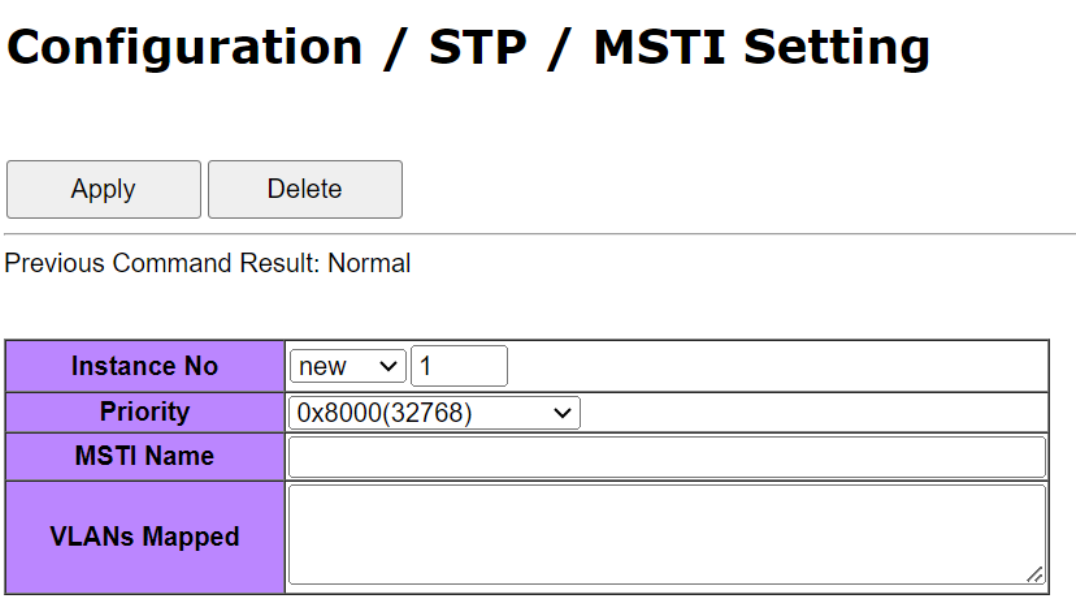
Previous Command Result:Normal

	Port	STP Port	Priority	Path Cost	Edge	Restricted		BPDU Guard
						Role	Tcn	
☐	*	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled
☐	G1	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled
☐	G2	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled
☐	G3	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled
☐	G4	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled
☐	G5	Enabled	0x80(128)	20000	Disabled	Disabled	Disabled	Disabled

Operation	To Modify STP Port: Push "Modify" button to apply all changes. Display "Success" when changes are successfully applied. Display "Fail" when changes are failed to be applied.
Field	Description
Port	Port identifier
STP Port	Specify the STP operation is enabled or disabled for this port.
Priority	Specify the port priority. The value will be referred when STP is operating on STP, RSTP and CIST case. The range is from 0 to 240 in step of 16. The default is 128.
Path Cost	The contribution of the path through this Port, when the Port is the Root Port, to the total cost of the path to the Root for this Bridge. This parameter is used, added to the value of the Designated Cost parameter for the Root Port, as the value of the Root Path Cost parameter offered in all Configuration BPDUs transmitted by the Bridge, when it is not the Root. The range is from 1 to 200000000. The default is 20.

Edge	Specify the port as admin-edge port or none. "Enabled" - this will make port instantly goes into forwarding state when port is link up. "Disabled" - the port follow normal state transition procedure when port is link up. This is default setting.
Restricted Role	Control the restricted role behavior specified in 802.1Q-2005. This is similar to "Root Guard" function operated on Cisco device. The default setting is disabled.
Restricted Tcn	Control the restricted tcn behavior specified in 802.1Q-2005. The default setting is disabled.
BPDU Guard	The protection mechanism to forbid BPDU received from unexpected source, and then cause STP topology change. When this mechanism is triggered, port goes into "Err-Disable" state. One timer, apply "recovery delay ", start to monitor port state till this timer expired without receiving any BPDU. Then port recovery to normal STP transition process; otherwise, port is staying in "Err-Disable" state. The default setting is disabled.

2.3.46 MSTI Setting



Operation	Apply:

	This button support "Add" and "Modify" function to configure the MSTI entry. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure. Delete: This button support "Delete" function to delete the MSTI entry. Push "Delete" button to delete current MSTI entry. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Instance No	The number for identifying the index of this MSTI entry. In case of "Creating", choose "new" option in a drop-down list with valid options. When this option is selected, one empty form is generated for user setting new MSTI entry. In case of "Modifying" or "Deleting", choose id number in a drop-down list with valid options. Then user can modify or delete this selected MSTI entry.
Priority	Configure value of priority used by this MST instance. The range is from 0 to 61440 in step of 4096. The default setting is 32768.
MSTI Name	Configure description for this MST instance. It accepts any printable character of ASCII table, that range is from 0 to 30.
VLAN Mapped	Configure one list of VLANs that mapped to this MST instance. When multiple VLANs are applied, enter these VLAN ids, separated by commas. (ex: 1,4,6,10) If successive VLANs are applied, just enter the start and end VLAN, separated by a hyphen. (ex: 1-5,10-14) Note: Each VLAN is only allowed to map to one unique MST instance.

2.3.47 MSTI Port

Configuration / STP / MSTI Ports

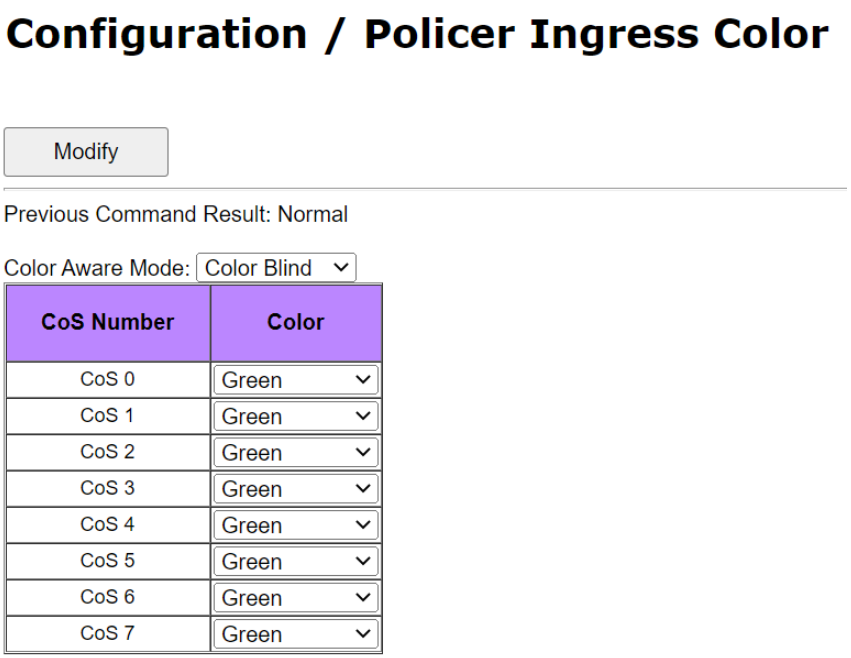
Modify

Previous Command Result:Normal

MST Instance No:

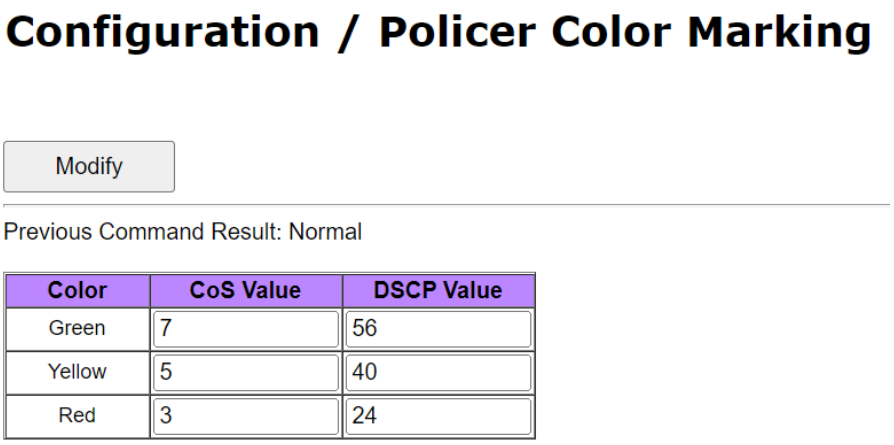
Operation	Modify: Push "Modify" button to apply changes on current MSTI entry. Display "Success" when previous operation succeeds. Display "Fail" when previous operation is failure.
Field	Description
Port	Port identifier
Priority	Configure value of priority used by this MSTI port. The range is from 0 to 240 in step of 16. The default is 128.
Path Cost	The contribution of the path through this Port, when the Port is the Root Port, to the total cost of the path to the Root for this Bridge. This parameter is used, added to the value of the Designated Cost parameter for the Root Port, as the value of the Root Path Cost parameter offered in all Configuration BPDUs transmitted by the Bridge, when it is not the Root. The range is from 1 to 200000000. The default is 20000.

2.3.48 Policer Ingress Color



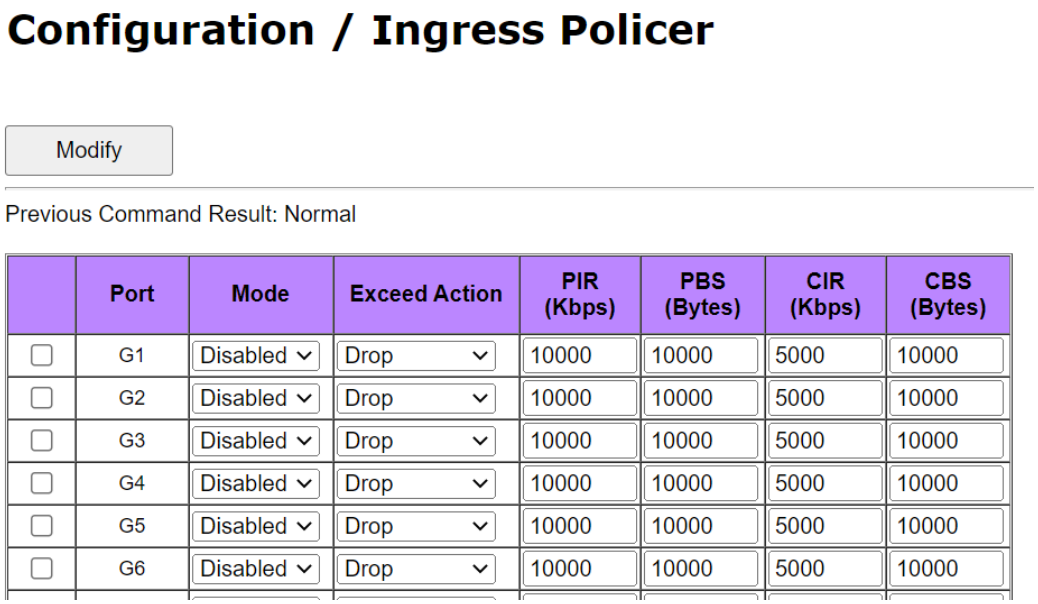
Operation	Modify: 1. Select “Color Blind” or “Color Aware” 2. Modify the configuration of CoS 0~7 3. Click “Modify” button to apply change
Field	Description
Color Aware Mode	Color Blind/ Color Aware. Default is Color Blind.
CoS 0	Green/Yellow/Red, default is green
CoS 1	Green/Yellow/Red, default is green
CoS 2	Green/Yellow/Red, default is green
CoS 3	Green/Yellow/Red, default is green
CoS 4	Green/Yellow/Red, default is green
CoS 5	Green/Yellow/Red, default is green
CoS 6	Green/Yellow/Red, default is green
CoS 7	Green/Yellow/Red, default is green

2.3.49 Policer Color Marking



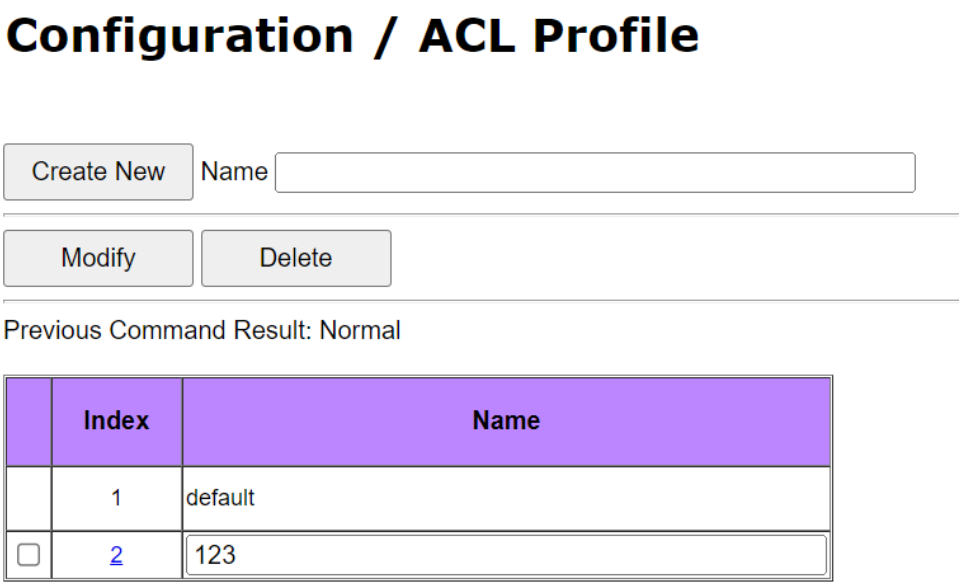
Operation	Modify: 1. Modify the configuration 2. Click “Modify” button to apply change
Field	Description
CoS Green	Range: 0~7, Default is 7
CoS Yellow	Range: 0~7, Default is 5
CoS Red	Range: 0~7, Default is 3
DSCP Green	Range: 0~63, Default is 56
DSCP Yellow	Range: 0~63, Default is 40
DSCP Red	Range: 0~63, Default is 24

2.3.50 Ingress Policer



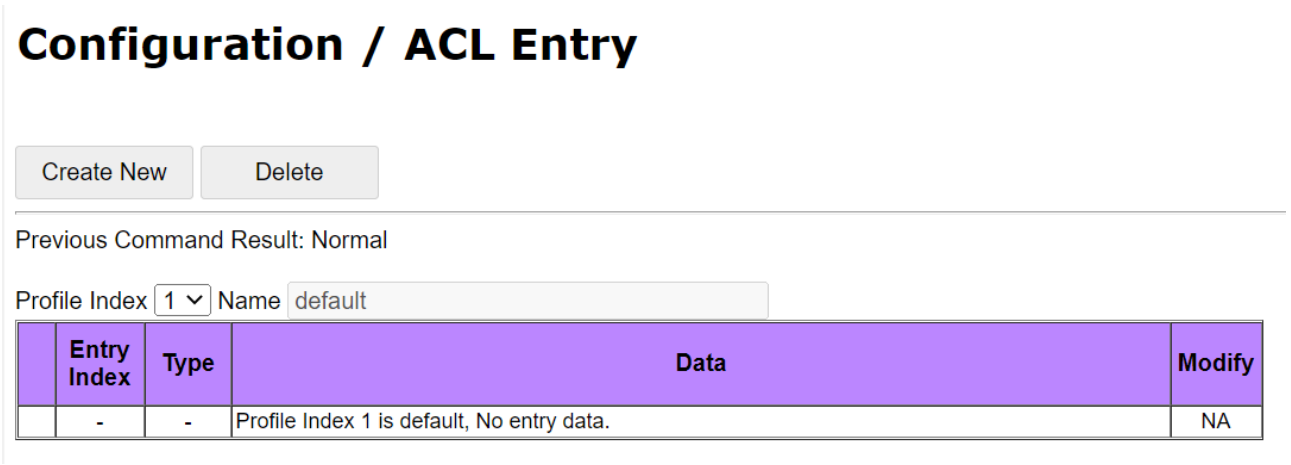
Operation	Modify: 1. Modify the configuration 2. Click “Modify” button to apply change
Field	Description
Port	Identify the port index. G1/10G1 ~ MAX Number of Port.
Mode	Ingress Policer Mode Enabled/Disabled, default is Disabled.
Exceed Action	Value range is Drop/CoS Mark/DSCP Mark, default is Drop.
PIR (Kbps)	G1 ~ G24 rate range is 1~1000000 Kbps, default is 10000 Kbps. 10G1 ~ 10G4 rate range is 1~10000000 Kbps, default is 10000 Kbps.
PBS (Bytes)	Value range is 1~65535 Bytes, default is 10000 Bytes.
CIR (Kbps)	G1 ~ G24 rate range is 1~1000000 Kbps, default is 5000 Kbps. 10G1 ~ 10G4 rate range is 1~10000000 Kbps, default is 5000 Kbps.
CBS (Bytes)	Value range is 1~65535 Kbps, default is 10000 Kbps.

2.3.51 ACL Profile



Operation	Create New: 1. Fill ACL Profile Name, the max length is 31. 2. Click “Create New” button to Create New ACL profile. Modify: 1. Select checkbox of profile to be changed. 2. Modify the “Name” of profile 3. Click “Modify” button to apply change Delete: 1. Select one row for delete 2. Click “Delete” button to delete data
Field	Description
Index	ACL Profile Index, index range depends on product type. Profile 1 is a default profile, cannot be modified. Click the Profile Index to modify the ACL Profile Entry.
Name	ACL Profile Name, the max length 31 characters.

2.3.52 ACL Entry



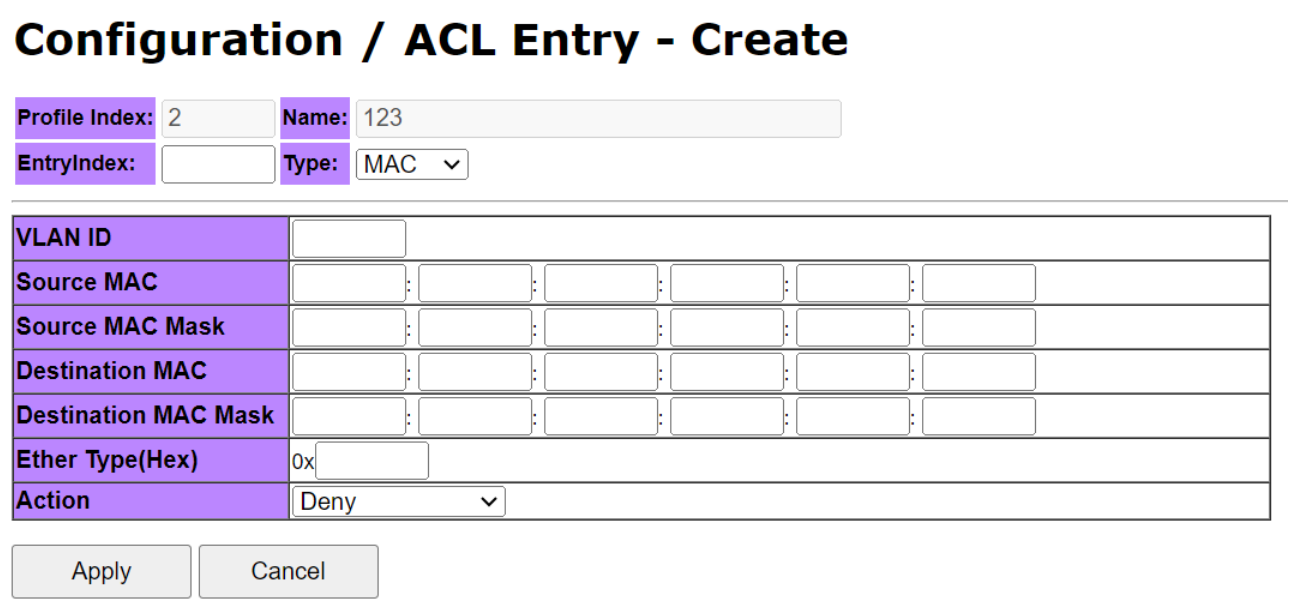
Configuration / ACL Entry

Create New | Delete

Previous Command Result: Normal

Profile Index 1 Name default

	Entry Index	Type	Data	Modify
	-	-	Profile Index 1 is default, No entry data.	NA



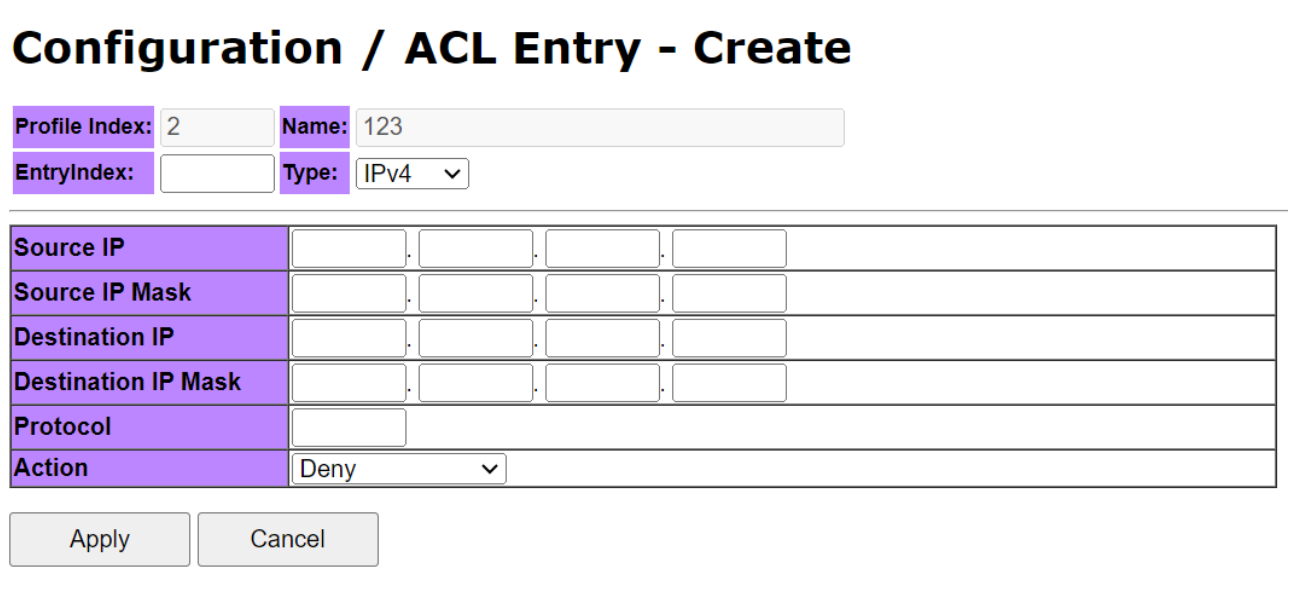
Configuration / ACL Entry - Create

Profile Index: 2 Name: 123

EntryIndex: Type: MAC

VLAN ID	
Source MAC	: : : : :
Source MAC Mask	: : : : :
Destination MAC	: : : : :
Destination MAC Mask	: : : : :
Ether Type(Hex)	0x
Action	Deny

Apply | Cancel



Configuration / ACL Entry - Create

Profile Index: 2 Name: 123

EntryIndex: Type: IPv4

Source IP	. . .
Source IP Mask	. . .
Destination IP	. . .
Destination IP Mask	. . .
Protocol	
Action	Deny

Apply | Cancel

Configuration / ACL Entry - Create

Profile Index:	2	**Name:**	123
EntryIndex:		**Type:**	L4Port

Protocol	TCP
Source IP	. . .
Source IP Mask	. . .
Port	
Destination IP	. . .
Destination IP Mask	. . .
Port	
Action	Deny

Apply Cancel

Configuration / ACL Entry - Create

Profile Index:	2	**Name:**	123
EntryIndex:		**Type:**	ToS

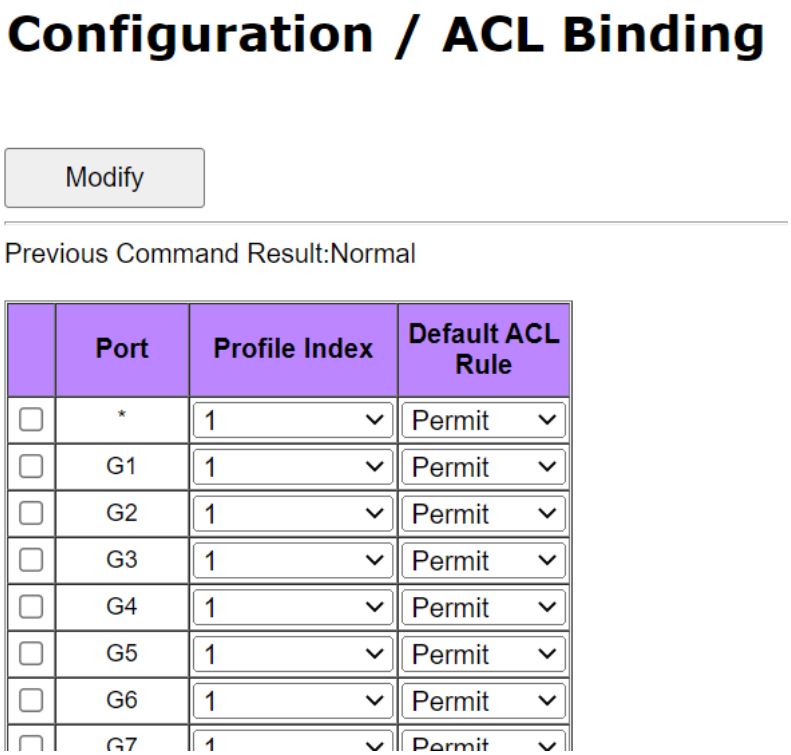
Source IP	. . .
Source IP Mask	. . .
Destination IP	. . .
Destination IP Mask	. . .
ToS Type	Precedence value:
Action	Deny

Apply Cancel

Operation	Create New: 1. Click “Create New” button to open page of Create New entry. 2. Fill ACL Entry Index field and select Type. 3. Fill fields and then click “Apply” to create or click “Cancel” to cancel. Modify: 1. Modify field data. 2. Click “Modify” button to open modification page. 3. Fill Entry Index field and select Type. 4. Fill fields and then click “Apply” to modify or click “Cancel” to cancel. Delete: 1. Select row to be deleted 2. Click “Delete” button to delete data.
Field	Description
Profile Index	Range: depends on product type.
Entry Index	Range: 1~32
Type	MAC/IPV4/L4PORT/TOS
Type = MAC	
VLAN ID	ACL Profile VLAN ID, value range is 1~4094.
Source MAC	ACL Profile Source MAC format XX:XX:XX:XX:XX:XX, each field value range 0~FF
Source MAC Mask	ACL Profile Source MAC Mask format XX:XX:XX:XX:XX:XX, each field value range 0~FF
Destination MAC	ACL Profile Destination MAC format XX:XX:XX:XX:XX:XX, each field value range 0~FF
Destination MAC Mask	ACL Profile Destination MAC Mask format XX:XX:XX:XX:XX:XX, each field value range 0~FF
Ether Type (Hex)	Value range 0,05DD~FFFE, 0 means any, format XXXX
Action	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type = IPV4	
Source IP	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Source IP Mask	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Destination IP	Format XXX:XXX:XXX:XXX, each field value range 0~255.

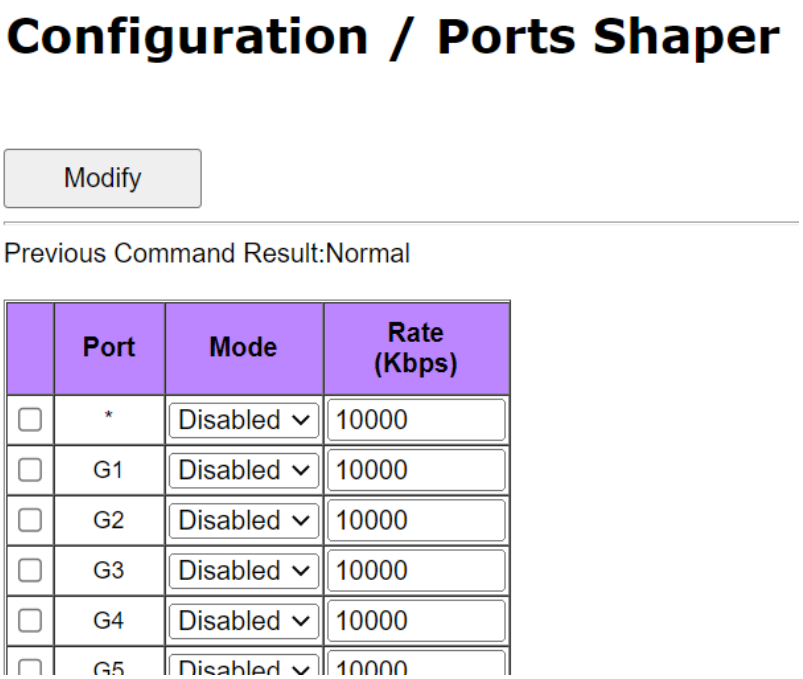
Destination IP Mask	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Protocol	Value range 0~255.
Action	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type = L4PORT	
Protocol	Option: TCP/UDP.
Source IP	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Source IP Mask	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Port	Source IP Port, value range 0~65535.
Destination IP	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Destination IP Mask	Format XXX:XXX:XXX:XXX, each field value range 0~255.
Port	Source IP Port, value range 0~65535. 0 means any port.
Action	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.
Type = ToS	
Source IP	Format XXX.XXX.XXX.XXX, each field value range 0~255.
Source IP Mask	Format XXX.XXX.XXX.XXX, each field value range 0~255.
Destination IP	Format XXX.XXX.XXX.XXX, each field value range 0~255.
Destination IP Mask	Format XXX.XXX.XXX.XXX, each field value range 0~255.
ToS Type	Value range Precedence/ToS/DSCP/Any, 0~7 in Precedence, 0~15 in ToS,0~63 in DSCP.
Action	Value range Deny/Permit/Queue Mapping/CoS Marking/Copy Frame.

2.3.53 ACL Binding



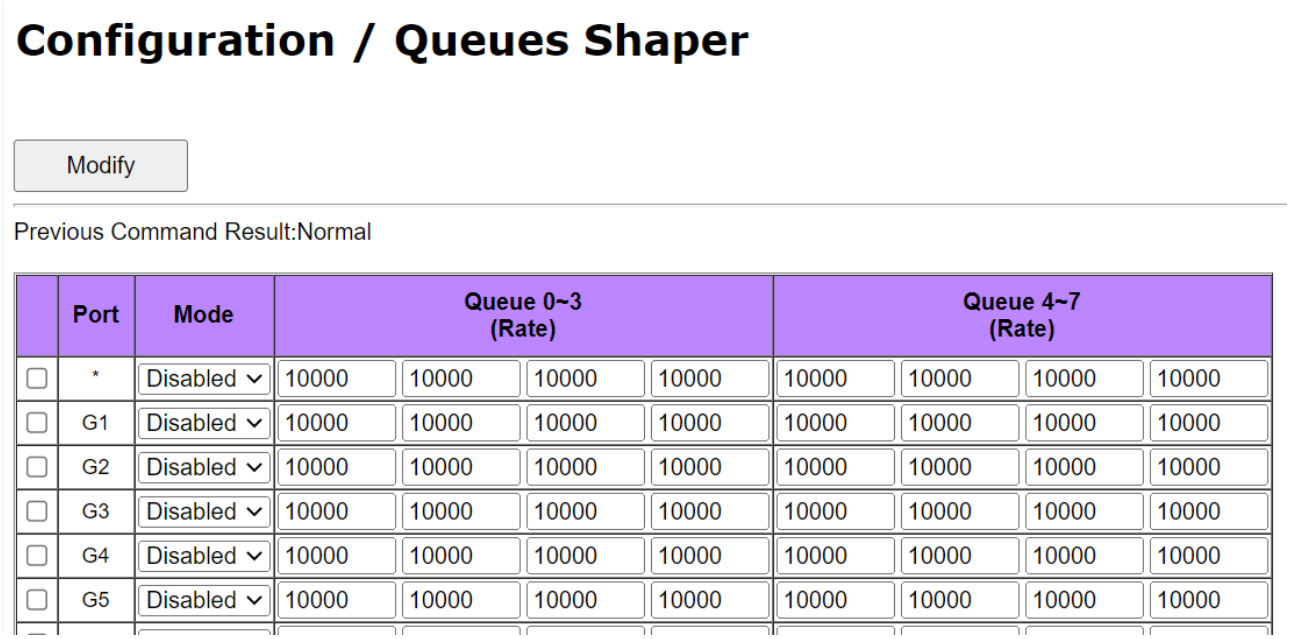
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Giga Port, G1/10G1 ~ MAX Number of Port.
Profile Index	ACL Profile Index, range is 1 ~ MAX SIZE of profile, default is 1.
Default ACL Rule	ACL Default Rule, could be Permit/Deny, default is Permit.

2.3.54 Port Shaper



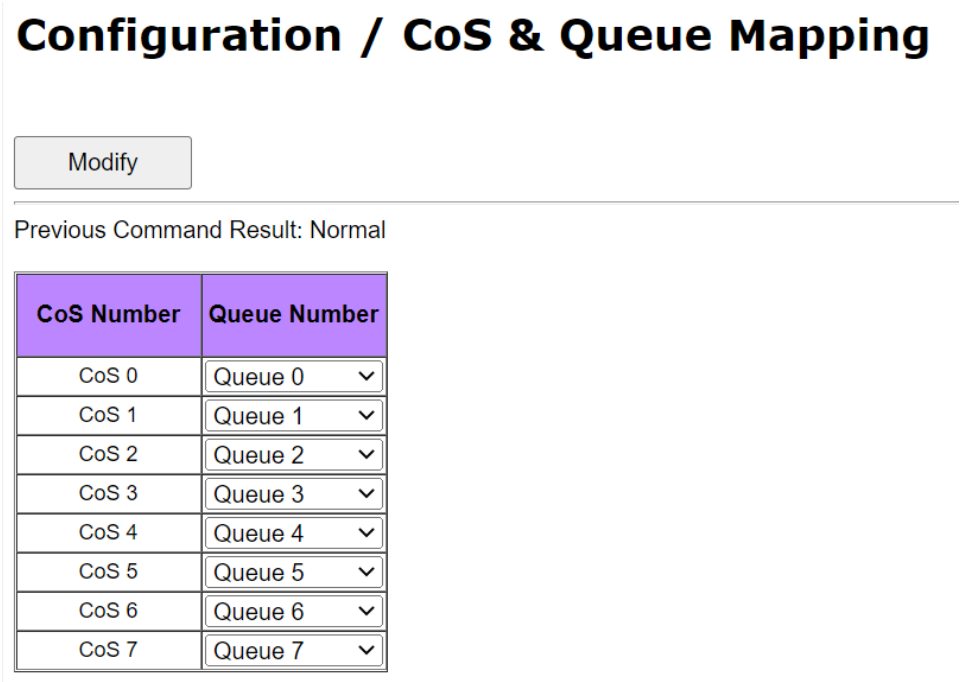
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Identify the port index, range is G1/10G1 ~ max number of ports.
Mode	Enabled/Disabled, default is Disabled.
Rate (Kbps)	G1 ~ G24 ports rate range is 100~1000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps. 10G1 ~ 10G4 ports rate range is 100~10000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps.

2.3.55 Queue Shaper



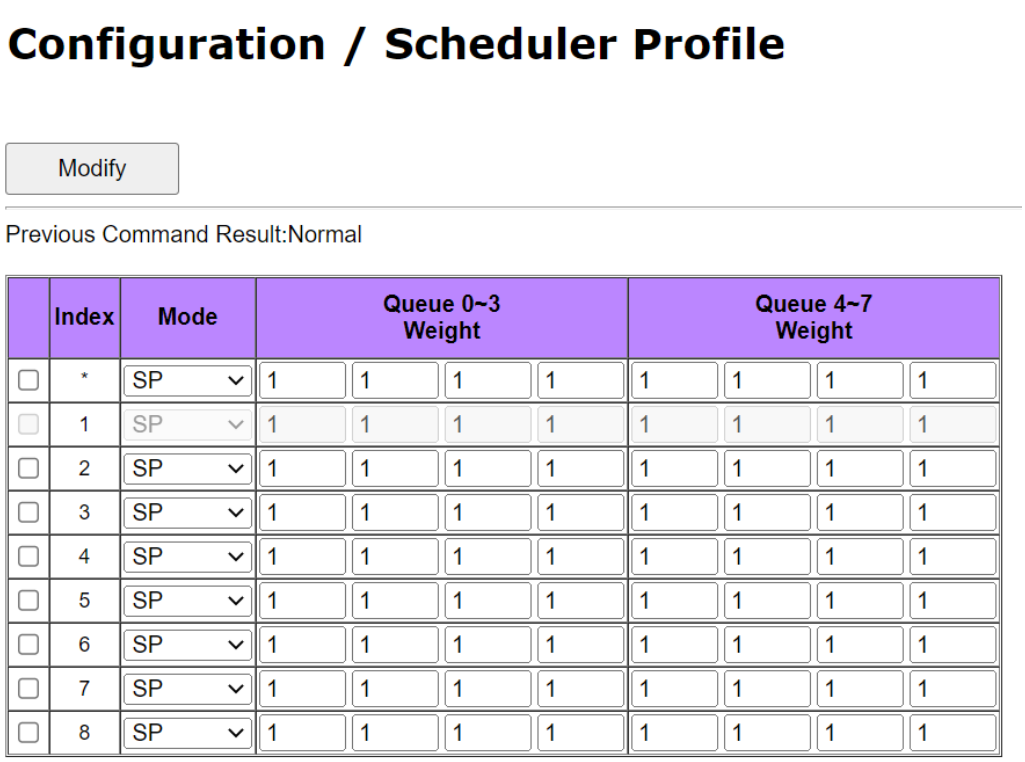
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
ID	Identify the port index, range is G1/10G1 ~ max number of ports.
Mode	Option: Enabled/Disabled, default is Disabled.
Queue 0~3 (Rate)	G1 ~ G24 port rate range is 100~1000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps. 10G1 ~ 10G4 port rate range is 100~10000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps.
Queue 4~7 (Rate)	G1 ~ G24 port rate range is 100~1000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps. 10G1 ~ 10G4 port rate range is 100~10000000 Kbps in step size of 4 Kbps. Default is 10000 Kbps.

2.3.56 CoS & Queue Mapping



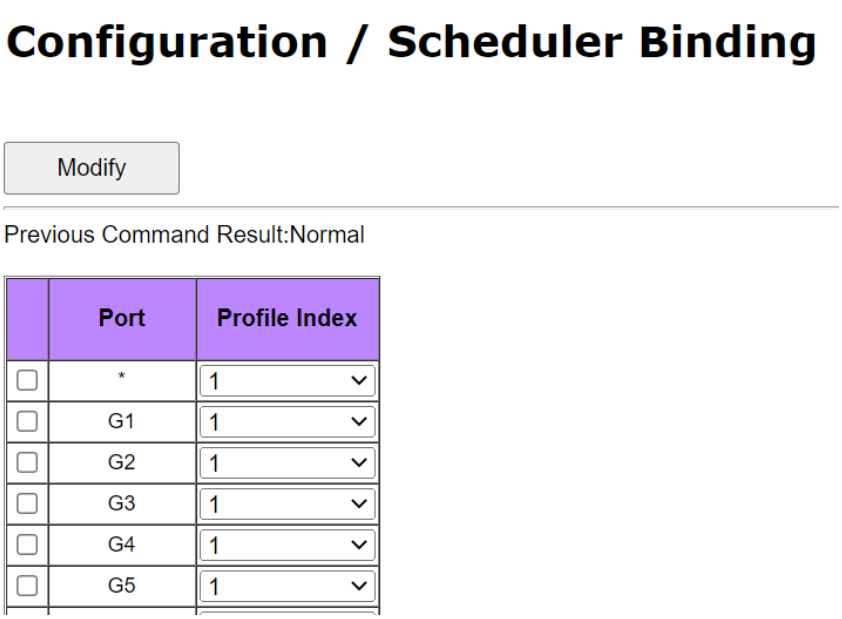
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
CoS 0	Queue 0~7, default is Queue 0.
CoS 1	Queue 0~7, default is Queue 1.
CoS 2	Queue 0~7, default is Queue 2.
CoS 3	Queue 0~7, default is Queue 3.
CoS 4	Queue 0~7, default is Queue 4.
CoS 5	Queue 0~7, default is Queue 5.
CoS 6	Queue 0~7, default is Queue 6.
CoS 7	Queue 0~7, default is Queue 7.

2.3.57 Scheduler Profile



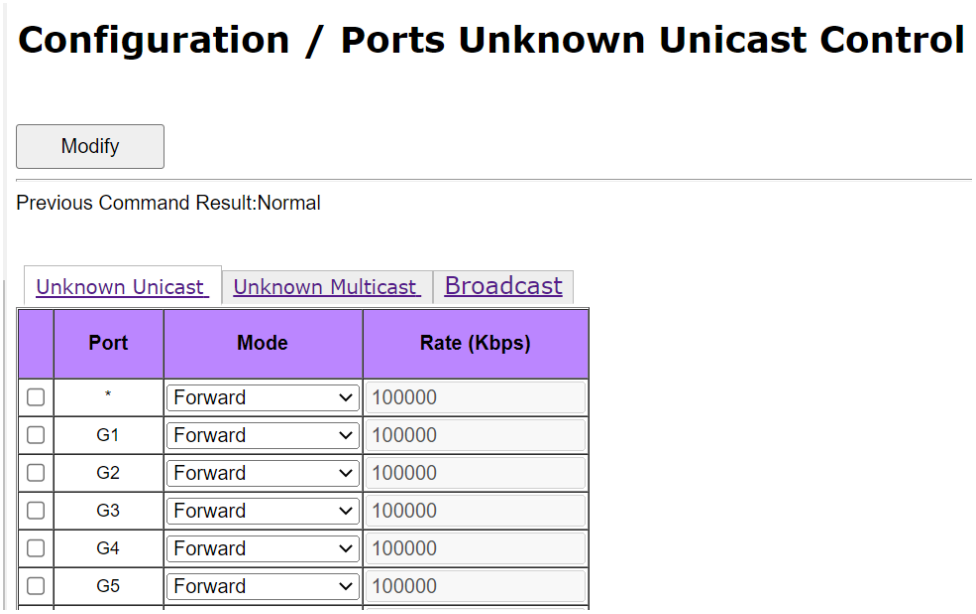
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Index	Value range is 1~8.
Mode	Option: SP/SPWRR/WRR, default is SP.
Queue 0~3 weight	Queue 0~3 Weight, range is 1~255, default is 1.
Queue 4~7 weight	Queue 4~7 Weight, range is 1~255, default is 1.

2.3.58 Scheduler Binding



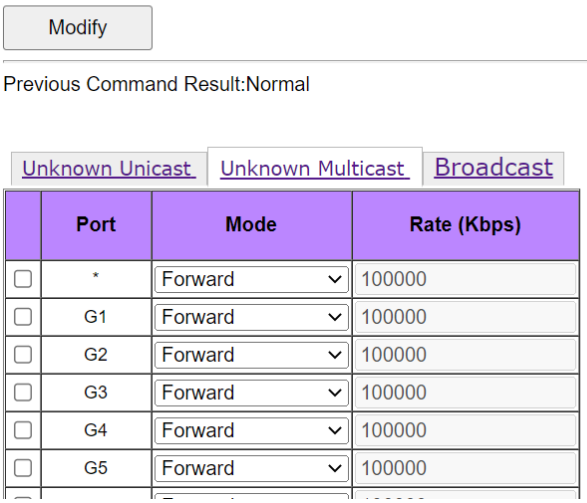
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Port ID
Profile Index	Range is 1~8, default is 1.

2.3.59 Storm Control - Ports



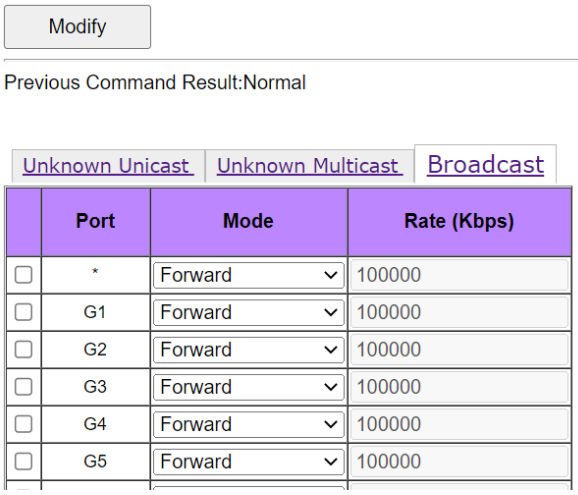
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Port range: G1 ~ MAX Number of Port.
Mode	Forward -> Forward unknown unicast packet (default) Block -> Block unknown unicast packet Rate limit -> Control rate. G1 ~ G24 rate range is 1~1000000 Kbps, default is 100000 Kbps. 10G1 ~ 10G4 rate range is 1~10000000 Kbps, default is 100000 Kbps.

Configuration / Ports Unknown Multicast Control



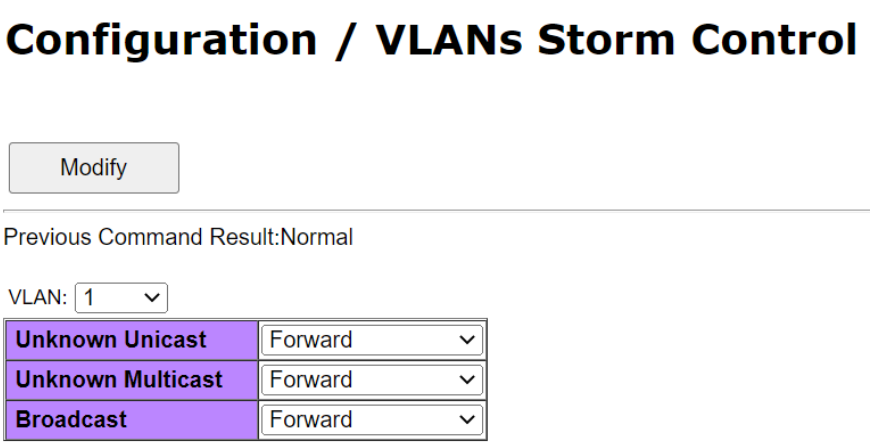
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Port range: G1 ~ MAX Number of Port.
Mode	Forward -> Forward unknown multicast unicast packet (default) Block -> Block unknown multicast packet Rate limit -> Control rate. G1 ~ G24 rate range is 1~1000000 Kbps, default is 100000 Kbps. 10G1 ~ 10G4 rate range is 1~10000000 Kbps, default is 100000 Kbps.

Configuration / Ports Broadcast Control



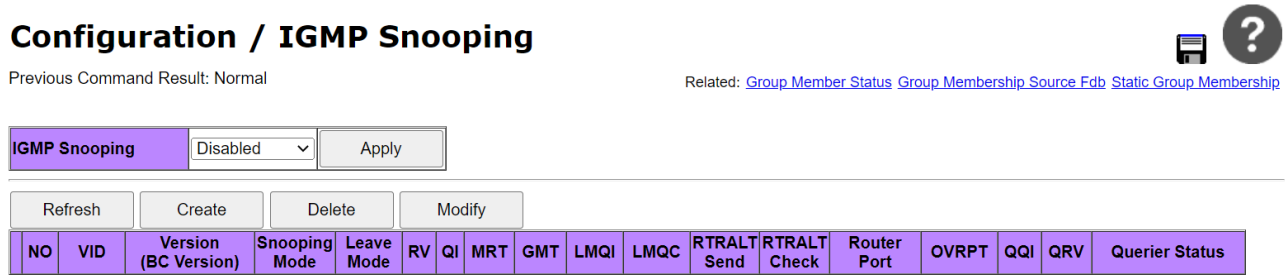
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Port	Port range: G1 ~ MAX Number of Port.
Mode	Forward -> Forward broadcast packet (default) Block -> Block broadcast packet Rate limit -> Control rate. G1 ~ G24 rate range is 1~1000000 Kbps, default is 100000 Kbps. 10G1 ~ 10G4 rate range is 1~10000000 Kbps, default is 100000 Kbps.

2.3.60 Storm Control - VLANs

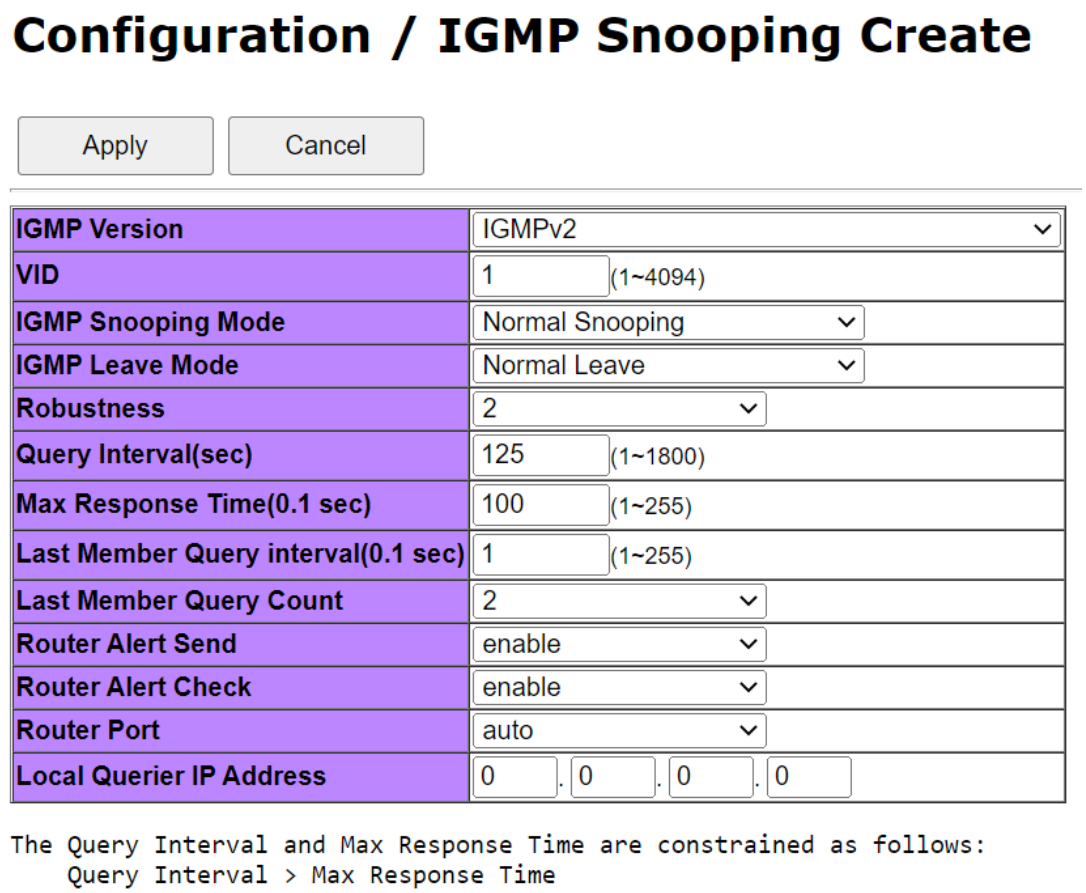


Operation	Modify: 1. Fill VLAN ID 2. Change Mode 3. Click “Modify” button to apply change
Field	Description
VLAN	Identify the VLAN operated storm-control in drop-down list.
Unknown Unicast	Specify blocking or forwarding when "Unknown Unicast" traffic storm occur on one VLAN domain. By default, "forward" is selected.
Unknown Multicast	Specify blocking or forwarding when "Unknown Multicast" traffic storm occur on one VLAN domain. By default, "forward" is selected.
Broadcast	Specify blocking or forwarding when "Broadcast" traffic storm occur on one VLAN domain. By default, "forward" is selected.

2.3.61 IGMP – VLAN Interface/IGMP Snooping



Create:




```
The Query Interval and Max Response Time are constrained as follows:
    Query Interval > Max Response Time
```

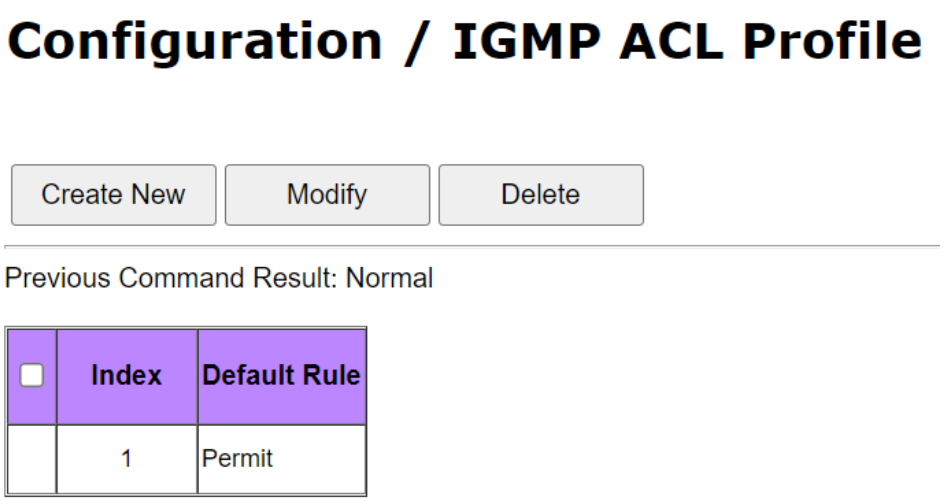
Operation	Refresh: 1. Click "Refresh" button to Refresh IGMP Snooping data. Create: 1. Click "Create" button into create page. 2. Fill config data. 3. Click "Apply" button to apply Config data or click "Cancel" button to cancel create config data. Modify: 1. Click "Modify" button into modify page. 2. Modify setting data 3. Click "Apply" button to apply Config data or click "Cancel" button to cancel create config data. Delete: 1. Select a row item to selected. 2. Click "Delete" button to Delete Config data.
Field	Description
NO	Entry Index, max 64.
VID	VLAN ID (1~4094)
Version	IGMPv2: Force IGMP snooping to use IGMPv2. IGMPv3: Force IGMP snooping to use IGMPv3. IGMPv3 Compatible: Enable IGMP snooping to use IGMPv3 as default version and is backward compatible with older version.
BC Version	When version is "IGMPv2" or "IGMPv3", this field is invalid. When version is "IGMPv3 Compatible", this field specify which version is used by IGMP snooping.
Snooping Mode	Normal Snooping: It will operate IGMP snooping as transparent processing. Snooping with Querier: It is normal snooping and always join querier-election on the network. When local querier is active querier on the network, active is present. When local querier is not active querier on the network, idle is present. Proxy: It will operate IGMP snooping as proxy processing.

Leave Mode	Normal Leave: The device will remove the host after one duration and sending group-specific queries to the other group members. Fast Leave: The device immediately removes host from the multicast group without sending group-specific queries to the other group members.
Robustness Variable (RV)	The Robustness Variable allows tuning for the expected packet loss on a subnet. The range is from 1 to 3. Default: 2
Query Interval (QI)	The Query Interval is the interval between General Queries sent by the Querier. The range is from 1 to 1800, in seconds. Default: 125 seconds
Max Response Time	The Max Response Time field is meaningful only in Membership Query messages, and specifies the maximum allowed time before sending a responding report in units of 1/10 second. The number of seconds represented by the [Max Response Time] must be less than the [Query Interval]. The range is from 1 to 255, in 1/10 seconds. Default: 10.0 seconds.
Group Membership Time	The Group Membership Time is the amount of time that must pass before a multicast router decides there are no more members of a group on a network. This value MUST be ((the Robustness Variable) times (the Query Interval)) plus (one Query Response Interval).
Last Member Query Interval (LMQI)	The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. The range is from 1 to 255, in 1/10 seconds. Default: 10 (1 second)
Last Member Query Count (LMQC)	The Last Member Query Count is the number of Group-Specific Queries sent before the router assumes there are no local members. The range is from 1 to 3. Default: 2.
Router Alert Send (RTRALT Send)	When "Router Alert Send" is enabled, the local device generates IGMP packet with carrying router-alert option. When "Router Alert Send" is disabled, the local device generates IGMP packet without router-alert option. Default is enabled.

Router Alert Check (RTRALT Check)	When "Router Alert Check" is enabled, the local device always verify router-alert option of incoming IGMP packet. If no router-alert option presents, ignore this IGMP packet. When "Router Alert Check" is disabled, the local device doesn’t care if incoming IGMP packet carry router-alert option. Default is enabled.
Router Port	The router port is the port that connects to a multicast router. The user can configure one switch port as fixed router port or auto learn to get dynamic router port where receives the general query message from querier. Default: auto.
Older Version Router Present Timeout (OVRPT)	This field is only valid when version is "IGMPv3 Compatible". When BC version is v2, it is the timeout for transitioning a host back to IGMPv3 mode once older version query is heard. This value MUST be ((the Robustness Variable) times (the Query Interval in the last Query received)) plus (one Query Response Interval). When BC version is v1, it is how long a host must wait after hearing a v1 query before it may send any v2 messages. Current [400 seconds] is applied when timeout value is updated in case of BC version is v1.
Querier's Query Interval(QQI)	This field is only valid when IGMPv3 is processing on the network. This is represented in units of seconds and is derived from the Querier's Query Interval Code as follows: If QQIC < 128, QQI = QQIC If QQIC >= 128, QQIC represents a floating-point value as follows: 0 1 2 3 4 5 6 7 +-+-+-+-+-+-+-+-+ | 1 | exp | mant | +-+-+-+-+-+-+-+-+ QQI = (mant | 0x10) << (exp + 3) Multicast routers that are not the current querier adopt the QQI value from the most recently received Query as their own [Query Interval] value, unless that most recently received QQI was zero.

Querier's Robustness Variable (QRV)	This field is only valid when IGMPv3 is processing on the network. If non-zero, the QRV field contains the [Robustness Variable] value used by the querier. If the querier's [Robustness Variable] exceeds 7, the maximum value of the QRV field, the QRV is set to zero. Routers adopt the QRV value from the most recently received Query as their own [Robustness Variable] value, unless that most recently received QRV was zero.
Local Querier IP Address	This field is only valid when snooping mode is "snooping with querier". It specifies the source IP address of local querier. Default: 0.0.0.0
Querier Status	(L)x.x.x.x - Local querier's IP address. (A)x.x.x.x - Active querier's IP address on a network. When active querier is other querier, one other querier present timer is updated.

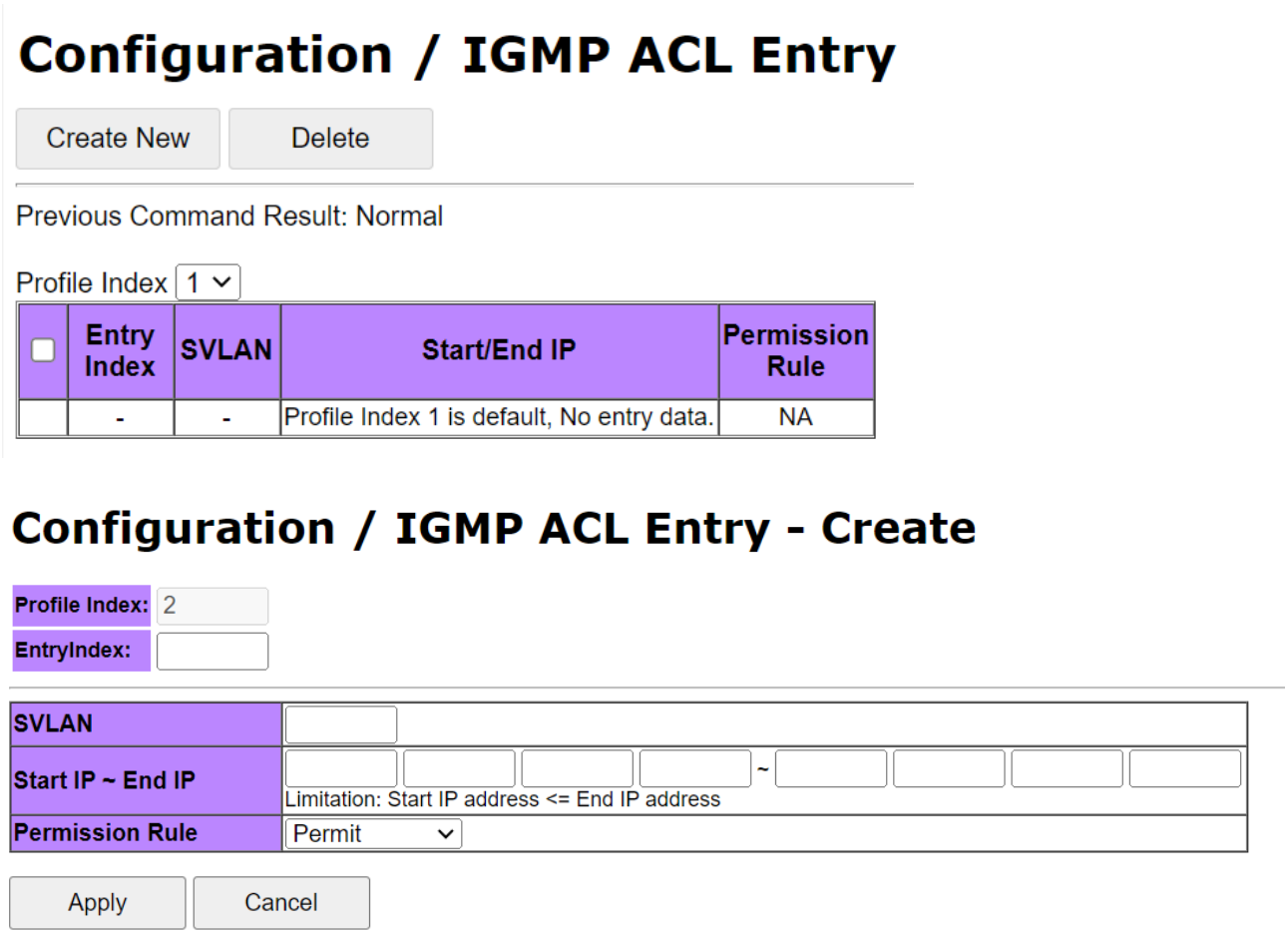
2.3.62 IGMP - ACL Profile



Operation	Create New: 1. Click "Create New" button to create a default profile. 2. Click "Modify" button to modify existing profile. Modify (allow multiple selection): 1. Check Profile Index and select Default Rule for profile. 2. Click "Modify" button to modify IGMP ACL Profile.

	Delete: Click Delete button to delete profile. (also allow multiple delete) If profile is in use, delete action will be failed.
Field	Description
Profile Index	IGMP ACL Profile Index: 1~15, but profile 1 is default existing and read-only.
Default Rule	IGMP ACL Default rule: Permit/Deny. Default is permit.

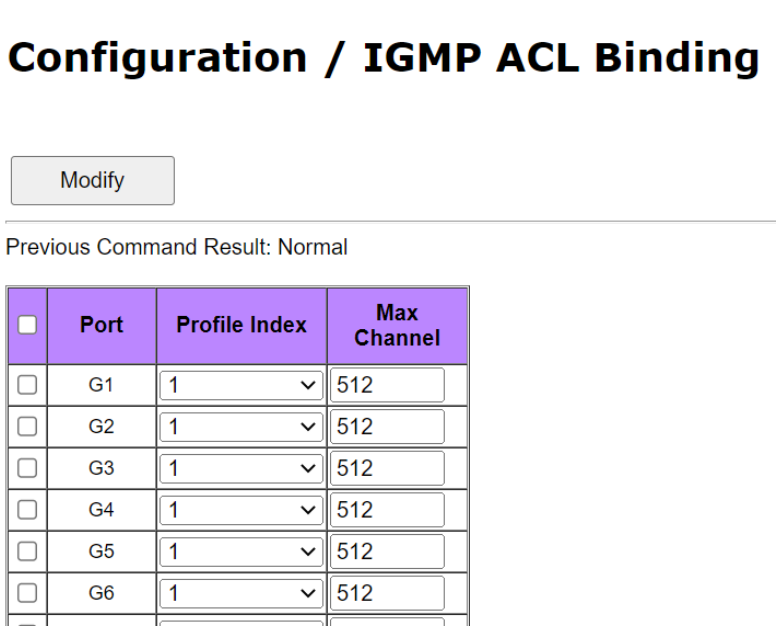
2.3.63 IGMP - ACL Entry



Operation	Create:

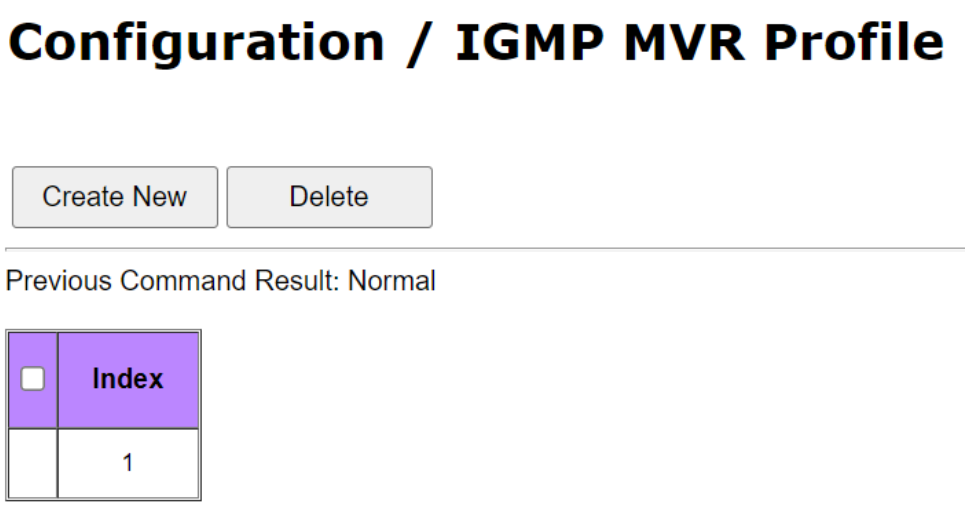
	1. Click "Create New" button to open new page for create. 2. Fill Entry Index, SVLAN, Start IP, End IP and select Permission Rule. 3. Click "Apply" button to create IGMP ACL entry or click "Cancel" to cancel create. Delete: Check up target entry, click Delete button to delete them. (also allow multiple delete) Refresh: 1. Select Profile index. 2. Click "Refresh" button to refresh current IGMP ACL profile entry(s).
Field	Description
Profile Index	IGMP ACL profile index. Index range is 2~15.
Entry Index	IGMP ACL entry index. Range is 1~32.
SVLAN	IGMP ACL VLAN: VLAN to be Permitted/Denied, 0 is any VLAN.
Start IP ~ End IP	IGMP ACL Start IP address. Range: 224.0.1.0 - 239.255.255.255 Start IP address <= End IP address
Permission Rule	IGMP ACL entry parameter. Default is Permit.

2.3.64 IGMP - ACL Binding



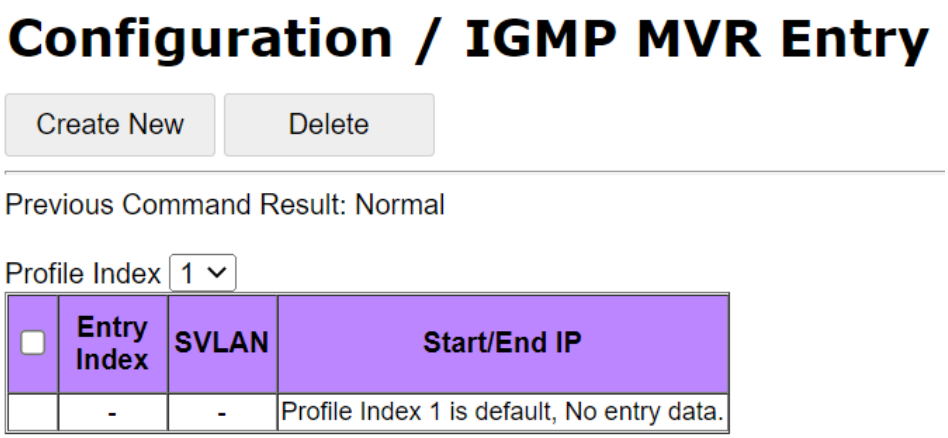
Operation	Modify: 1. Check up the rows to be modified, select ACL Profile and set Max channel. 2. Click "Modify" button to change IGMP ACL Binding.
Field	Description
Port	GE Port: 1 ~ MAX Number of Port.
Profile Index	IGMP ACL profile index: 1~15. Default is 1.
Max channel	Port Max channel. Range is 1~512. Default is 512.

2.3.65 IGMP - MVR Profile



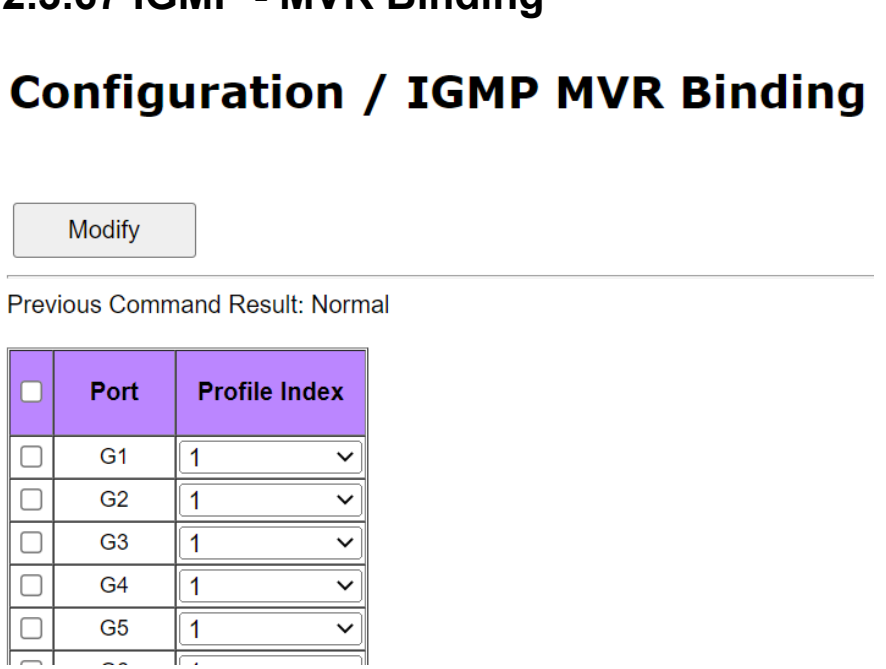
Operation	Create: 1. Click "Create New" button to create a new profile. Modify: 1. Check up Profile Index. 2. Click the Profile Index hyper link to open page for profile entry modification. [or click "Delete" delete Profile, allow multiple delete. If profile is in use, delete action will be failed.]
Field	Description
Profile Index	Profile 1 is default existing and read-only, IGMP MVR Profile 2~15 allow to create.

2.3.66 IGMP - MVR Entry



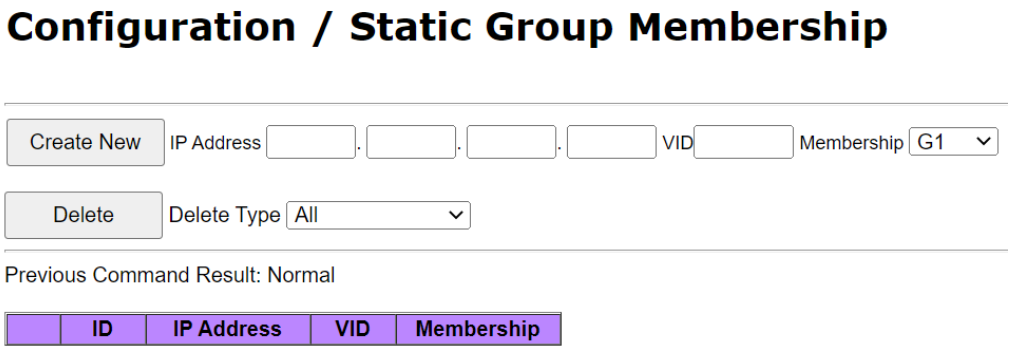
Operation	Create New: 1. Click "Create New" button to open new page for creating entry. 2. Fill Entry Index, SVLAN, Start IP, End IP. 3. Click "Apply" button to create IGMP MVR entry or click "Cancel" to cancel create. Delete: Check up target entry, click Delete button to delete them. (also allow multiple delete) Refresh: 1. Change Profile index. 2. Click "Refresh" button to refresh current IGMP MVR profile entry(s).
Field	Description
Profile Index	IGMP MVR profile index. Index range is 2~15.
Entry Index	IGMP MVR entry index. Range is 1~32.
SVLAN	IGMP MVR VLAN: VLAN to be Permitted/Denied
Start IP ~ End IP	IGMP MVR Start IP address. Range: 224.0.1.0 - 239.255.255.255 Start IP address <= End IP address

2.3.67 IGMP - MVR Binding



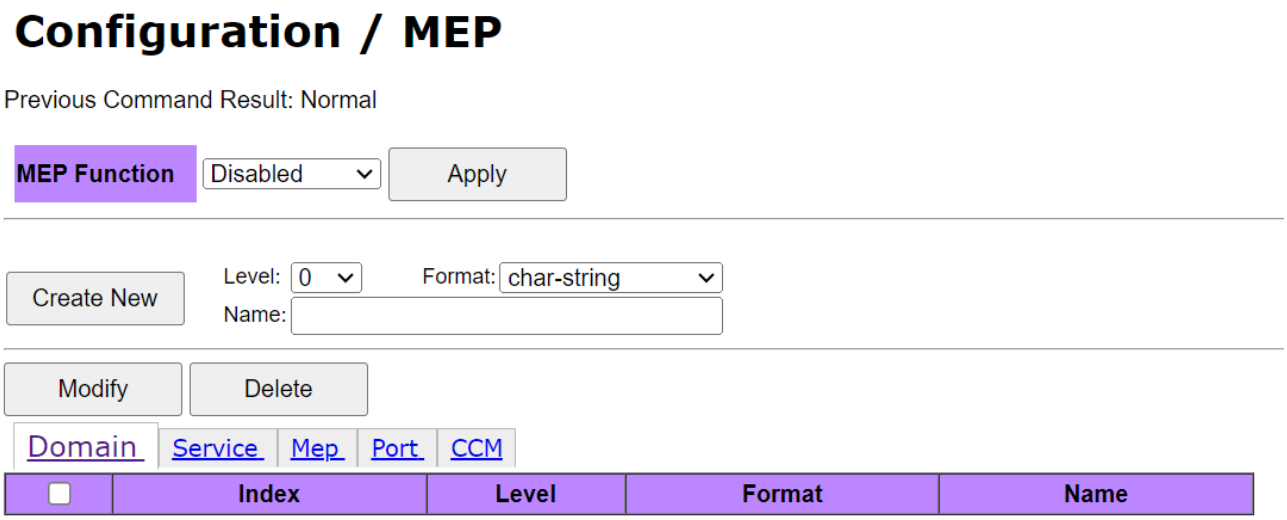
Operation	Modify: 1. Check up the rows to be modified, select MVR Profile. 2. Click "Modify" button to change IGMP MVR Binding.
Field	Description
Port	G1 ~ MAX Number of Port
Profile Index	IGMP MVR profile index. Value range is 1~15. Default is 1.

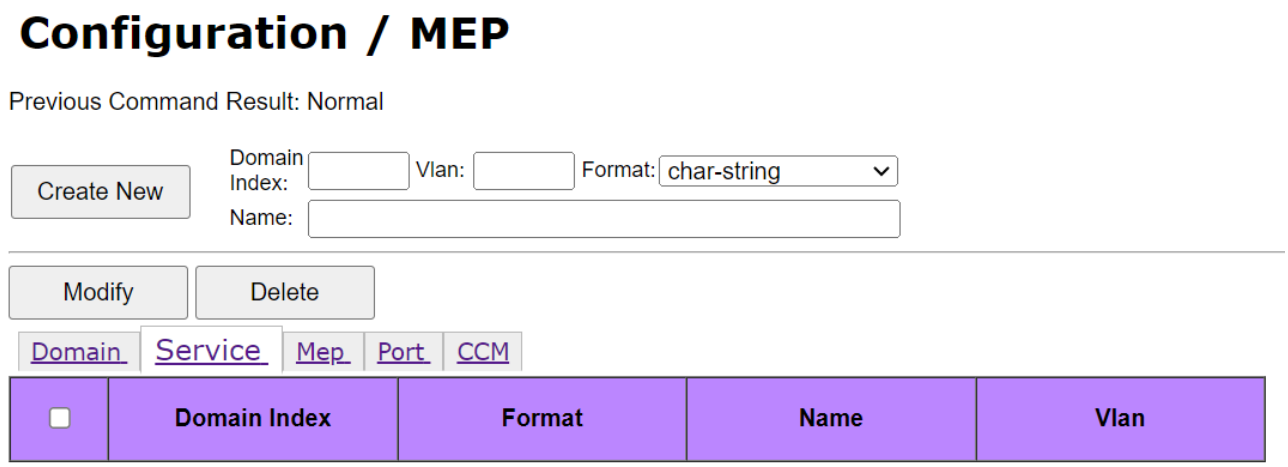
2.3.68 IGMP – Static Group Membership

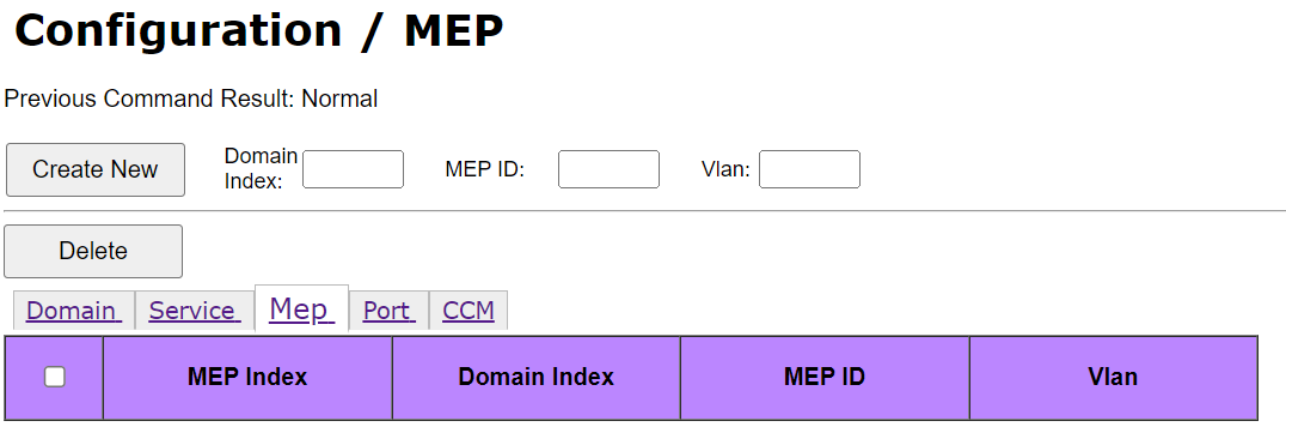


Operation	Create New: 1. Fill IP Address, VID and select Membership. 2. Click “Create New” button to create new data. Delete: 1. Select Delete Type "All/ Membership/ VID/ Selected" 2. If delete type is “Port”, then select a port 3. If delete type is "VID", then fill a VID 4. If delete type is "Selected", then select one row 5. Click “Delete” button to delete data.
Field	Description
ID	Entry Index, value range is 1~128.
IP Address	Group Membership IP Address, range is 224.0.0.0~239.255.255.255
VID	VLAN ID, range is 1 ~ 4094.
Membership	Giga Port, G1/10G1 ~ MAX Number of Port.

2.3.69 MEP


Configuration / MEP
Previous Command Result: Normal
MEP Function
Disabled
Apply
Create New
Level: 0
Format: char-string
Name:
Modify
Delete
Domain
Service
Mep
Port
CCM
Index
Level
Format
Name


Configuration / MEP
Previous Command Result: Normal
Create New
Domain Index:
Vlan:
Format: char-string
Name:
Modify
Delete
Domain
Service
Mep
Port
CCM
Domain Index
Format
Name
Vlan


Configuration / MEP
Previous Command Result: Normal
Create New
Domain Index:
MEP ID:
Vlan:
Delete
Domain
Service
Mep
Port
CCM
MEP Index
Domain Index
MEP ID
Vlan

Configuration / MEP

Previous Command Result: Normal

Modify

Domain | Service | Mep | Port | CCM

	Port	Direction	Level	MPID	Vlan	Active
☐	1	Down	0	1	1	Inactive
☐	2	Down	0	1	1	Inactive
☐	3	Down	0	1	1	Inactive
☐	4	Down	0	1	1	Inactive
☐	5	Down	0	1	1	Inactive

Configuration / MEP

Previous Command Result: Normal

Create New

Level: 0 Vlan: ActionType: Domain-Service Interval: 1S

Domain Name: Service Name:

Delete

Domain | Service | Mep | Port | CCM

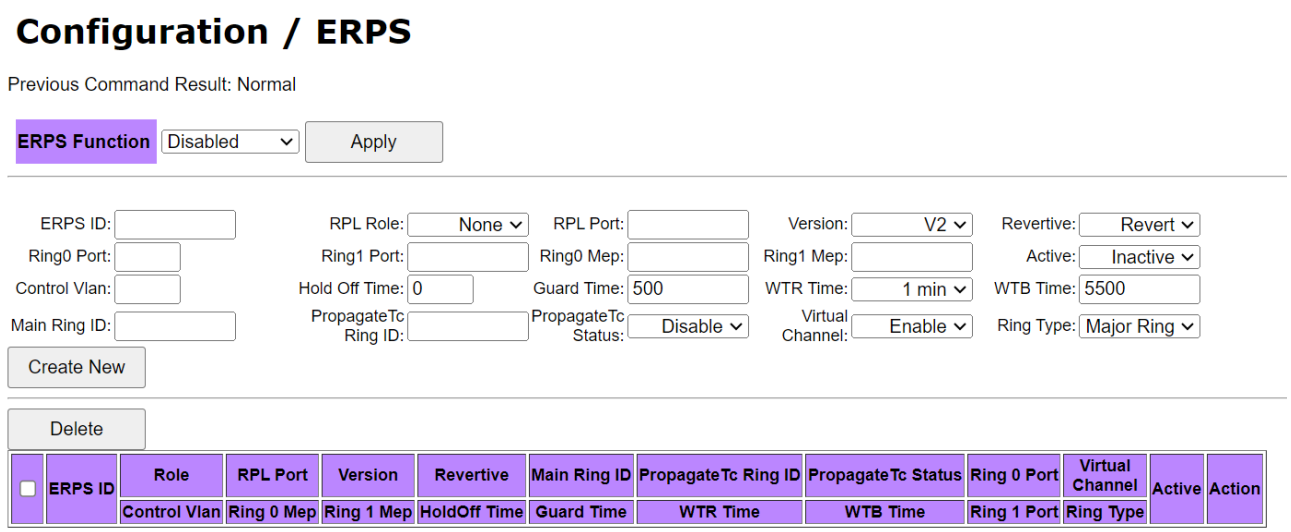
	Index	Level	Vlan	Action Type	Interval	Domain Name	Service Name

Operation	To modify MEP Function: 1. Select MEP Function. 2. Click "Apply" button to apply change. To create MEP Domain : 1. Fill below fields. 2. Click "Create New" button to create MEP Domain configuration. To modify MEP Domain : 1. Select table checkbox to modify. 2. Modify table checkbox row fields. 3. Click "Modify" button to modify MEP Domain configuration. To delete MEP Domain : 1. Select table checkbox to delete. 2. Click "Delete" button to delete MEP Domain configuration. To create MEP Service : 1. Fill below fields. 2. Click "Create New" button to create MEP Service configuration. To modify MEP Service : 1. Select table checkbox to modify. 2. Modify table checkbox row fields. 3. Click "Modify" button to modify MEP Service configuration. To delete MEP Service : 1. Select table checkbox to delete. 2. Click "Delete" button to delete MEP Service configuration. To create MEP : 1. Fill below fields. 2. Click "Create New" button to create MEP configuration. To delete MEP : 1. Select table checkbox to delete. 2. Click "Delete" button to delete MEP configuration. To modify MEP Port : 1. Select table checkbox to modify. 2. Modify table checkbox row fields. 3. Click "Modify" button to modify MEP Port configuration.

	To create MEP CCM : 1. Fill below fields. 2. Click "Create New" button to create MEP CCM configuration. To delete MEP Service : 1. Select table checkbox to delete. 2. Click "Delete" button to delete MEP Service configuration.
Field	Description
Domain	
MEP Function	Enable/Disable MEP function. Default value is Disabled.
Index	Must: MEP index ID.
Level	Must: MEP level, value range is 0-7.
Format	Domain name format. Value range is dns-like-name, mac-addr, char-string, none.
Name	Must: ERPS domain name. Value length is 1-43. The name will follow format to check. The dns-like-name format example: www.sample.com The mac-add format example: 00:01:02:03:04:05:65535
Service	
Index	Must: MEP index ID.
Format	Service name format. Value range is primary-vid, char-string, unsigned-int16, rfc2865-vpn-id, icc.
Name	Must: MEP service name. Value length is 1-43. The name will follow format to check. The primary-vid format name is vlan number. The unsigned-int16 format name is unsigned word(16 bits). The rfc2865-vpn-id format name example: 313233:34353637. The icc format format name example: 65536.(domain format must be none)

VLAN	Must: MEP vlan, value range is 1-4094.
MEP	
MEP Index	Must: MEP index ID.
Domain Index	Must: MEP domain index ID, value range is 1-8.
MEP ID	Must: MEP ID, value range is 1-8191.
VLAN	Must: MEP vlan, value range is 1-4094.
Port	
Port	Must: Port interface index.
Direction	Must: MEP control message direction, default is down.
Level	Must: MEP level, value range is 0-7.
MPID	Must: MEP ID, value range is 1-8191.
Vlan	Must: MEP control message vlan. Value length is 1-4094.
Active	Must: Active configuration in MEP.
CCM	
Index	Must: MEP CCM index ID.
Level	Must: MEP level, value range is 0-7.
Vlan	Must: MEP control message vlan. Value length is 1-4094.
Action Type	Must: Action type. The options are Domain-Service, Domain-Vlan and Level-Vlan.
Interval	Must: MEP CCM Interval, the options are 100MS, 1S, 10S, 1Min, 10Mins, default is 1S.
Domain Name	Must: MEP domain name. Value length is 1-43.
Service Name	Must: MEP service name. Value length is 1-43.

2.3.70 ERPS



Operation	<u>To modify ERPS Function:</u> 1. Select ERPS Function. 2. Click "Apply" button to apply change. <u>To create ERPS :</u> 1. Fill below fields. 2. Check up the port(s) to be changed. 3. Click "Create New" button to create ERPS configuration. <u>To Execute ERPS Action:</u> 1. Select group interface port action (Force Switch / Manual Switch / Clear). 2. Fill group interface port number. 3. Click same group row "Execute" button to execute action.
Field	Description
ERPS ID	Must: ERPS group ID.
RPL Role	Must: RPL Role, value range is None, Owner or Neighbor.
ROL Port	It must be fill when the RPL Role is Owner. No need to fill this field when the role is Others.

Version	Must: ERPS version. V1 or V2. Default is V2.
Revertive	Must: The role is Owner, it will recover RPL port to blocked when the ring is good. Default is true.
Ring0 Port	Must: Assign ERPS ring port 0.
Ring1 Port	Assign ERPS ring port 1. No need to fill this field when the ERPS is sub-ring.
Ring0 MEP	Must: ERPS ring 0 Mep ID.
Ring1 MEP	ERPS ring 1 Mep ID. No need to fill this field when the ERPS is sub-ring.
Active	Must: Active configuration in ERPS.
Hold Off Time	Must: Hold off timer value configuration. Value range 0 - 10000, unit: ms, step 100 ms, default is 0 ms.
Guard Time	Must: Guard Interval to prevent reception of outdated RAPS messages. Value range 10 - 2000, unit: ms, step 10 ms, default is 500 ms. Rule: WTB time >= Guard Time + 5000 (ms)
WTR Time	Must: The period of the WTR time can be configured by the operator in 1 minute steps between 1 and 12 minutes with a default value of 1 minute.
WTB Time	Must: The period of the WTB time can be configured by the operator. This value is not configurable explicitly as it is 5 seconds longer than the guard timer. The range of the WTB timer. Value range 5010 - 7000, unit: ms, default is 5500 ms. Rule: WTB time >= Guard Time + 5000 (ms)
Virtual Channel	Assign ERPS sub-ring control message communication type.
Main Ring ID	Assign ERPS sub-ring follow main ring group id.
Control Vlan	Must: Assign ERPS control message vlan.
Data Vlan	Must: Assign ERPS data vlan.
PropagateTc Ring ID	PropagateTc Ring ID, only work on sub-ring.
PropagateTc Status	PropagateTc status, only work on sub-ring.

Ring Type	Assign ERPS group ring type, default is Major Ring.

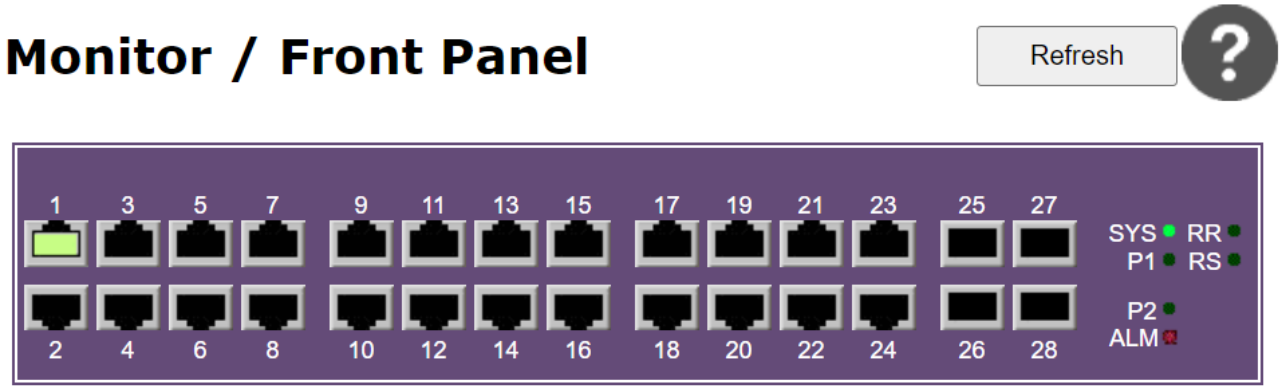
2.4 Monitor

2.4.1 Front Panel

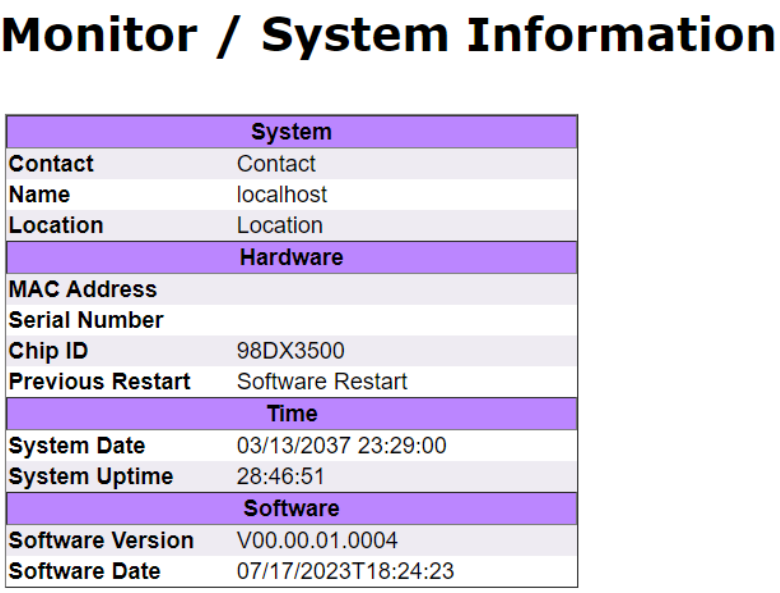
This page displays the real status of system's panel.

Use the Monitor/Front Panel screen to view the graphic of front panel.

Get Port status when cursor move to port icon.



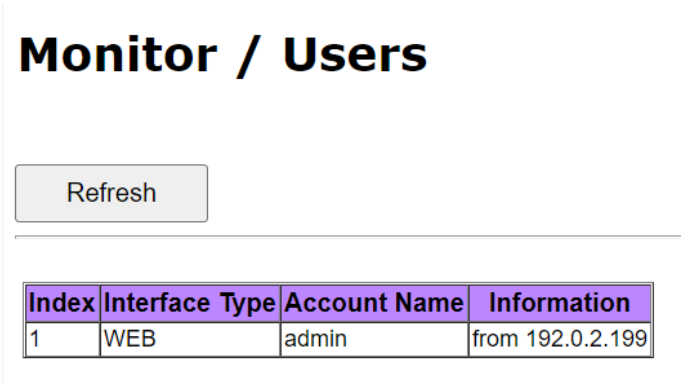
2.4.2 System Information



Field	Description
Contact	Contact information.
Name	Name information.

Location	Location information.
MAC Address	MAC Address information.
Serial Number	Serial Number information.
Chip ID	Chip ID information.
Previous Restart	Previous Restart information.
System Date	System Date information.
System Uptime	System Uptime information.
Software Version	Software Version information.
Software Date	Software Date information.

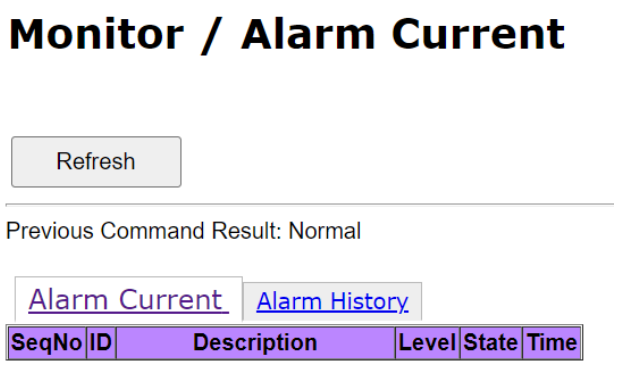
2.4.3 Users



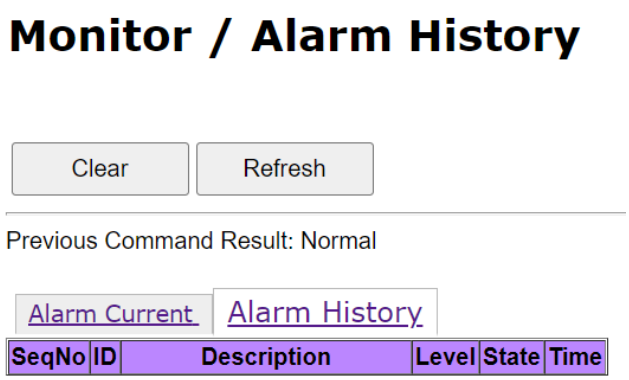
Operation	Refresh: Click “Refresh” button to refresh current data.
Field	Description
Index	Show the index of login user list.
Interface Type	Show the mode of access. Possible values Console, CLI, Web.
Account Name	Show the account name of the user.
Information	Show more information about the user, including IP address of the management host.

2.4.4 Alarm Log

Alarm Current

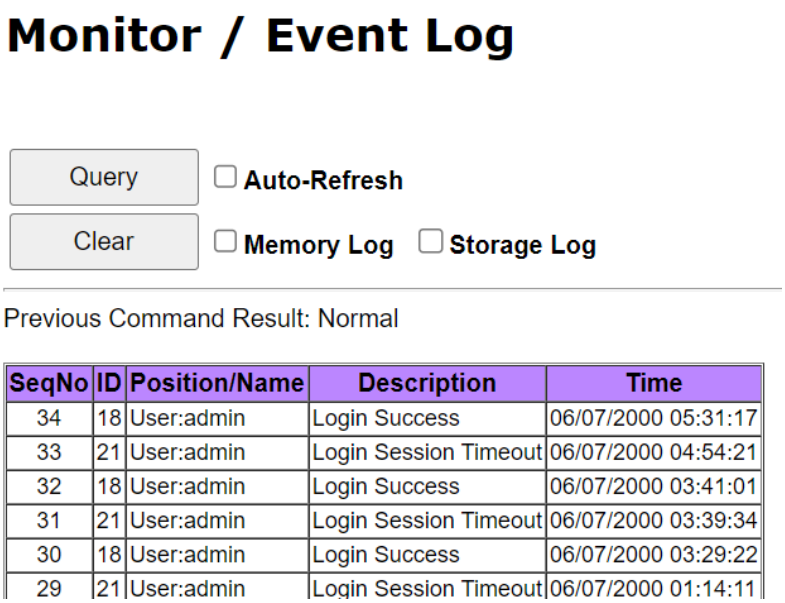


Alarm History



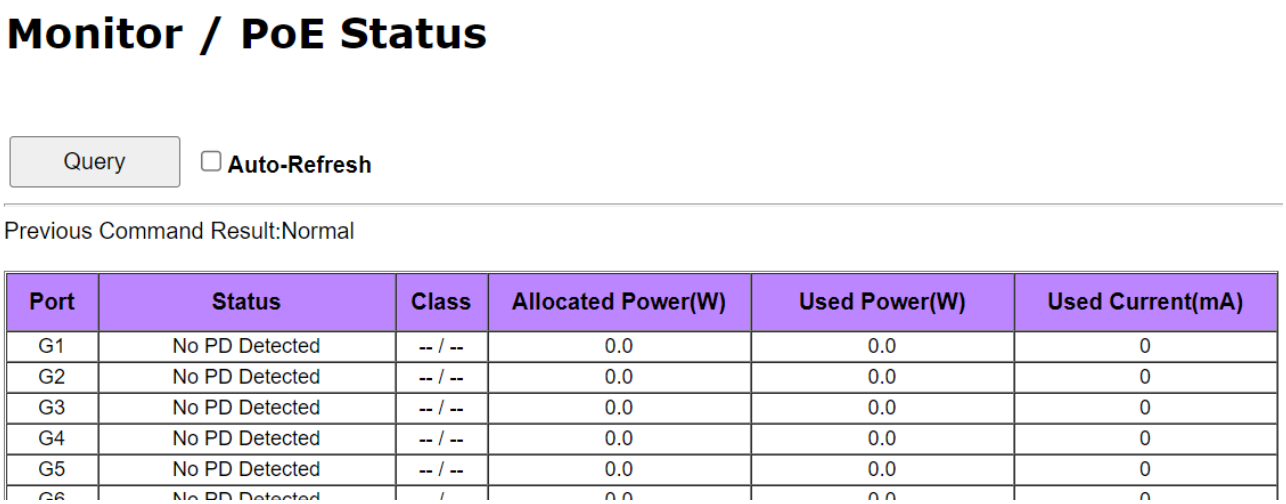
Operation	Refresh: 1. Click "Refresh" button to refresh data. Clear: 1. Click "Clear" to clear data.
Field	Description
SeqNo	Alarm Sequential Number.
ID	Alarm Type ID.
Description	Alarm Type Description.
Level	No matter alarm is major/minor, Alarm LED color always be red.
State	Alarm State. Value is Set/Cleared.
Time	Show the Time when the Alarm occurred.

2.4.5 Event Log



Operation	To Clear Event Log: Click "Clear" to clear data. To Refresh Event Log: Click "Refresh" button to refresh data.
Field	Description
SeqNo	Event Sequential Number.
ID	Event Type ID.
Description	Event Type Description.
Position/Name	Event Position/Name.
Time	Show the Time when the Event occurred.

2.4.6 PoE Status



Field	Description
Port	The user description of port that performs PoE function
Status	PoE Status. No Supported Power Budget Exceeded No PD Detected PD On PD Off PD Overload PoE Disabled PG Budget Exceeded PD Thermal Shutdown Unknown State
Class	PoE class level on the port. The class level is detected from PoE classification. There are 2 class level. The first one is the allocated class of the Primary alternative in case of SSPD or DSPD, range from 1 to 8. The second one is the allocated class of the Secondary alternative in case of DSPD, range from 1 to 5.

	Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W Class 5: Max. power 45.0 W Class 6: Max. power 60.0 W Class 7: Max. power 75.0 W Class 8: Max. power 99.0 W
Allocated Power (W)	The total power allocated for the PD, per port. The unit is Watt.
Used Power (W)	Power consumption which is really used by PD, per port. The unit is Watt.
Used Current (mA)	'Current' which is used by PD, per port. The unit is mA.

2.4.7 EEE

Monitor / EEE Status

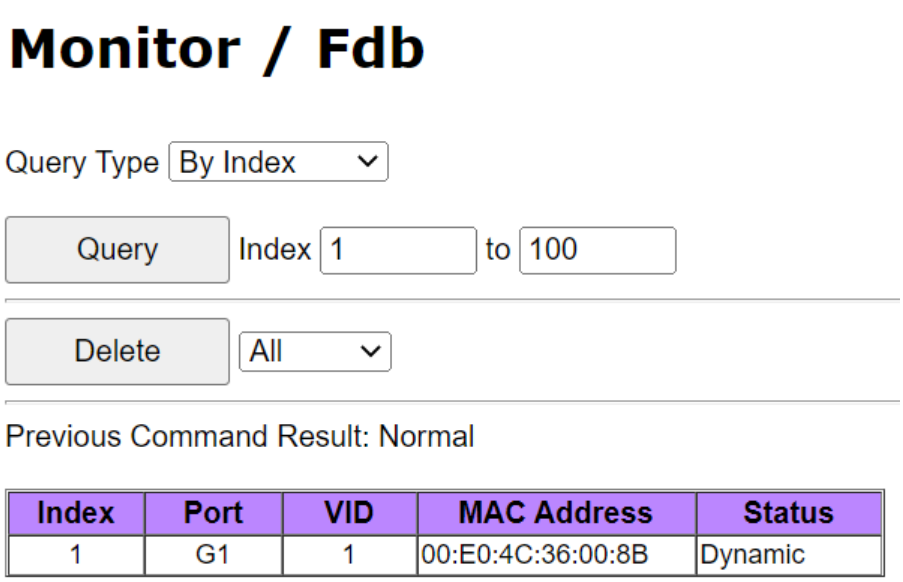
Query Auto-Refresh

Previous Command Result:Normal

Port	EEE Cap.	EEE Enable	LP EEE Cap.	LP Idle		LP idle indicate	
				Rx	Tx	Rx	Tx
G1	Yes	No	No	No	No	No	No
G2	Yes	No	No	No	No	No	No
G3	Yes	No	No	No	No	No	No
G4	Yes	No	No	No	No	No	No
G5	Yes	No	No	No	No	No	No
G6	Yes	No	No	No	No	No	No
G7	Yes	No	Yes	No	No	No	No
G8	Yes	No	No	No	No	No	No
G9	Yes	No	No	No	No	No	No

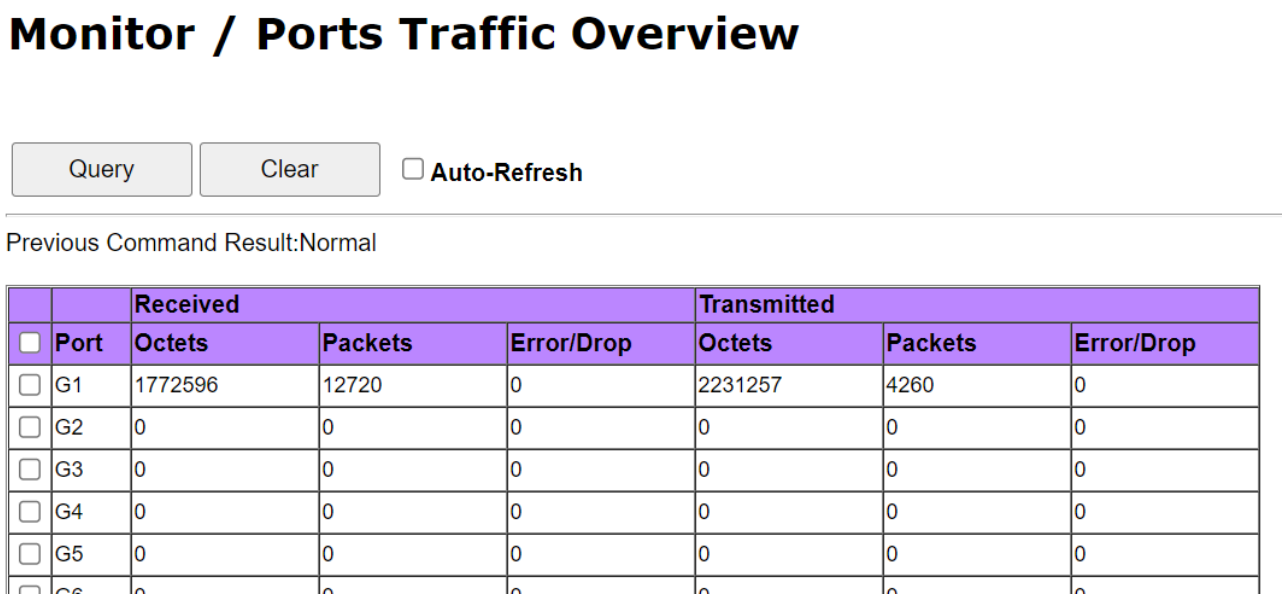
Field	Description
Port	The user description of port that monitor EEE status.
EEE Cap.	Show EEE capability status of local port(s).
EEE Enable	Indicate if EEE operating is enabled on the port.
LP EEE Cap.	Indicate if EEE capability is supported on the link partner.
LP idle.	RX - Rx PCS has received LP idle if yes; otherwise, LP Idle not received. TX - Tx PCS has received LP idle if yes; otherwise, LP Idle not received.
LP idle indicate.	RX - Rx PCS is currently receiving LP idle if yes; otherwise, PCS is not currently receiving LP idle. TX - Tx PCS is currently receiving LP idle if yes; otherwise, PCS is not currently receiving LP idle

2.4.8 Fdb



Operation	Query: 1. Select a Query Type 2. Fill condition for query record 3. Click “Query” button to query Delete: 1. Select delete type (All/ By VID/By Port) 2. Fill delete condition 3. Click “Delete” to delete data.
Field	Description
Port	Port description, include physical port and LAG interface.
VID	VLAN ID: 1~4094
MAC Address	Format xx:xx:xx:xx:xx:xx
Status	Data type: Dynamic/ Static

2.4.9 Ports - Traffic Overview



		Received			Transmitted		
	Port	Octets	Packets	Error/Drop	Octets	Packets	Error/Drop
	G1	1772596	12720	0	2231257	4260	0
	G2	0	0	0	0	0	0
	G3	0	0	0	0	0	0
	G4	0	0	0	0	0	0
	G5	0	0	0	0	0	0

Operation	Query: Push "Query" button to show traffic overview of all ports. Clear: Support clearing port counter for specific ports. User can choose the check-box of the port counter to determine it will be cleared. And then push "Clear" button to clear these selected ports counter.
Field	Description
Port	Port identifier.
Octets	Specify the total octets for received and transmitted side.
Packets	Specify the total packets for received and transmitted side. This is sum of some unique counter, includes : unicast packets, multicast packets, broadcast packet and pause frames.
Drop/Error	For received side, this is sum of drop-event counter and rx-mac-error counter. For transmitted side, this indicates tx-mac-error counter.

2.4.10 Ports - Detail Statistics

Monitor / Port Ethernet Statistics

Query | Clear | Port : G1 | Auto-Refresh

Previous Command Result:Normal

Rx Octets/Packets	
Total Octets	1791157
Unicast Packets	5786
Broadcast Packets	4337
Multicast Packets	2726
Pasue Frames	0

Tx Octets/Packets	
Total Octets	2246322
Unicast Packets	4273
Broadcast Packets	0
Multicast Packets	21
Pause Frames	0

Rx/Tx Size Counter	
64Octets Packets	4835
65to127Octets	7742
128to255Octets Packets	1738
256to511Octets Packets	511
512to1023Octets Packets	1092
1024toMaxOoctets Packets	1225

Rx Error Counter	
Drop Event	0
UnderSize	0
Fragments	0
OverSize	0
Jabber	0
RxMAC Error	0
Bad CRC	0

Tx Error Counter	
Collisions	0
Excessive Collisions	0
Late Collisions	0
TxMAC Error	0

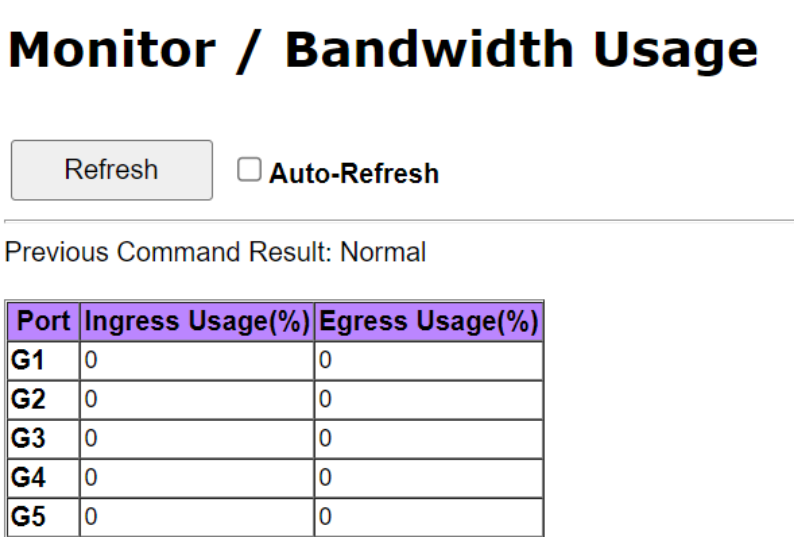
Operation	Query : Push "Query" button to show detail statistics for this port. Clear : Push "Clear" button to clear port statistics for this port.
Field	Description

Total Octets	Specified in Rx Octets/Packets table, It is number of ethernet frames received that are not bad ethernet frames or MAC Control pkts. This includes Bridge Control packets (LCAP, BPDU) Specified in Tx Octets/Packets table, it is sum of lengths of all good ethernet frames sent from this port. This does not include 802.3 Flow Control packets, packets dropped due to excessive collision or packets with a Tx Error.
Unicast Packets	Specified in Rx Octets/Packets table, It is number of Ethernet Unicast frames received that are not bad Ethernet frames or MAC Control packets. Note that this number includes Bridge Control packets such as LCAP and BPDU. Specified in Tx Octets/Packets table, it is number of good frames sent that had a Unicast destination MAC Address.
Broadcast Packets	Specified in Rx Octets/Packets table, It is total number of undamaged packets received that were directed to the broadcast address. Specified in Tx Octets/Packets table, it is total number of good packets sent that have a broadcast destination MAC address. This does not include 802.3 Flow Control packets, packets dropped due to excessive collision or packets with a Tx Error.
Multicast Packets	Specified in Rx Octets/Packets table, It is total number of undamaged packets received that were directed to a multicast address. Specified in Tx Octets/Packets table, it is total number of good packets sent that have a multicast destination MAC address. This does not include 802.3 Flow Control packets, packets dropped due to excessive collision or packets with a Tx Error.
Pause Frames	Specified in Rx Octets/Packets table, It is number of good Flow Control frames received. Specified in Tx Octets/Packets table, it is number of Flow Control frames sent.

64Octets Packets	Total number of received and transmitted undamaged and damaged frames which are 64 bytes in size. This does not include MAC Control Frames.
65to127Octets Packets	Total number of received and transmitted undamaged and damaged frames which are 65 to 127 bytes in size. This does not include MAC Control Frames.
128to255Octets Packets	Total number of received and transmitted undamaged and damaged frames which are 128 to 255 bytes in size. This does not include MAC Control Frames.
256to511Octets Packets	Total number of received and transmitted undamaged and damaged frames which are 256 to 511 bytes in size. This does not include MAC Control Frames.
512to1023Octets Packets	Total number of received and transmitted undamaged and damaged frames which are 512 to 1023 bytes in size. This does not include MAC Control Frames.
1024toMaxOoctets Packets	Total number of received and transmitted undamaged and damaged frames which are more than 1024 bytes in size. This does not include MAC Control Frames.
Drop Event	Total Number of instances that the port was unable to receive packets due to insufficient bandwidth to one of the packet processor internal resources, such as the DRAM or buffer allocation.
UnderSize	Total number of undersize packets received.
Fragments	Total number of fragments received.
OverSize	Total number of oversize packets received.
Jabber	Total number of jabber packets received.
RxMAC Error	Total number of Rx Error events seen by the receive side of the MAC.
Bad CRC	Total number of CRC error events.
Collisions	Total number of collisions seen by the MAC.
Excessive Collisions	Total number of frames dropped in the transmit MAC due to excessive collisions. This is an applicable for Half-Duplex mode only.
Late Collisions	Total number of late collisions seen by the MAC.

TxMAC Error	Total number of frames not transmitted correctly or dropped due to internal MAC Tx error.

2.4.11 Ports - Bandwidth Usage



Monitor / Bandwidth Usage

Refresh Auto-Refresh

Previous Command Result: Normal

Port	Ingress Usage(%)	Egress Usage(%)
G1	0	0
G2	0	0
G3	0	0
G4	0	0
G5	0	0

Operation	Refresh: Click “Refresh” button to refresh current data.
Field	Description
Port	The interface port number.
Ingress Usage(%)	The ingress bandwidth rate percentage with port capacity.
Egress Usage(%)	The egress bandwidth rate percentage with port capacity.

2.4.12 Ports - RMON Statistics

Monitor / RMON Statistics

Refresh Auto-Refresh

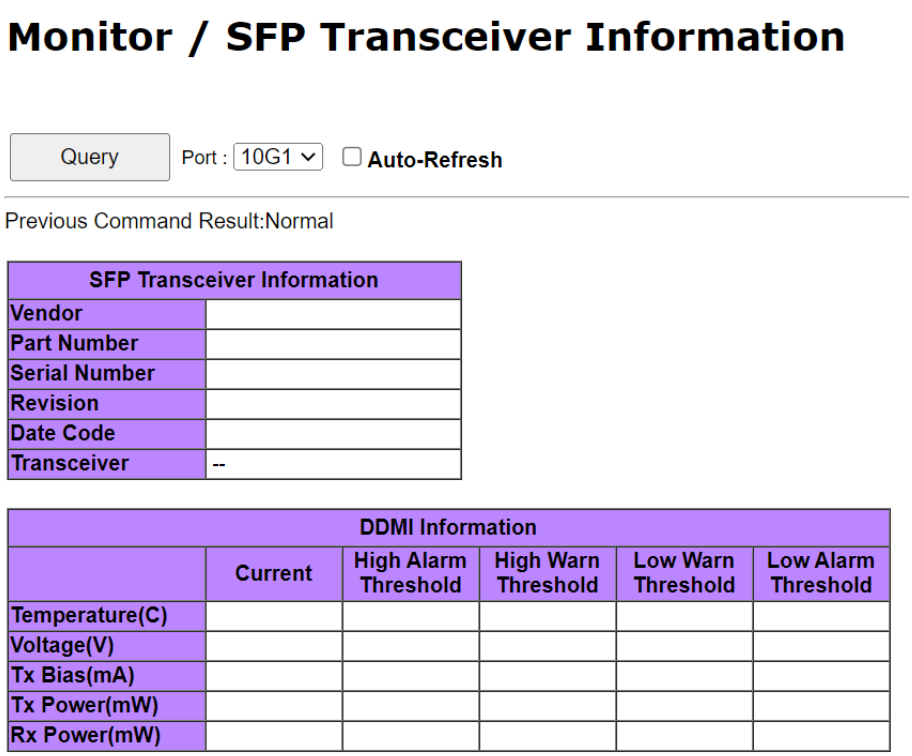
Previous Command Result: Normal

ID	ifIndex	Drop	Octets	Pkts	Broadcast	Multicast	CRC Errors	Undersize	Oversize	Fragments	Jabber	Collisions	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ max
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	7	0	255619489	2263468	749370	1490856	0	0	0	0	0	0	609702	1324063	237348	51490	25147	15718

Operation	Query: Push "Refresh" button to update statistics for all ports.
Field	Description
ID / ifIndex	Port interface index.
Drop	Total Number of instances that the port was unable to receive packets due to insufficient bandwidth to one of the packet processor internal resources, such as the DRAM or buffer allocation.
Octets	It is number of ethernet frames received that includes Bridge Control packets (LCAP, BPDU), does not include 802.3 Flow Control packets, packets dropped due to excessive collision or packets with an Error.
Pkts	The number of packets of unicast, broadcast, and multicast.
Broadcast	The number of packets of broadcast.
Multicast	The number of packets of multicast.
CRC Errors	Total number of CRC error events.
Undersize	Total number of undersize packets received.
Oversize	Total number of oversize packets received.
Fragments	Total number of fragments received.
Jabber	Total number of jabber packets received.

Collisions	Total number of collisions, excessive collisions and late collisions.
64 Bytes	Total number of received and transmitted undamaged and damaged frames which are 64 bytes in size. This does not include MAC Control Frames.
65 ~ 127	Total number of received and transmitted undamaged and damaged frames which are 65 to 127 bytes in size. This does not include MAC Control Frames.
128 ~ 255	Total number of received and transmitted undamaged and damaged frames which are 128 to 255 bytes in size. This does not include MAC Control Frames.
256 ~ 511	Total number of received and transmitted undamaged and damaged frames which are 256 to 511 bytes in size. This does not include MAC Control Frames.
512 ~ 1023	Total number of received and transmitted undamaged and damaged frames which are 512 to 1023 bytes in size. This does not include MAC Control Frames.
1024 ~ max	Total number of received and transmitted undamaged and damaged frames which are more than 1024 bytes in size. This does not include MAC Control Frames.

2.4.13 DDMI



Monitor / SFP Transceiver Information

Query Port : 10G1 Auto-Refresh

Previous Command Result:Normal

SFP Transceiver Information	
Vendor	
Part Number	
Serial Number	
Revision	
Date Code	
Transceiver	--

DDMI Information					
	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)					
Voltage(V)					
Tx Bias(mA)					
Tx Power(mW)					
Rx Power(mW)					

Operation	"Manual Query" - Directly push "Query" button to get data manually. "Auto Refresh" - Choose check-box of "auto-refresh" field to get data per 3 second.
Field	Description
SFP Transceiver Information	
Vendor	Vendor name of this SFP device.
Part Number	Part number provided by SFP vendor.
Serial Number	Serial number provided by SFP vendor.
Revision	Revision level for part number provided by SFP vendor.
Date Code	SFP vendor's manufacturing date code.
Transceiver	Transceiver compatibility model.
DDMI Information	
Current	The current value of temperature, voltage, TX bias, TX power, and RX power.
High Alarm Threshold	The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

High Warn Threshold	The high warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Warn Threshold	The low warn threshold value of temperature, voltage, TX bias, TX power, and RX power.
Low Alarm Threshold	The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

2.4.14 RingV2 Status

Monitor / RingV2 Status

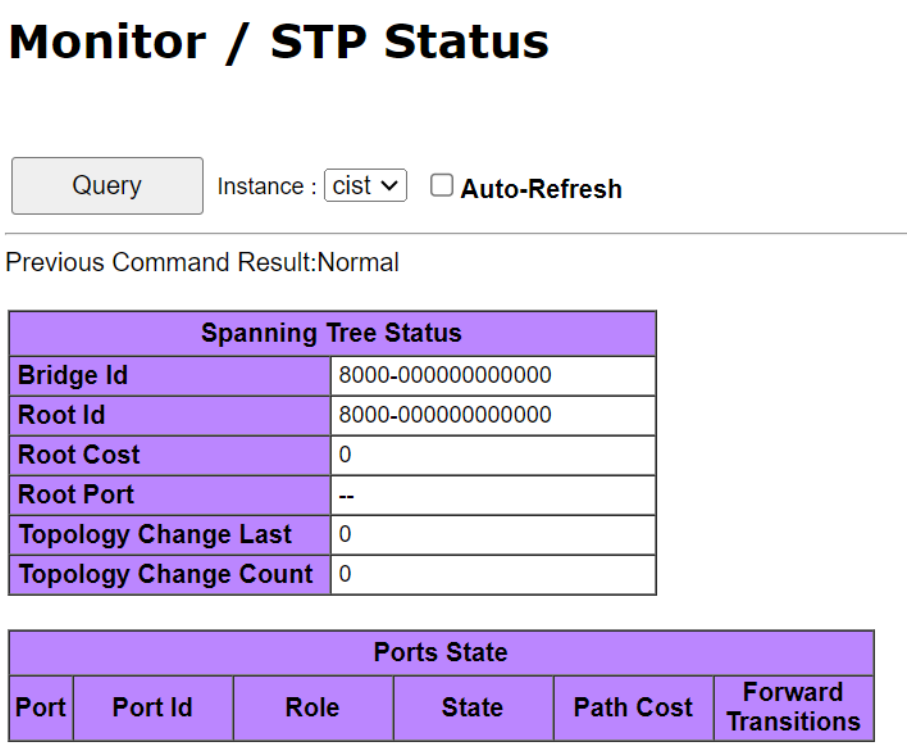
Query ☐ **Auto-Refresh**

Previous Command Result: Normal

Group index	Information
1	Mode : Disabled State : n/a Role : Ring(Slave) Node1 : G1 (Forward Port) Node2 : G2 (Forward Port)
2	Mode : Disabled State : n/a Role : Ring(Slave) Node1 : G3 (Forward Port) Node2 : G4 (Forward Port)
3	Mode : Disabled State : n/a Role : Chain(Member) Node1 : G1 (Member Port) Node2 : G2 (Member Port)
4	Mode : Disabled State : n/a Role : Coupling(Backup) Node1 : G5 (Backup Port)
5	Mode : Disabled State : n/a Role : Coupling(Backup) Node1 : G6 (Backup Port)
6	Mode : Disabled State : n/a Role : Coupling(Backup) Node1 : G7 (Backup Port)
7	Mode : Disabled State : n/a Role : Coupling(Backup) Node1 : G8 (Backup Port)
8	Mode : Disabled State : n/a Role : Coupling(Backup) Node1 : G9 (Backup Port)

Operation	Refresh: Click “Query” button to refresh current data.
Group Index	The group index. This parameter is used for easy to identify the ring when user to configure it.
Information	Show ring group's information.

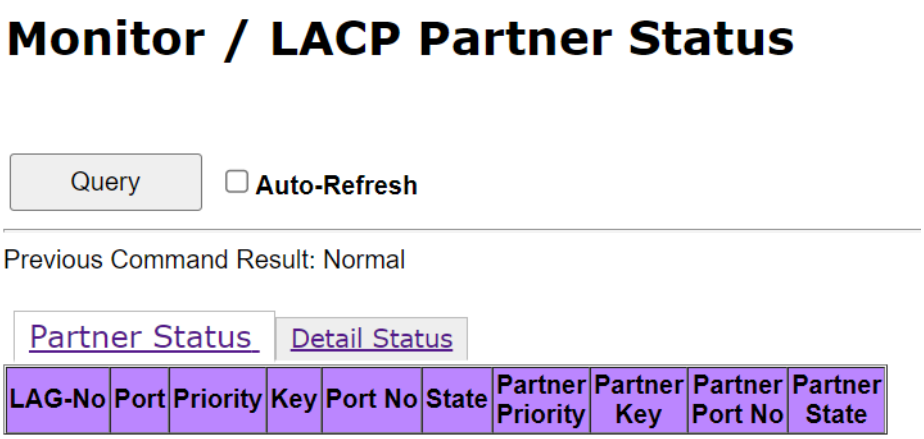
2.4.15 STP Status



Operation	Query: Push "Query" button to show information of this spanning tree instance.
Spanning Tree Status	
Bridge Id	Local bridge id of this spanning tree.
Root Id	Bridge id of root device for this spanning tree.
Root Cost	The distance what spent from local device to root device.
Root Port	The local port that goes through to root device.
Topology Change Last	The time since last topology change occur.
Topology Change Count	How many times that topology change occur since spanning tree start operating.
Ports State	
Port	Port description.
Port Id	The port id is used by STP stack. It is consisted of port priority and logical port index of bridge port.

Role	Display the current port role. There are "Disable", "Root", "Designated", "Alternate", "Backup", "Master" and "Unknown".
State	Display the current port state. There are : "Disabled", "Blocking", "Listening", "Learning", "Forwarding", "Broken", "Err-Disable" and "Unknown". First 5 states are specified in STP standard document. The others three state are : "Broken" - When the bridge has detected the port that is malfunctioning it will place the port into the broken state. "Err-Disable" - When BPDU guard is enabled and receives BPDU on the port, port goes into "Err-Disable" state. This state is similar to "Blocking" state with discarding received BPDU. "Unknown" - When it detects unexpected situation occur, it goes into this state.
Path Cost	Display the current port path cost.
Forward Transitions	Display the transition count that the port goes into "Forwarding".

2.4.16 LACP Status



Monitor / LACP Detail Status

Query Auto-Refresh

Previous Command Result: Normal

Partner Status | Detail Status

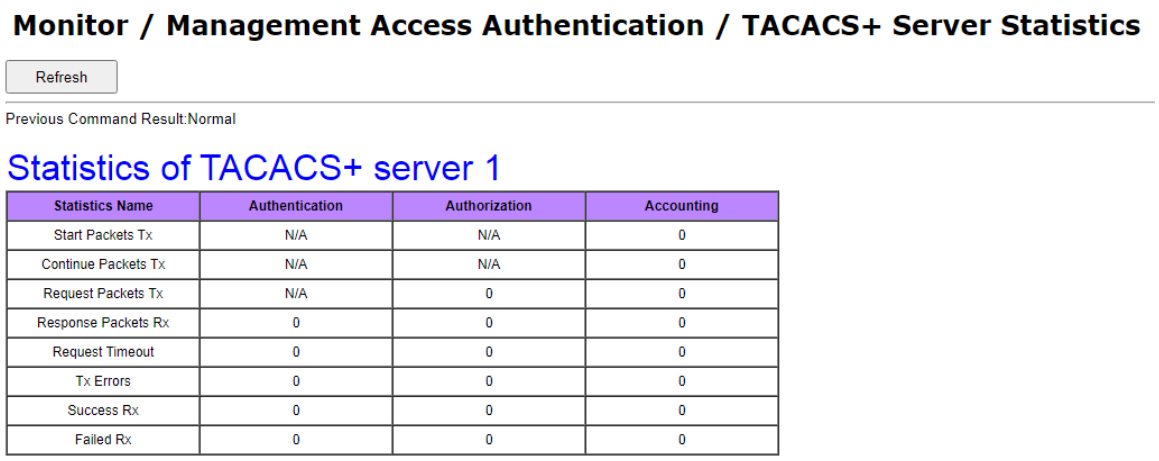
LAG-No	Actor					Partner				
	Port Number	Port priority	Admin Key	Oper Key	Port State	System ID	System Priority	Port Number	Port priority	Oper Key	Port State

Operation	Query LACP Status: 1.Click "Query" button to refresh LACP Status data.
Field	Description
LAG-No	The index of LACP aggregator. This specifies the LAGs are processing by LACP.
Actor Port Number	The port number assigned to the port. It is assigned by internal policy.
Actor Port Priority	The priority value assigned to the port, used to converge dynamic Key changes.
Actor Admin Key	The administrative value of Key assigned to this port by administrator or System policy. When "auto" is setting on the port, the key will be generated depended on link speed of physical port. When "specific" is setting on the port, user can configure the key value in the range of 1 to 65535.
Actor Oper Key	The operational value of Key assigned to this port by the Actor.
Actor Port State	The operational values of the Actor's state parameters. This consists of the following set of variables, encoded as individual bits within a single octet, as follows: 1) LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP is encoded as a 0. 2)LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout is encoded as a 0. 3) Aggregation is encoded in bit 2.

	If TRUE (encoded as a 1), this flag indicates that the System considers this link to be Aggregateable. If FALSE(encoded as a 0), the link is considered to be Individual. 4) Synchronization is encoded in bit 3. If TRUE (encoded as a 1), the System considers this link to be IN_SYNC. If FALSE(encoded as a 0), then this link is currently OUT_OF_SYNC. 5) Collecting is encoded in bit 4. TRUE (encoded as a 1) means collection of incoming frames on this link is definitely enabled. Its value is otherwise FALSE (encoded as a 0). 6) Distributing is encoded in bit 5. FALSE (encoded as a 0) means distribution of outgoing frames on this link is definitely disabled. Its value is otherwise TRUE (encoded as a 1). 7) Defaulted is encoded in bit 6. If TRUE (encoded as a 1), it is using Defaulted operational Partner information, administratively configured for the Partner. If FALSE (encoded as a 0), the operational Partner information in use has been received in a LACPDU. 8) Expired is encoded in bit 7. If TRUE (encoded as a 1), it indicates that the Actor's Receive machine is in the EXPIRED state; if FALSE (encoded as a 0), it indicates that the Actor's Receive machine is not in the EXPIRED state.
Partner System ID	The operational value of the MAC address component of the System Identifier of the Partner.
Partner System Priority	The operational value of the System Priority of the Partner.
Partner Port Number	The operational value of the port number assigned to this link by the Partner.
Partner Port Priority	The operational value of the priority value assigned to this link by the Partner, used to converge dynamic Key changes.
Partner Oper Key	The operational value of the Key value assigned to this link by the Partner.
Partner Port State	The operational value of the Actor's view of the current values of the Partner's state

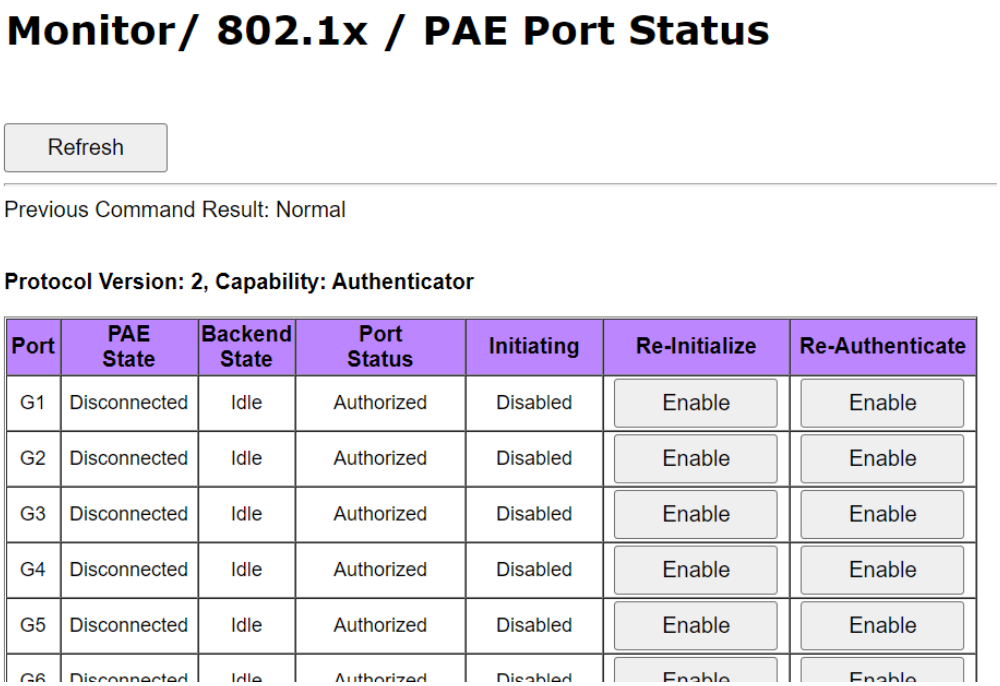
	parameters. The value consists of the following set of variables, as described in "Actor Oper Key".

2.4.17 TACACS+ Server Statistics



Operation	Refresh: Push "Refresh" button to refresh the page.
Field	**Description**
Start Packets Tx	Start Packets Tx Counter for Accounting
Continue Packets Tx	Continue Packets Tx for Accounting.
Request Packets Tx	Request Packets Tx for Authorization and Accounting
Response Packets Rx	Response Packets Rx for Authentication, Authorization and Accounting
Request Timeout	Request Timeout for Authentication, Authorization and Accounting
Tx Errors	Tx Errors for Authentication, Authorization and Accounting
Success Rx	Success Rx for Authentication, Authorization and Accounting
Failed Rx	Failed Rx for Authentication, Authorization and Accounting

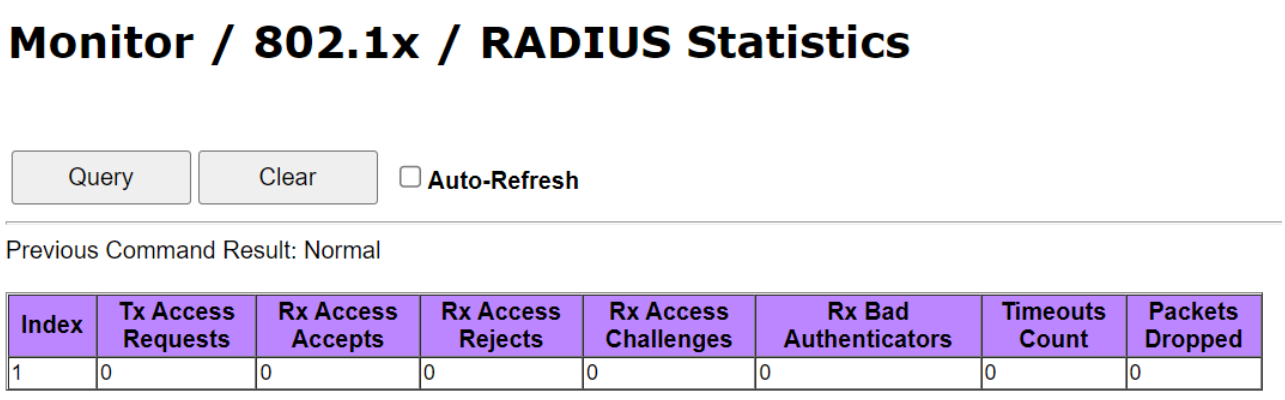
2.4.18 802.1x - PAE Port Status



Operation	Refresh: Click “Refresh” button to refresh current data.
Field	**Description**
Port	The index of PAE Port: Value Range 1 ~ MAX Number of Port.
PAE State	The authenticator status of PAE port: Possible state: Initialize Disconnected Authenticating Authenticated Aborting Held Force Auth Force Unauth
Backend State	The number of RADIUS Access-Accept received from RADIUS server. Range: 0~65535.

Rejects	The backend authenticator status of PAE port. Possible state: Initialize Idle Request Response Success Fail Timeout Ignore
Port Status	The authentication status of PAE port. Possible state: Authorized/Unauthorized
Initiating	Enable stands for force PAE port re-initialize. Disable stands for no action.
Re-Initialize	Set Enable to force PAE port re-initialize.
Re-Authenticate	Set Enable to force PAE port re-authenticate.

2.4.19 802.1x - RADIUS Statistics



Operation	Refresh: Click “Query” button to refresh current data. Clear:

	Click "Clear" button to reset the counters.
Field	Description
Index	The index of RADIUS Server: Current only support 1 RADIUS server
Requests	The number of RADIUS Access-Request sent to RADIUS server Range 0~65535.
Accepts	The number of RADIUS Access-Accept received from RADIUS server: Range 0~65535.
Rejects	The number of RADIUS Access-Reject received from RADIUS server: Range 0~65535.
Challenges	The number of RADIUS Access-Challenge received from RADIUS server: Range 0~65535.
Bad Authenticators	The number of invalid RADIUS response packet received from RADIUS server: Range 0~65535.
Timeout	The number of server Timeout happens on Backend Authentication state machine: Range 0~65535
Packets Dropped	The number of packet from RADIUS server to be silent drop by Authenticator Range 0~65535

2.4.20 802.1x - EAPOL Statistics

Monitor / 802.1x / EAPOL Statistics

Relatec

Refresh | Clear | Clear Type All

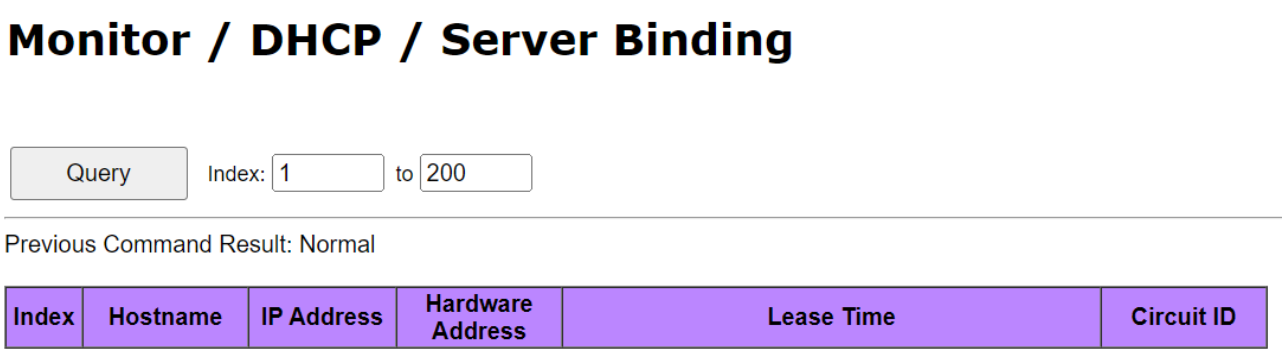
Previous Command Result: Normal

Port	Frame version	Frame Tx			Frame Rx						
		Total	ReqID	Req	Total	Start	Logoff	RespID	Resp	Invalid	Length Error
G1	0	0	0	0	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0	0	0	0	0
G3	0	0	0	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0	0	0	0	0

Operation	Clear: 1. Select "Clear Type". 2. If clear type is "Port", then select port number to be cleared. 3. Click "Clear" button.
Field	Description
Port	The index of PAE port: Value range 1 ~ MAX Number of port.
Protocol Version	The protocol version number carried in the most recently received EAPOL frame. Range 0~65535.
Frame Tx	The number of EAPOL frames of any type that has been transmitted. Range 0~65535.
Req Id Frame Tx	The number of EAP Req/Id frames that have been transmitted. Range 0~65535.
Req Frame Tx	The number of EAP Request frames (other than Req/Id frames) that have been transmitted. Range 0~65535.
Frame Rx	The number of valid EAPOL frames of any type that has been received. Range 0~65535.

Start Frame Rx	The number of EAPOL Start frames that have been received. Range 0~65535.
Logoff Frame Rx	The number of EAPOL Logoff frames that have been received. Range 0~65535.
Resp Id Frame Rx	The number of EAP Resp/Id frames that have been received. Range 0~65535.
Resp Frame Rx	The number of valid EAP Response frames(other than Resp/Id frames) that have been received. Range 0~65535.
Invalid Frame Rx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized. Range 0~65535.
Length Error Frame Rx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid. Range 0~65535.

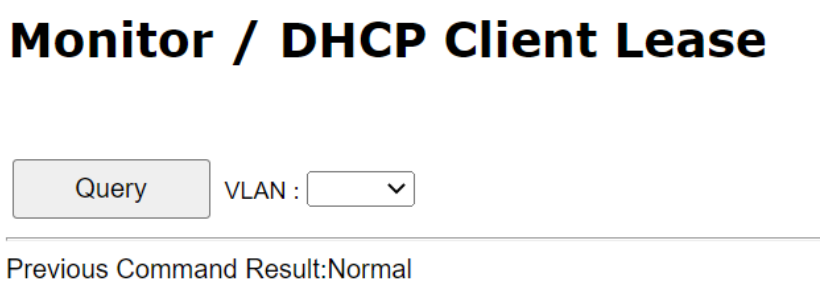
2.4.21 DHCP Server Binding



The DHCP Pool binding table contains the IP address, MAC address, start/end time and VLAN interface of DHCP Server in this switch. Select "Display All" to show all DHCP binding entries, or show specific binding per VLAN interface.

Operation	Query: 1. Select a VLAN interface 2. Modify query record range (Index range) 3. Click "Query" button to query and get DHCP Binding Status.
Field	**Description**
Index	Binding entries index.
Hostname	DHCP binding Hostname.
IP Address	Client's IP Address.
Hardware address	Hardware MAC address.
Lease time	DHCP Lease time.
Circuit ID	Agent Circuit ID.

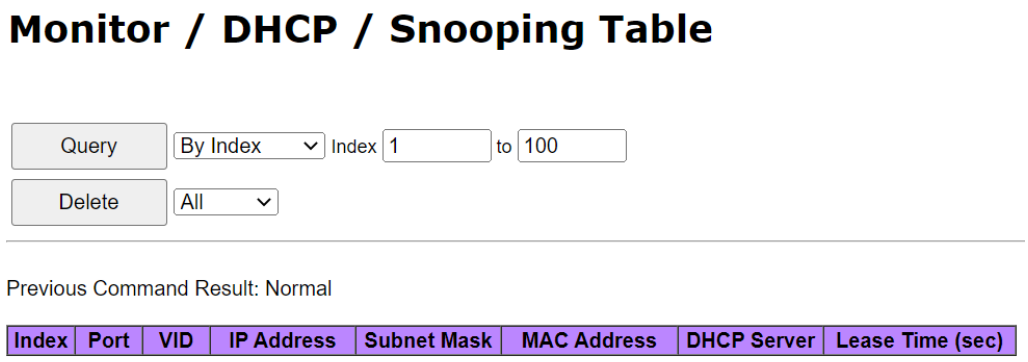
2.4.22 DHCP Client Lease



Field	Description
Index	Binding entries index.
State	Specify current state of this DHCP client. All states are as following table. INIT, SELECTING, REQUESTING, BOUND, RENEWING, REBINDING, INIT_REBOOT, REBOOTING: Defined in RFC2121-4.4 (DHCP client behavior). BOUND_ARP_CHECK: Before transit to "BOUND", trigger this state to confirm if leased IP is used by other client. This state is only available when "Check Lease IP" is configured as enabled. FALLBACK: When IP address is not available on local DHCP client, one temporal IP address is assigned on local device. This state is only available when "fallback IP address" is configured. NOT AVAILABLE: It is defined when any unexpected situation happens.
IP Address	IP address assigned by DHCP server. That is displayed in dotted-decimal notation. (ex:w.x.y.z)
IP Netmask	IP netmask assigned by DHCP server. That is displayed in dotted-decimal notation. (ex:w.x.y.z)
Default Gateway	The default gateway for this leased IP address. That is displayed in dotted-decimal notation. (ex:w.x.y.z)
Server Address	IP address of DHCP server that assign this leased IP. That is displayed in dotted-decimal notation. (ex:w.x.y.z)
Domain Name	Domain name specify where the leased IP allocated on.
DNS Address	The address that local device use to translate name address to numerical address. That is displayed in dotted-decimal notation. (ex:w.x.y.z)
Lease Time	Specify lease duration of this leased IP address.

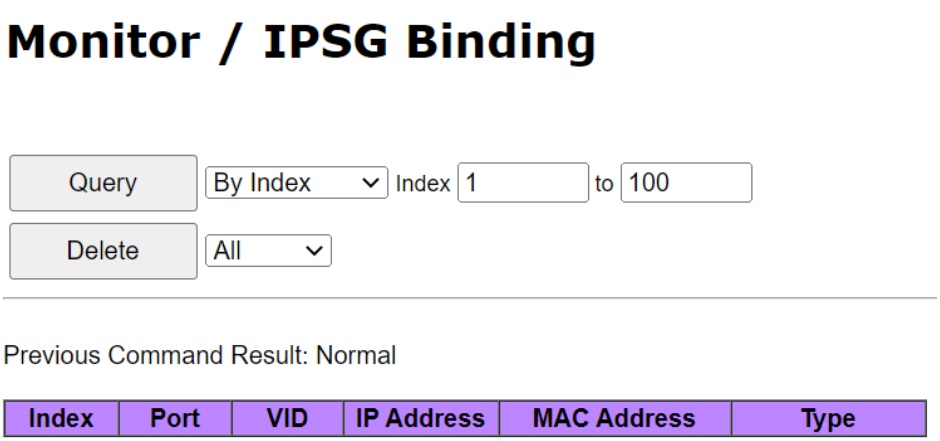
	This format is displayed as example - "Wed Nov 28 20:55:23 2000 ~ Thu Nov 29 00:55:23 2000"

2.4.23 DHCP Snooping Table



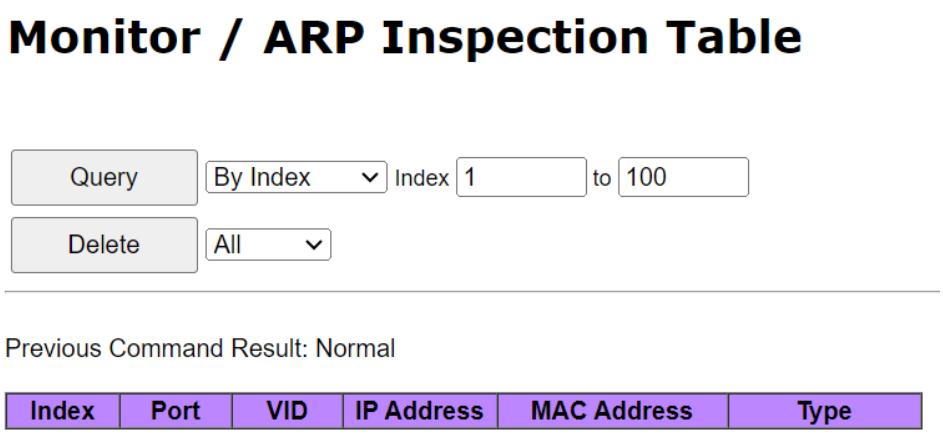
Operation	Query: Push "Query" button to show binding entries associated to specific type. Delete: Push "Delete" button to delete binding entries associated to the specific type.
Field	Description
Index	Index for this entry.
Port	Port identifier where the entry learned on.
VID	VLAN that entry is regarding.
IP Address	IP Address for this snooping leased entry.
Subnet Mask	Netmask Address for this snooping leased entry.
MAC Address	MAC Address for this snooping leased entry.
DHCP Server	IP Address of DHCP server that assign this lease.
Lease Time	Time associated to this lease that DHCP server agrees. This field is in unit of one second.

2.4.24 IPSG Binding



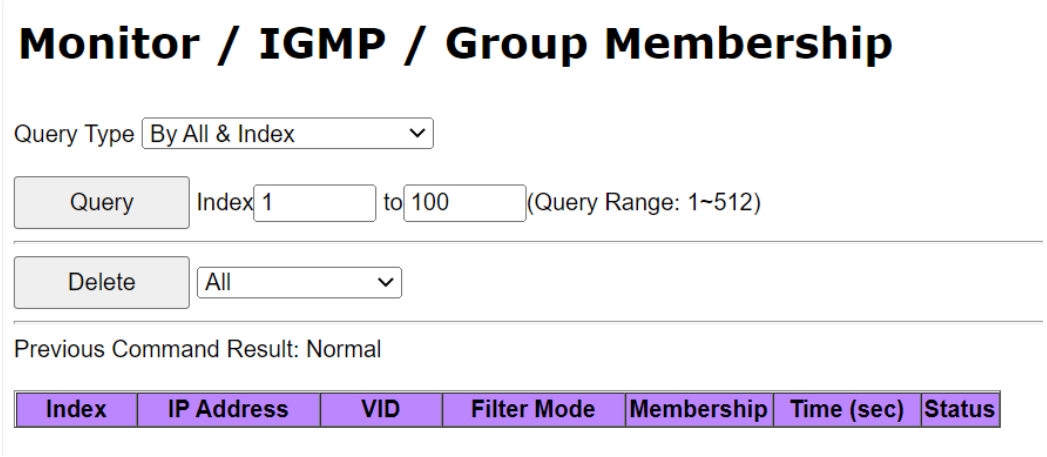
Operation	Query: Push "Query" button to show binding entries associated to specific type. Delete: Push "Delete" button to delete binding entries associated to the specific type.
Field	Description
Index	Index for this entry.
Port	Port identifier allowed for this entry.
VLAN	VLAN allowed for this entry.
IP Address	IP Address allowed for this entry.
MAC Address	MAC Address allowed for this entry.
Type	Specify this entry how to be learned, include : "static" - this entry is manually configured. "dhcp-snooping" - this entry is dynamic learned by DHCP-Snooping process.

2.4.25 ARP Inspection Table



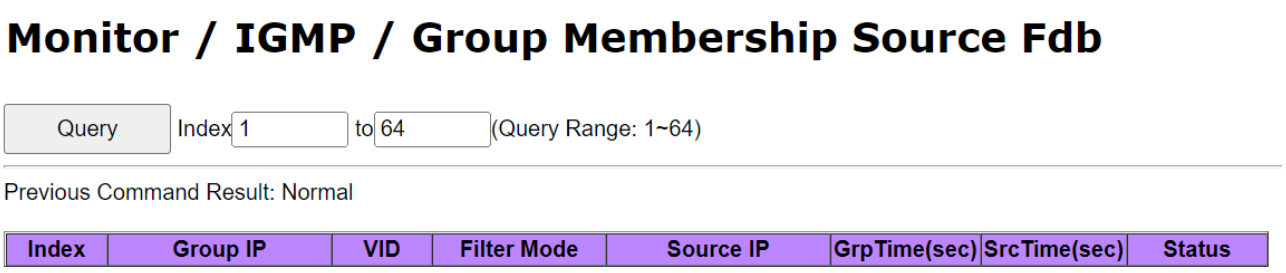
Operation	Query: Push "Query" button to show binding entries associated to specific type. Delete: Push "Delete" button to delete binding entries associated to the specific type.
Field	Description
Index	Index for this entry.
Port	Port identifier allowed for this entry.
VLAN	VLAN allowed for this entry.
IP Address	IP Address allowed for this entry.
MAC Address	MAC Address allowed for this entry.
Type	Specify this entry how to be learned, include : "static" - this entry is manually configured. "dhcp-snooping" - this entry is dynamic learned by DHCP-Snooping process

2.4.26 IGMP - Group Membership



Operation	Query: 1. Select a Query Type. 2. Fill Query condition. 3. Modify query record range (Index range). 4. Click "Query" button to query. Delete: 1. Select Delete Type 2. Fill VLAN ID when delete type is “By VID” 3. Select one membership when delete type is “By Membership” 4. Click “Delete” button to delete data.
Field	Description
Index	Index, value range 1~512
IP Address	Group IP Address.
VID	VLAN ID, range 1~4094
Filter Mode	Multicast FDB entry Filter Mode.
Membership	Bridge Port ID, range G1 ~ MAX Number of Port.
Time (sec)	Remain Time, unit is second
Status	Group Membership status, Dynamic or Static.

2.4.27 IGMP – Group Membership Source Fdb



Operation	To get IGMP Group Membership Source Fdb: 1. Select a Query Type. 2. Fill Query condition.(Index 1~64)
Field	Description
Index	Multicast Source FDB table. Max entry size: 64
Group IP	Multicast Source FDB group IP address.
VID	Multicast Source FDB VLAN ID, range 1~4094
Filter Mode	Multicast Source FDB Filter Mode: Include/Exclude In INCLUDE mode, the GroupRemainTime has no timeout. In EXCLUDE mode, the block list's source has no timeout.
Source IP	Source IP Address
GrpTime(sec)	Group Remain Time: if it shows "--", represents time is 0.
SrcTime(sec)	Source Remain Time: if it shows "--", represents time is 0.
Status	Multicast Source FDB entry type: Allow/Block

2.4.28 LLDP Neighbors

Operation	To Refresh LLDP Neighbors information: 1.Click "Refresh" to refresh.
Field	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Description	System Description is the name advertised by the neighbor unit.
TTL	TTL(Time to live) is the remaining time of the remote information. And this valid period is set to TxHold multiplied by TxInterval. (seconds)
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

2.4.29 LLDP Statistics

Monitor / LLDP Statistics

Refresh

Previous Command Result: Normal

LLDP Global Counters

Last Changed Time	Inserts	Deleted	Dropped	Aged Out
177759 seconds ago	0	0	0	0

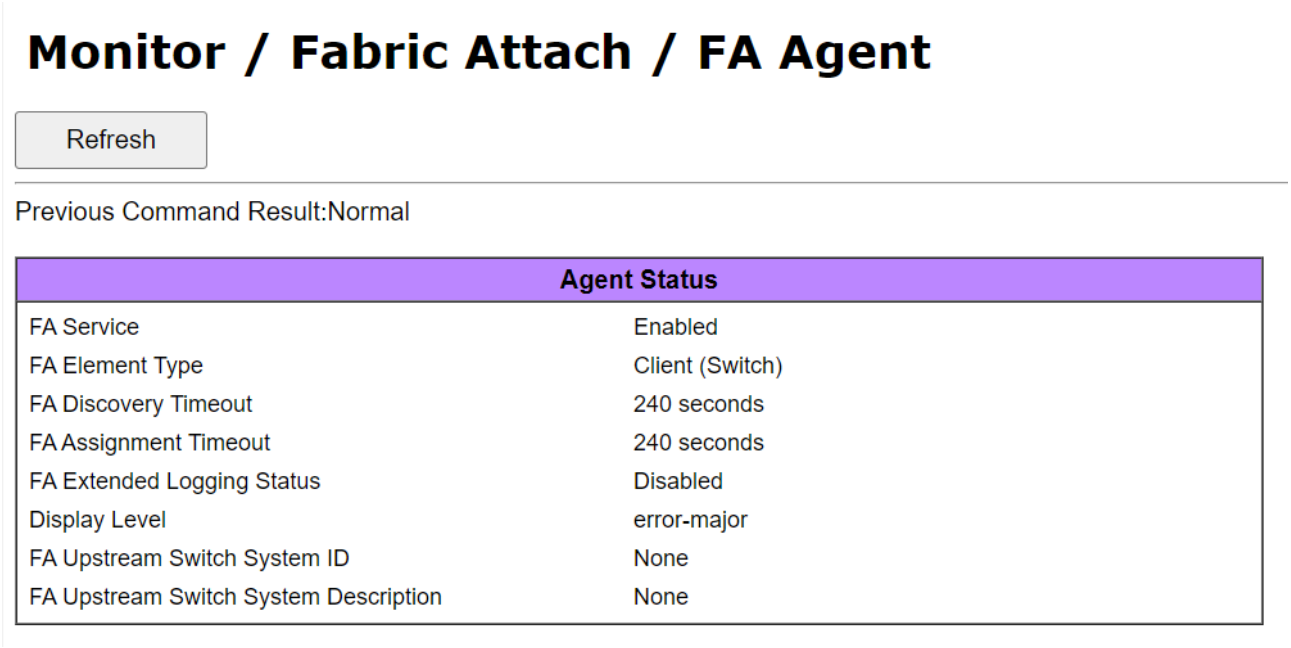
LLDP Statistics Local Counters

Port	Tx Frames	Rx Frames	Rx Errors	Rx Discarded	TLVs Discarded	TLVs Unknown	Age-Outs
G1	0	0	0	0	0	0	0
G2	0	0	0	0	0	0	0
G3	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0

Operation	To Refresh LLDP Global Counters, and LLDP Statistics Local Counters: Click "Refresh" to refresh.
Field	Description
Last Changed Time	Neighbor entries were last changed.
Inserts	Total Neighbors Entries Inserts.
Deleted	Total Neighbors Entries Deleted.
Dropped	Total Neighbors Entries Dropped.
Aged Out	Total Neighbors Entries Aged Out.
Port	The port index.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.

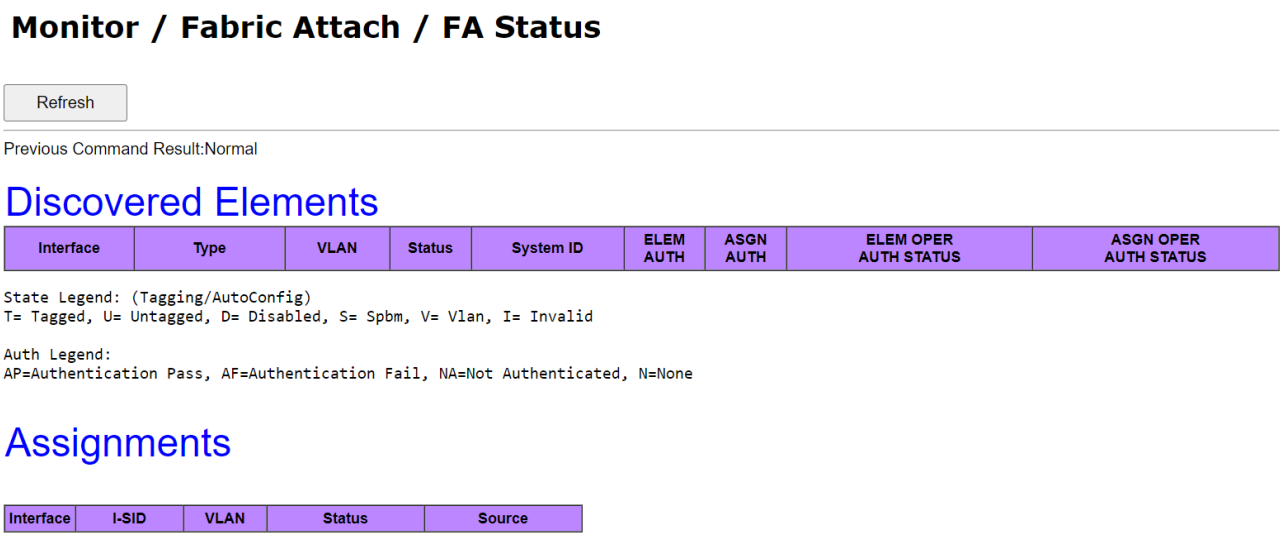
Rx Errors	The number of received LLDP frames containing some kind of error.
Rx Discarded	The number of received LLDP frames discarded.
TLVs Discarded	The number of received LLDP TLVs discarded.
TLVs Unknown	The number of received LLDP TLVs Unrecognized.
Age-Outs	The number of received LLDP frames Aged Out.

2.4.30 FA Agent



Operation	Refresh: Push "Refresh" button to refresh the page.
Field	Description
FA Service	Enabled or disabled.
FA Element Type	Element Type of this system.
FA Discovery Timeout	FA Discovery Timeout in seconds
FA Assignment Timeout	FA Assignment Timeout in seconds.
FA Extended Logging Status	Enabled or disabled.
Display Level	FA Message Display Level.
FA Upstream Switch System ID	System ID of the FA Upstream Stream.
FA Upstream Switch System Description	System Description of the FA Upstream Stream

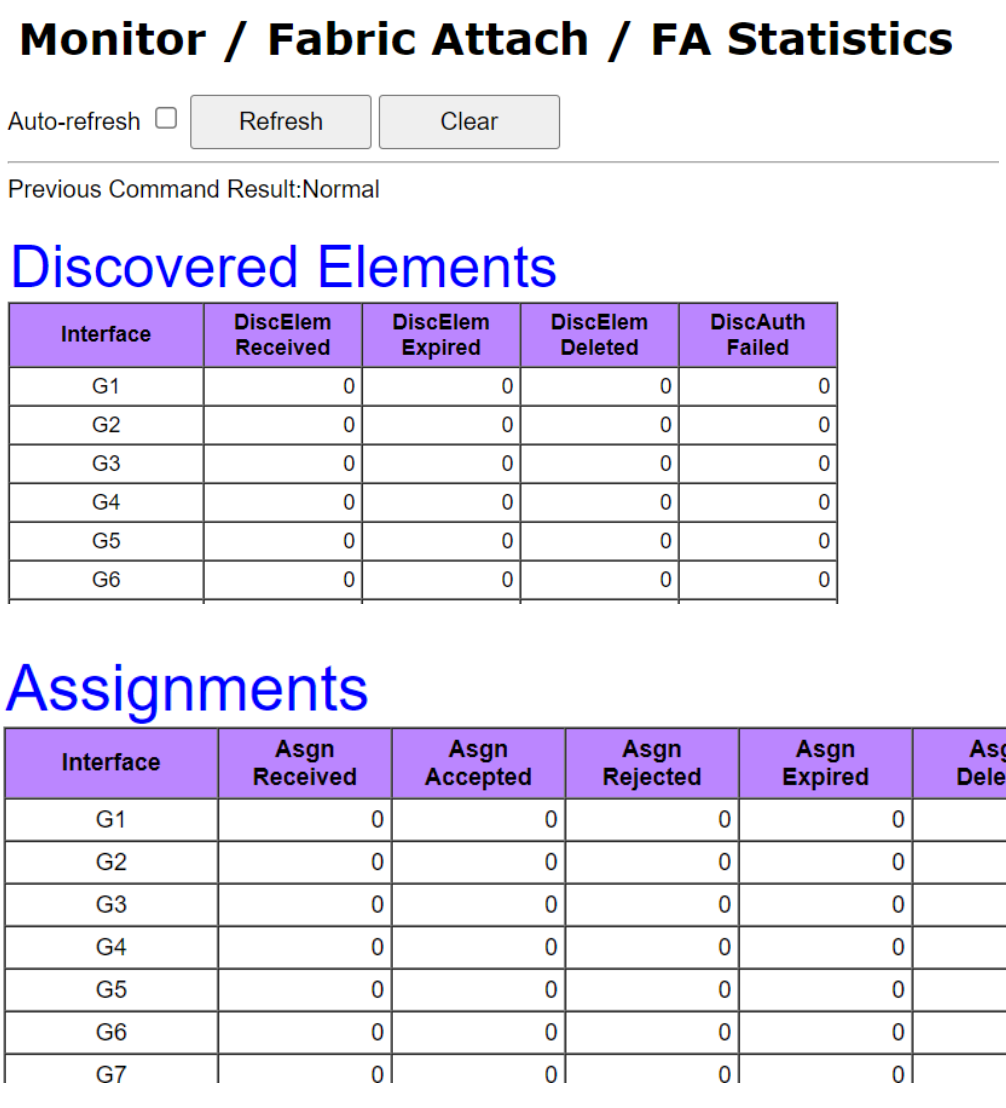
2.4.31 FA Status



Operation	Refresh: Push "Refresh" button to refresh the page.
Field	Description
Discovered Elements	
Interface	The interface that the FA element was discovered.
Type	FA Element Type.
VLAN	Management VLAN
Status	Element State
System ID	System ID of the element.
ELM AUTH	Element Authentication Status.
ASGN AUTH	Assignment Authentication Status.
ELEM OPER AUTH STATUS	Element Detail Authentication Status
ASGN OPER AUTH STATUS	Assignment Detail Authentication Status
Assignments	
Interface	The interface that the assignment was advertised.

I-SID	I-SID value.
VLAN	VLAN ID
Status	Assignment Status
Source	Source of the assignment.

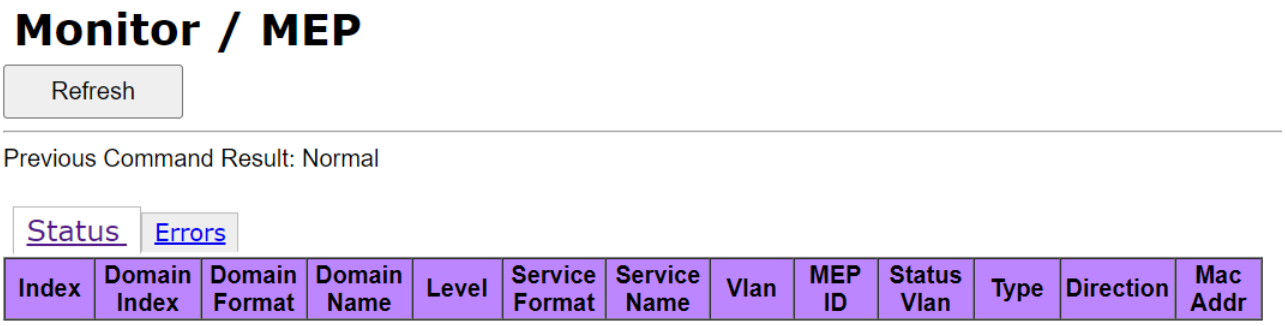
2.4.32 FA Statistics

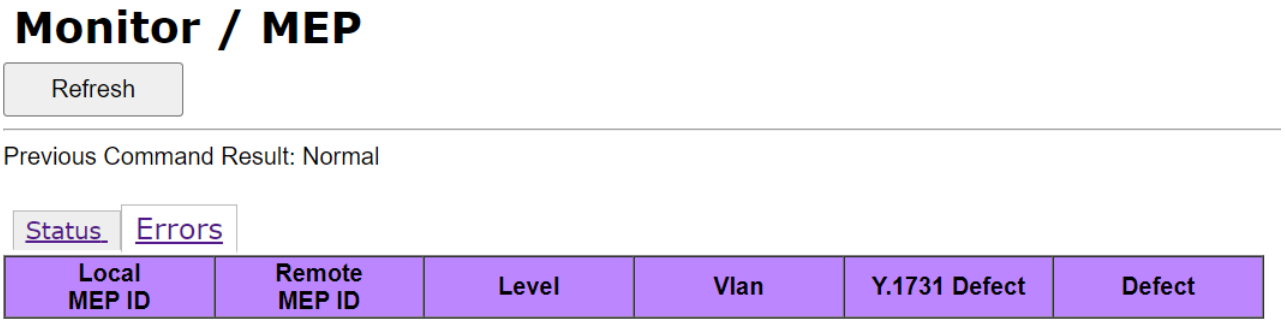


Operation	Refresh: Push "Refresh" button to refresh the page. Auto Refresh: Click "Auto Refresh" checkbox to start / stop auto-refresh.

	Clear: Push "Clear" button to clear all statistics counters.
Field	Description
Interface	The name of the interface
DiscElem Received	The number of received discovered elements.
DiscElem Expired	The number of times discovered elements expires.
DiscElem Deleted	The number of times discovered elements were deleted.
DiscAuth Failed	The number of times discovered elements with authentication failure.
Asgn Received	The number of times assignment TLVs received.
Asgn Accepted	The number of times assignments were accepted.
Asgn Rejected	The number of times assignments were rejected.
Asgn Expired	The number of times assignments expired.
Asgn Deleted	The number of times assignments deleted.
AsgnAuth Failed	The number of times assignment TLVs with authentication failure.

2.4.33 MEP Status

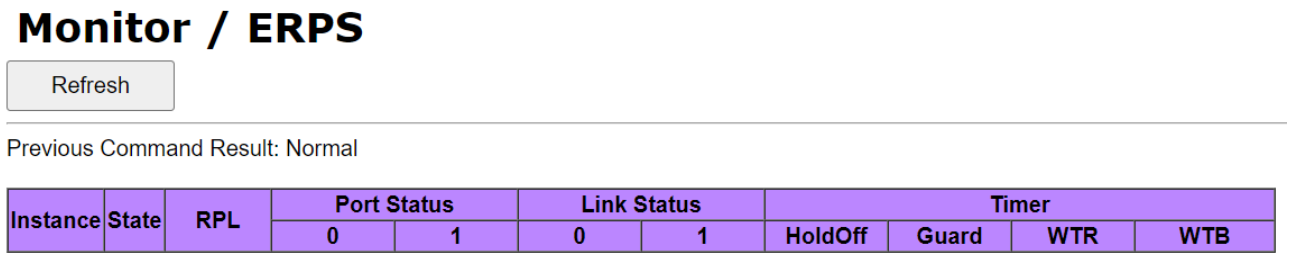




Operation	Refresh: Push "Refresh" button to refresh the page.
Field	Description
Status	
Index	MEP index ID.
Domain Index	Domain MEP index ID.
Domain Format	Domain name format.
Domain Name	ERPS domain name.
Level	MEP level
Service Format	Service name format.
Service Name	MEP service name.
Vlan	MEP vlan
MEP ID	MEP ID

Status Vlan	Status VLAN
Type	Action type
Direction	MEP control message direction
Mac Addr	MAC address
Errors	
Local MEP ID	Local MEP ID
Remote MEP ID	Remote MEP ID
Level	MEP level
Vlan	MEP VLAN
Y.1731 Defect	Y.1731 Defect
Defect	Defect

2.4.34 ERPS Status

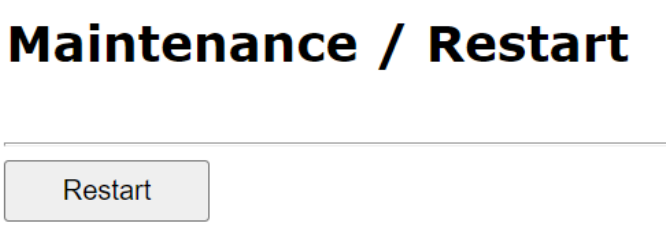


Operation	Refresh: Push "Refresh" button to refresh the page.
Field	Description
Instance	Display the instance
State	Display the state
RPL	Display RPL information
Port Status 0	Display port status 0
Port Status 1	Display port status 1
Link Status 0	Display link status 0
Link Status 1	Display link status 1

HoldOff	Hold off timer value configuration
Guard	Guard Interval to prevent reception of outdated RAPS messages.
WTR	The period of the WTR time can be configured by the operator
WTB	The period of the WTB time can be configured by the operator.

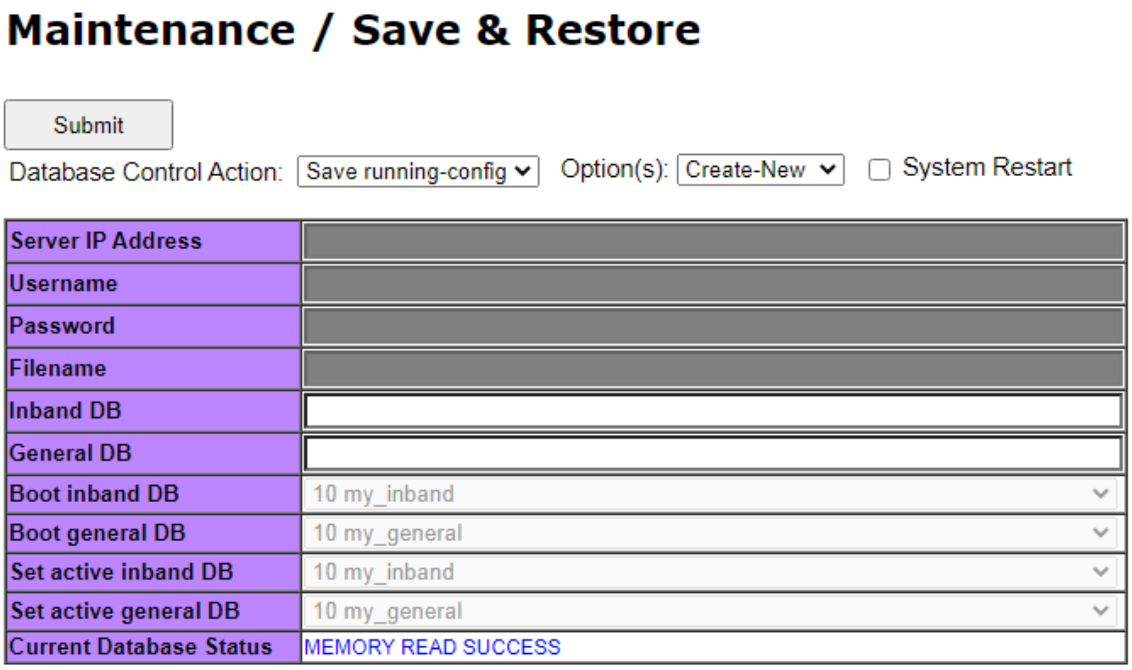
2.5 Maintenance

2.5.1 Restart



Operation	Restart: Click “Restart” button will restart the system

2.5.2 Save & Restore



Operation	Submit: 1. Select Control Action. 2. Fill necessary data for action. 3. Click “Submit” button to start the instruction.

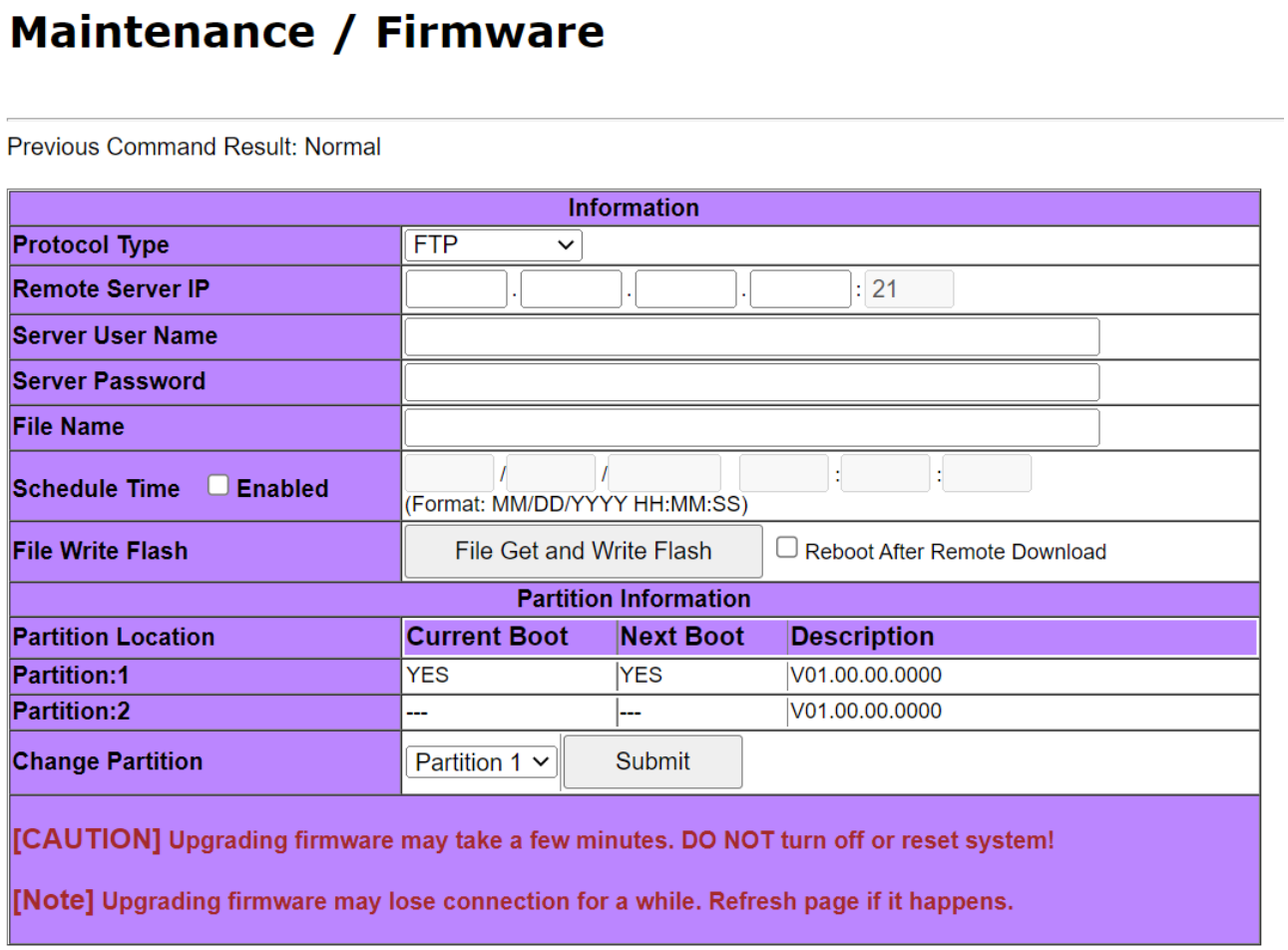
Field	Description
Database Control action	Select Database control. Save running config (*)Save inband configuration and runtime configuration as the active restoration database for next power-on restoration: (*)Save inband configuration and runtime configuration as the active restoration database for next power-on restoration and system restart: This option allows you to save inband configuration and runtime configuration as the active restoration database for next power-on restoration. You can specify the configuration database name for saving or not. And you can specify the same or different name for inband DB and general DB. After you click on Submit, the system starts to write runtime configuration to flash. The Current Database Status shows "Memory write in progress". While configuration is saved successfully, Current Database Status will show "Memory write success", and you will see the filename you save (if you have specified) appear in the Set active inband DB Set active general DB. (*)Save running config to flash and replace the specified backup: (*)Save running config to flash and replace the specified backup and system restart: It is the same as Save running config. The only difference is that it replaces an existing flash backup instead of creating a new entry. Select active DB (*)Restore inband configuration and control plane configuration by setting another restoration database active: (*)Restore inband configuration and control plane configuration by setting another restoration database active and system restart: These two options allow you to restore inband configuration and control plane configuration (other general configuration) by setting another restoration database active. Click on Set active inband DB and Set active general DB drop-down list to select the database you want to restore. There are up to 16 inband and general databases respectively for you to select. Click on Submit button. Clear active DB (*)Clear active DB including inband: (*)Clear active DB including inband and restart: These two options allow you to clear inband configuration and control plane configuration (general configuration) in the active restoration database (Warn:

	runtime configuration is also cleared and inband configuration is lost). Click on Submit button. (*)Clear active DB excluding inband: (*)Clear active DB excluding inband and restart: These two options allow you to clear control plane configuration (general configuration) in the active restoration database (Warn: runtime configuration is also changed.). Click on Submit button. Export CLI config (*)Export runtime configuration in cli command format to FTP server: This option allows you to export runtime configuration in CLI command format to FTP server. Type in the FTP server's IP address, user name & password and specify the CLI command file name, then click on Submit button. Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show "FTP Put Success" (actually there will be two files config11 and config12 saved). (*)Export runtime configuration in cli command format to TFTP server: This option allows you to export runtime configuration in CLI command format to TFTP server. Type in the TFTP server's IP address and specify the CLI command file name, then click on Submit button. Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show "TFTP Put Success" (actually there will be two files config11 and config12 saved). (*)Export runtime configuration in cli command format to SCP server: This option allows you to export runtime configuration in CLI command format to SCP server. Type in the SCP server's IP address, user name & password and specify the CLI command file name, then click on Submit button. Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show "SCP Put Success" (actually there will be two files config11 and config12 saved). (*)Export runtime configuration in cli command format to USB-Flash: This option allows you to export runtime configuration in CLI command format to USB-Flash. Type in the CLI command file name, then click on Submit button. Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show "USB-Flash Put Success" (actually there will be two files config11 and config12 saved). (*)Export runtime configuration in cli command format to SFTP server:

	This option allows you to export runtime configuration in CLI command format to SFTP server. Type in the SFTP server's IP address, user name & password and specify the CLI command file name, then click on Submit button. Click on Database on the menu tree to refresh Current Database Status. While the CLI command file is exported successfully, the Current Database Status will show "SFTP Put Success" (actually there will be two files config11 and config12 saved). Import CLI config (*)Import database in cli command format from FTP server and set it to the active restoration database: (*)Import database in cli command format from FTP server and set it to the active restoration database and system restart: These two options allow you to import database in CLI command format from FTP server and set it to the active restoration database. Type in FTP server IP address, user name & password, CLI command file name, and then click on Submit button. (*)Import database in cli command format from TFTP server and set it to the active restoration database: (*)Import database in cli command format from TFTP server and set it to the active restoration database and system restart: These two options allow you to import database in CLI command format from TFTP server and set it to the active restoration database. Type in TFTP server IP address, CLI command file name, and then click on Submit button. (*)Import database in cli command format from SCP server and set it to the active restoration database: (*)Import database in cli command format from SCP server and set it to the active restoration database and system restart: These two options allow you to import database in CLI command format from SCP server and set it to the active restoration database. Type in SCP server IP address, user name & password, CLI command file name, and then click on Submit button. (*)Import database in cli command format from USB-Flash and set it to the active restoration database: (*)Import database in cli command format from USB-Flash and set it to the active restoration database and system restart: These two options allow you to import database in CLI command format from USB-Flash server and set it to the active restoration database. Type in CLI command file name, and then click on Submit button. (*)Import database in cli command format from SFTP server and set it to the active restoration database:

	(*)Import database in cli command format from SFTP server and set it to the active restoration database and system restart: These two options allow you to import database in CLI command format from SFTP server and set it to the active restoration database. Type in SFTP server IP address, user name & password, CLI command file name, and then click on Submit button.
Server IP Address	Input Server IP Address
Username	Input User Name to login Server
Password	Input Password to login Server
Filename	Input File Name for Import/Export file
Inband DB	Inband Backup Name (1 ~ 31 characters)
General DB	General Backup Name (1 ~ 31 characters)
Boot inband DB	Show the current inband database used for boot up
Boot general DB	Show the current general database used for boot up
Set active inband DB	Select the inband database to be used for boot up
Set active general DB	Select the general database to be used for boot up
Current Database Status	Display current status

2.5.3 Firmware



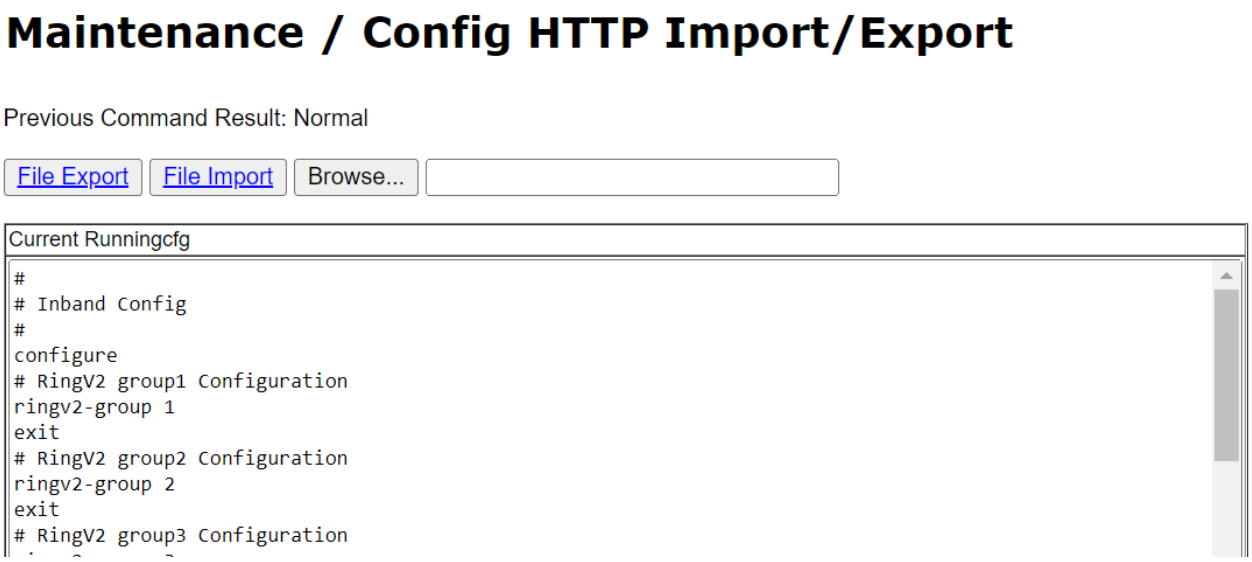
Operation	FTP Get and Write Flash: 1. Input FTP Server IP Address, user name and password for login 2. Select Schedule time checkbox and set schedule (optional) 3. Click “FTP Get and Write Flash” button will load firmware from remote server IP. **Note**: The firmware will be loaded and written to non-activated partition, if the Current Boot is partition 0, then new firmware will be written in partition1. If the “Reboot After Remote Download” is selected, system will restart itself when the firmware download is done. Submit: Click “Submit” button will change the partition for next system reboot. The system will use the selected partition for boot when it restarts. This “Submit” button only changes the boot partition, won’t restart system.
Field	Description

Protocol Type	Support multiple methods to download firmware file from remote server, include ftp, tftp, scp, sftp and usb-flash.
Remote Server IP	Type in the IP address of the server where the firmware is stored.
Server User Name	Type in a user name accepted by the server.
Server Password	Type in a password accepted by the server.
File Name	Type in the name of the firmware file (string length 1 ~ 64).
Schedule Time	Select Enable checkbox and type in the schedule time to update of the firmware file. The time format: MM/DD/YYYY HH:MM:SS
Get and Write Flash	After you have entered the server, user name, password and firmware file name, click this button to start the firmware update process.
Reboot After Remote Download	Select the checkbox if you want the system reboot automatically once the firmware update is finished.

2.5.4 Firmware HTTP Upload

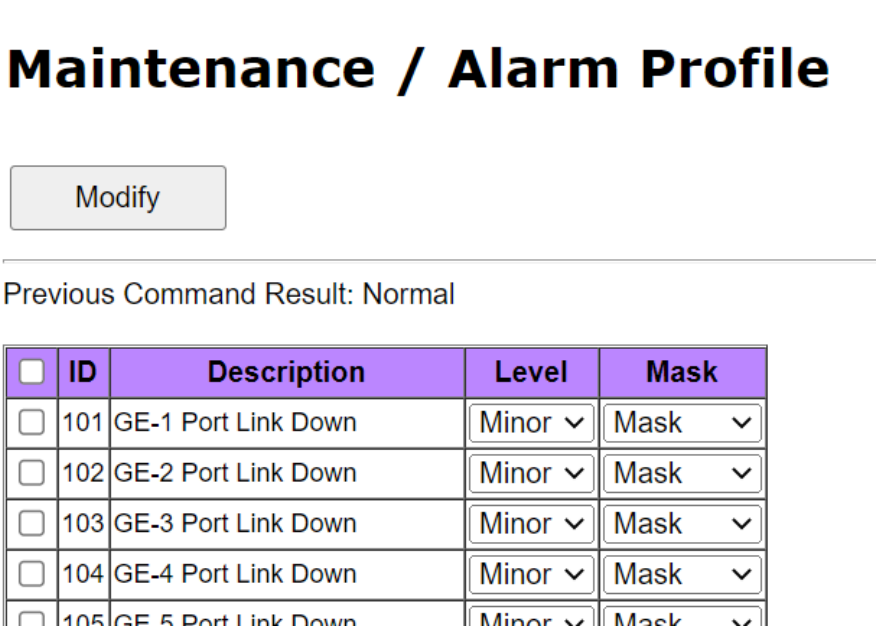
Operation	Use the Maintenance / HTTP Upload screen to upload firmware with HTTP. To Upload firmware: 1. Click "Browse" button to select config import file. 2. Select "Reboot after firmware upgraded" check box when we need to reboot the system. 3. Click "Upload" button to upload firmware.

2.5.5 Config HTTP Import/Export



Operation	Use the Maintenance / Config HTTP Import/Export screen to import or export config data. To File Export: 1. Click "File Export" button. 2. Select save file location and name. To File Import: 1. Click "Browse" button to select config import file. 2. Click "File Import" button to config import with file.

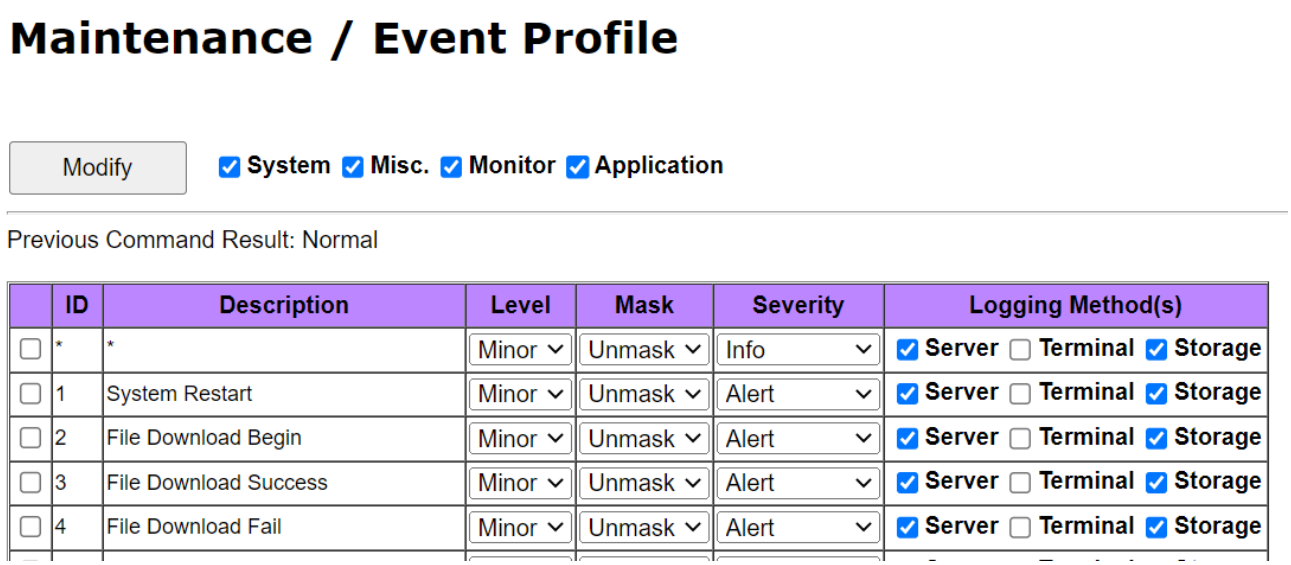
2.5.6 Alarm Profile



Operation	Modify Alarm Profile: 1. Select alarm entry with checkbox. 2. Modify Level and Mask if necessary Note: When any alarm exists, the Alarm LED will be light on, and Alarm Output Relay will also be enabled. 3. Click "Modify" button to modify data. Note: 1. When any one alarm exists, the Alarm LED will be lit. 2. Switch has 2 types Power Alarm: - System Power Feed Alarm: System has 2 inputs(2 power feeds), if only one power is supplied, Power Alarm occurs. (Default: Alarm masked) - PoE Power Budget Alarm: PoE Power Budget is measured by whole system, if total PoE Power used exceeds threshold, PoE Alarm occurs. (Default: PoE Alarm threshold is 75 percentage, Alarm unmasked.)
Field	Description
ID	Alarm Type ID.
Description	Alarm Type Description.
Level	When system has alarm, no matter alarm is major/minor, Alarm LED color always be red in Web Panel View. However, the HW Panel could show with Amber.

Mask	If alarm is masked, then alarm item will not be captured in alarm history/current; SNMP trap either. If specific alarm item is masked, then it will not trigger the Alarm LED on or off.

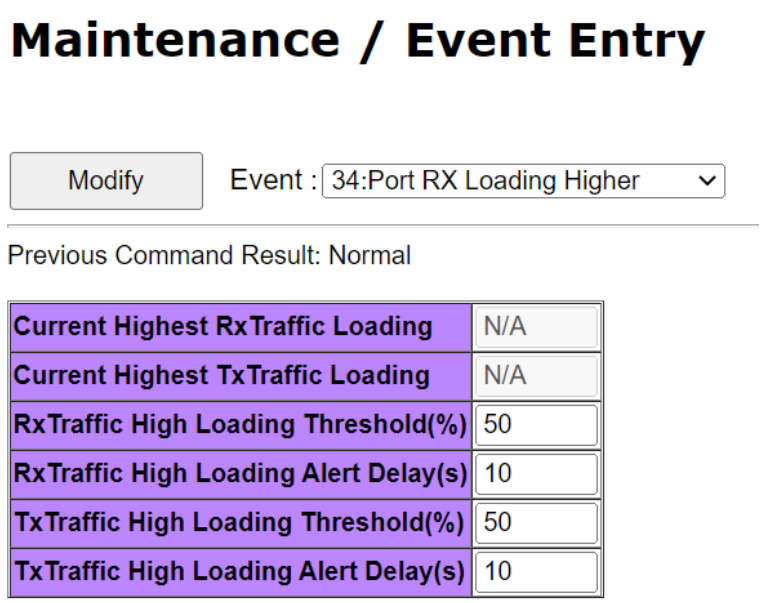
2.5.7 Event Profile



Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
ID	The number to identify the event.
Description	Simple description for one event.
Level	Use "Major" or "Minor" to mark one event as important or not.
Mark	Inform if it triggers event note while it happens. Ther are: 'Unmask' - It always trigger this event note while it happens. This is default action for all events. Mask' - It always ignore this event while it happens.
Severity	This is severity level for logging through syslog. There are: "Emergency/Alert/Critical/Error/Warning/Notice/Info". "Info" is used by default.
Logging Method(s)	Indicates how to log one event message while it happens. By default, all event messages only exist in dynamic memory. They will disappear when

	system restart. For debug purpose, it supports message logging to local or remote storage. There are: 'Server' - Save event message through syslog. 'Terminal' - Show event message on terminal. 'Storage' - Save event message to local storage while auto-saving mechanism is enabled.

2.5.8 Event Threshold

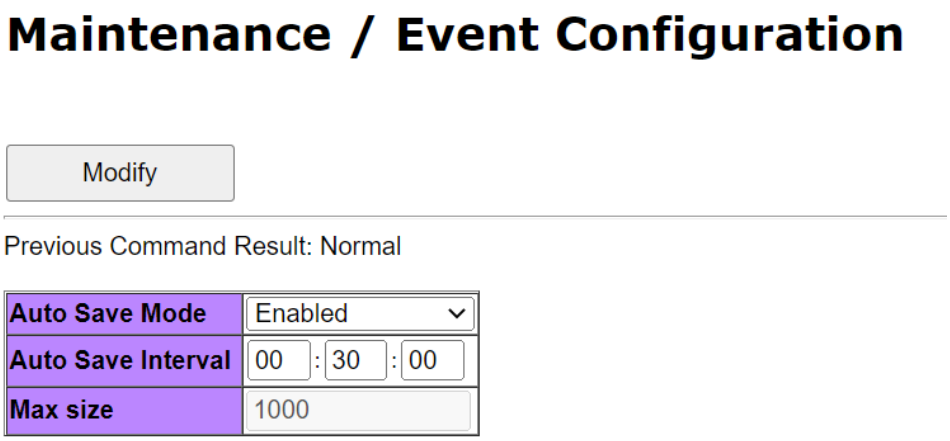


Operation	Push "Modify" button to apply new configuration when some fields' value change. Display "Success" when the changes are successfully applied. Display "Fail" when the changes are failed to applied.
Field	Description
Current Highest RxTraffic Loading	Show the port that has highest Rx traffic loading now.
Current Highest TxTraffic Loading	Show the port that has highest Tx traffic loading now.
RxTraffic High Loading Threshold	One threshold percentage to trigger high RX traffic loading alert.
RxTraffic High Loading Alert Delay(s)	A time gap between starting of detecting high RX traffic loading to continuous duration time.

	It supports the range of 10 to 300, in unit of one second. The default is 10.
TxTraffic High Loading Threshold	One threshold percentage to trigger high TX traffic loading alert.
TxTraffic High Loading Alert Delay(s)	A time gap between starting of detecting high TX traffic loading to continuous duration time. It supports the range of 10 to 300, in unit of one second. The default is 10.
Current System Temperature	Show current system temperature in unit of degrees Celsius.
High Temperature Threshold	Configure one threshold to indicate system temperature is too high. When current system temperature continues to equal or more than this threshold in duration time. System will alert "System temperature higher" that device may fail down since system temperature is closed to limitation. This support range of -55 to -85, in unit of degrees Celsius. The default is 65.
High Temperature Alert Delay (Seconds)	To avoid the short-instant high temperature then it causes meaningless event trigger. A time gap between the start of detecting high temperature to continuous duration time. And then it generates high temperature alert. This support range of 1 to 255, in unit of second. The default is 10.
Low Temperature Threshold	Configure one threshold to indicate system temperature is too low. When current system temperature continues to equal or less than this threshold in duration time. System will generate "System Temperature Lower" event to alert operator that device can fail down since system temperature is closed to limitation. This support range of -55 to 85, in unit of degrees Celsius. The default is -40.
Low Temperature Alert Delay (Seconds)	To avoid the short-instant low temperature then it causes meaningless event trigger. A time gap between the start of detecting low temperature to continuous duration time. And then it generates low temperature alert.
Current CPU Loading (%)	Show current CPU loading in unit of one percentage.
CPU Loading Threshold (%)	One threshold percentage to trigger high CPU loading alert.
Current Memory Loading (%)	Show current memory loading in unit of one percentage.

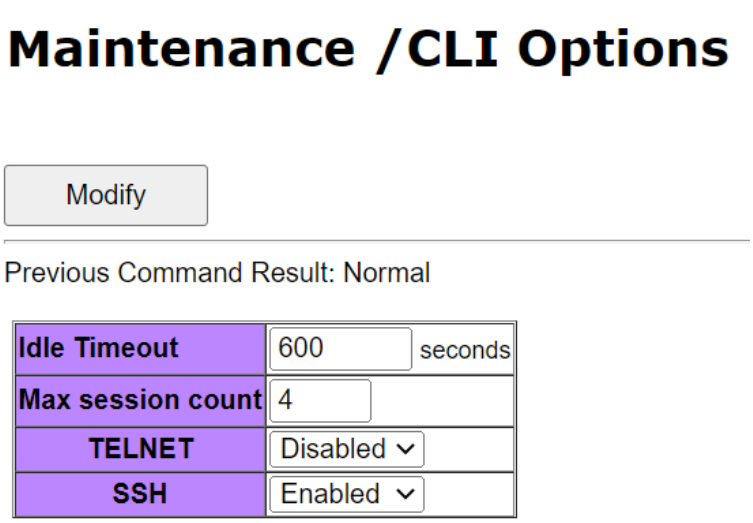
Memory Loading Threshold (%)	One threshold percentage to trigger high memory loading alert.
Current PoE Power Budge Loading (%)	Show current PoE power budge loading in unit of one percentage.
PoE Power Budge Loading Threshold (%)	One threshold percentage to trigger high PoE power budge loading alert.

2.5.9 Event Auto Save



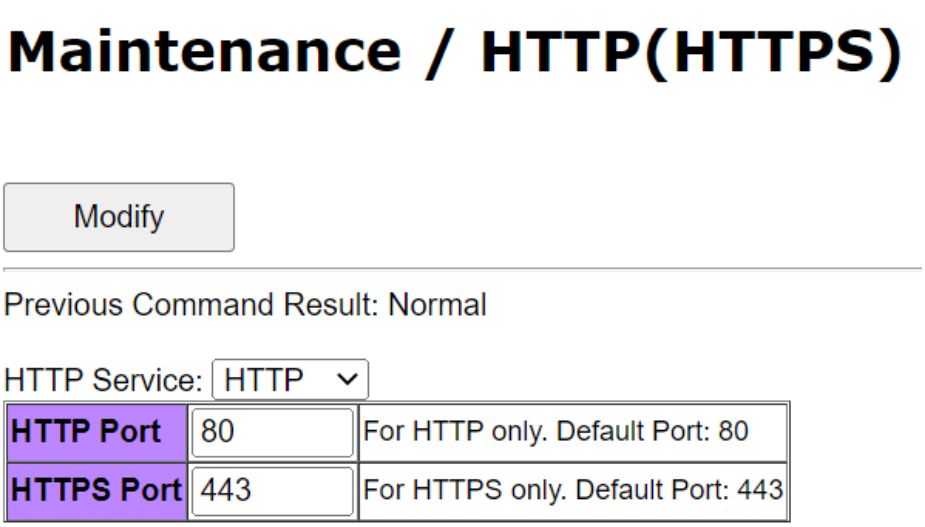
Operation	Push "Modify" button to apply new configuration when some fields' value change. Display "Success" when the changes are successfully applied. Display "Fail" when the changes are failed to applied.
Field	Description
Auto Save Mode	Configure capability of automatically saving events to flash storage. There are: Disabled : Disable auto saving. Enabled : Enable auto saving.(It is default.)
Auto Save Internal	Specify one timeout of that format is "HH:MM:SS" to save events, where "HH" is hour(s) in range of 0 ~ 23, "MM/SS" are minutes(s)/second(s) in range of 0 ~ 59. This filed is only available when "Auto Save Mode" is enabled. This time value can not be less than 300 seconds.
Max Size	Indicate the maximum size of events. This field is read-only.

2.5.10 CLI Options



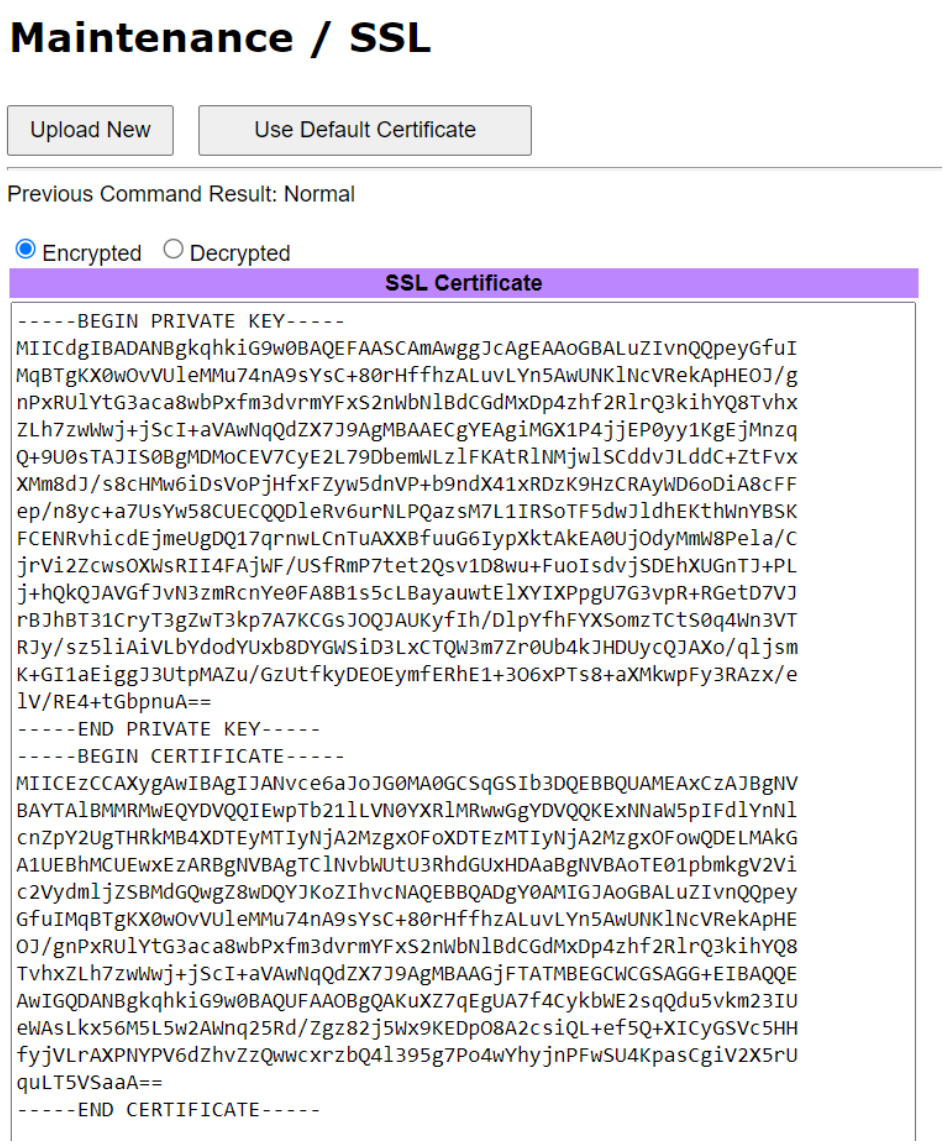
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to apply change.
Field	Description
Idle Timeout	Specify the timeout seconds for the operational interface. The session will be closed once the idle time exceeds this timeout value. Value range is 60 ~ 65535. 0 means disable timeout.
Max session count	Specify the maximum allowed sessions for the operational interface (1 ~ 10). The TELNET and SSH would share the session number together. Default is 4 sessions.
TELNET	To enable/disable TELNET of system. Default TELNET is disabled.
SSH	To enable/disable SSH of system. Default SSH is enabled.

2.5.11 HTTP (HTTPS)



Operation	Modify: 1. Select HTTP or HTTPS. 2. Change the port number if necessary. 3. Click “Modify” button to apply the change.
Field	Description
HTTPS Service	HTTPS / HTTP. Default is HTTP (HTTPS disabled).
HTTPS Port	HTTPS service port. Range: 1~65535, Default Port: 443.
HTTP Port	HTTP service port. Range: 1~65535, Default Port: 80.

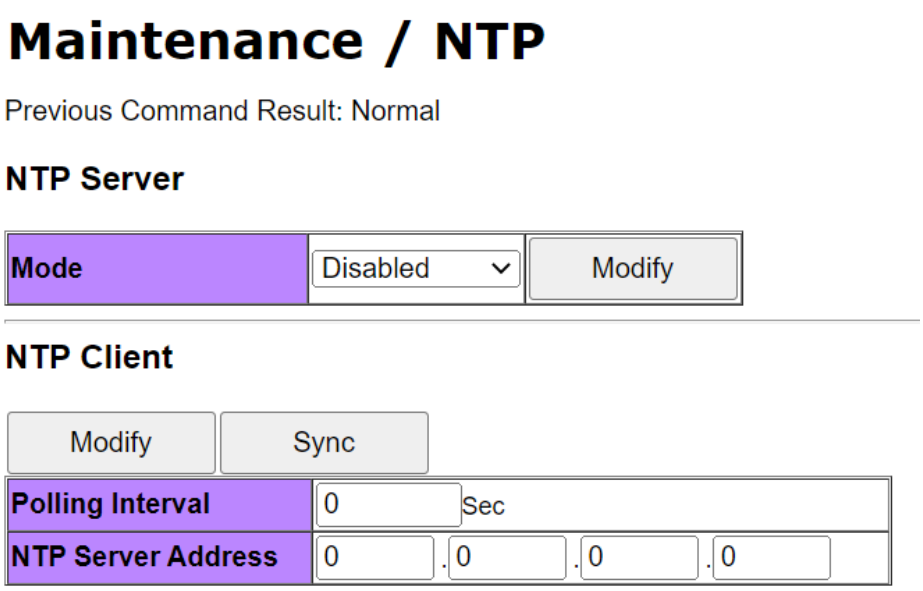
2.5.12 SSL



Operation	Use Default Certificate: 1. Click "Use Default Certificate" button. 2. System will delete uploaded certificate, if it exists. 3. After delete success, it will show default SSL certificate. Upload New: 1. Click "Upload New" button. 2. Copy and Paste both Private Key (privatekey) and Self-Signed SSL Certificate (cert) in the input area. 3. The certificate must be in PEM format as the following, otherwise upload would be failed:

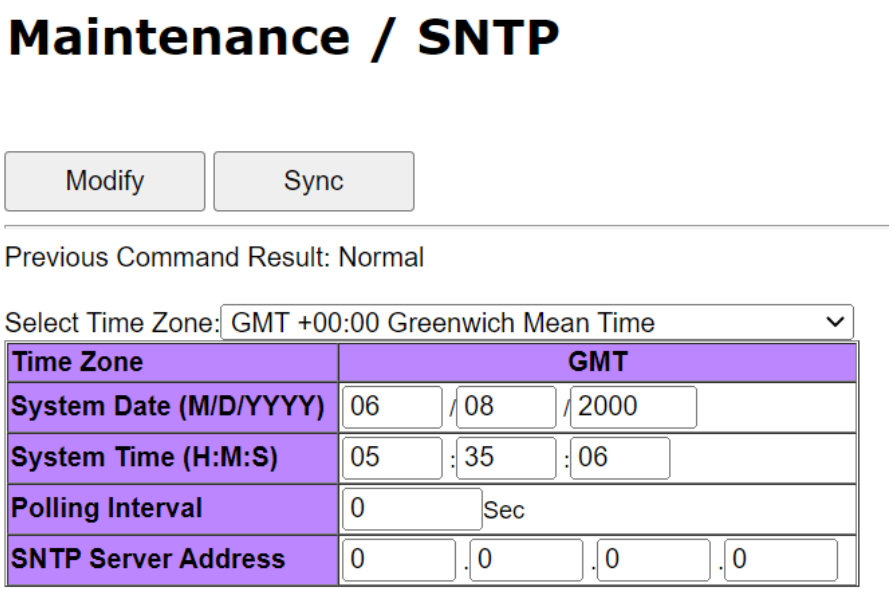
	-----BEGIN RSA PRIVATE KEY----- **....** **-----END RSA PRIVATE KEY-----** **-----BEGIN CERTIFICATE-----** **....** **-----END CERTIFICATE-----**

2.5.13 NTP



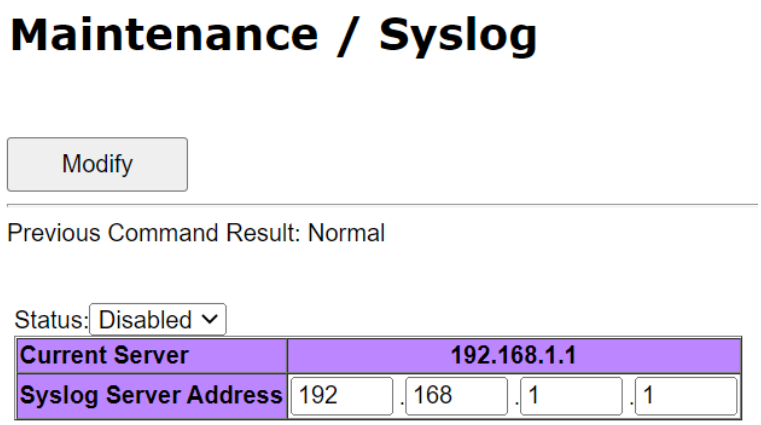
Operation	<u>To set the NTP Server:</u> 1. Enter or select the following fields 2. Click Modify button to modify data <u>To set the NTP Client:</u> 1. Enter or select the following fields 2. Click Modify button to modify data 3. Click Sync button to Manual synchronization
Field	Description
Mode	Enable/Disable NTP Server. Value range is Disabled/Enabled, default value is Disabled.
Polling Interval	Sets polling interval (seconds) that NTP client will sync with designated NTP server.
NTP Server address	Sets NTP server IP address for your system.

2.5.14 SNTP



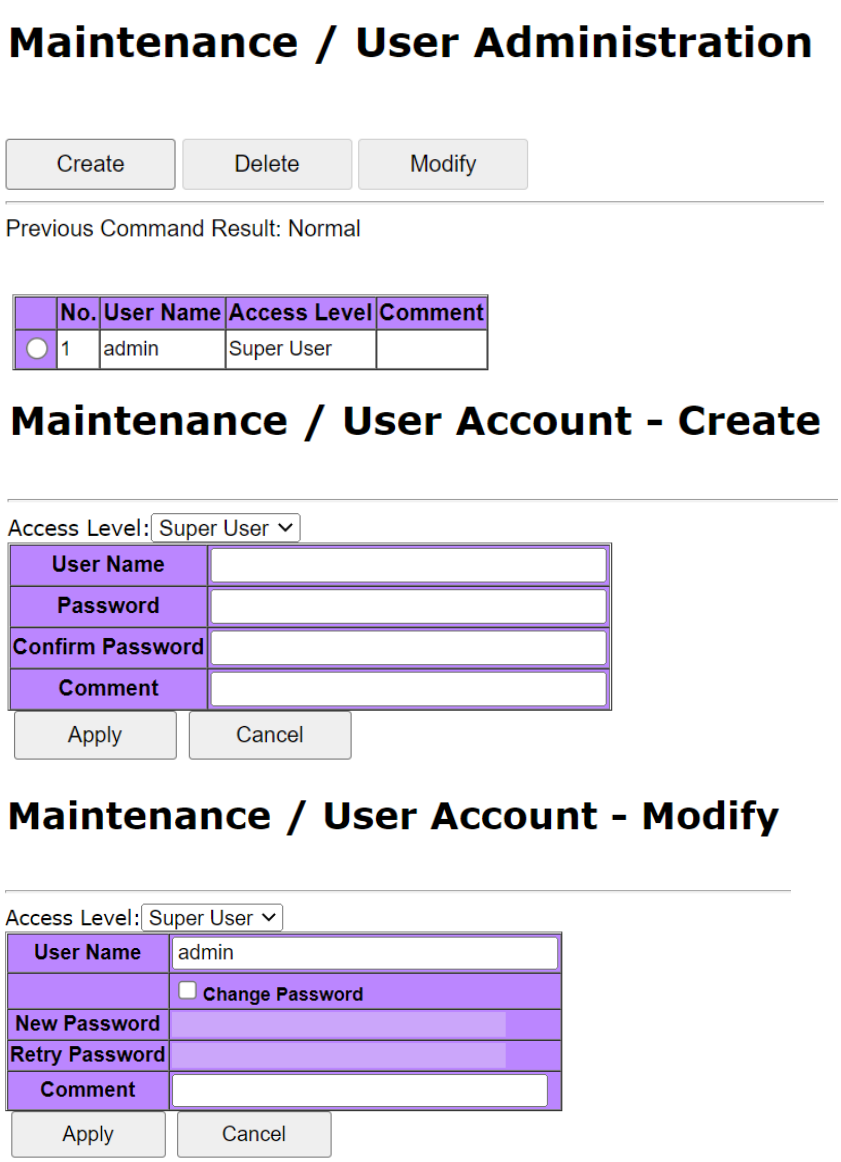
Operation	Modify: 1. Modify the configuration. 2. Click “Modify” button to modify data. Sync: Click “Sync” button to manual synchronize system time from SNTP server.
Field	Description
Select Time zone	Sets the local time zone with Time Zone list. Sixty-six of the world's time zones are presented (including those using standard time and summer/daylight savings time).
System Date	Sets system date (mm/dd/yyyy).
System Time	Sets system time (hh:mm:ss).
Polling Interval	Sets polling interval (seconds) that SNTP client will sync with designated SNTP server.
SNTP Server address	Sets SNTP server IP address for your system.

2.5.15 Syslog



Operation	Modify: 1. Select Enabled/Disabled option for Syslog function. 2. Modify the configuration. 3. Click “Modify” button to modify data.
Field	Description
Status	Value is Enabled/Disabled, default is Disabled. It will control the system log work or not.
Current Server IP	Current Syslog server IP address.
Syslog Server Address	New Syslog server IP address. The server must be a remote host.

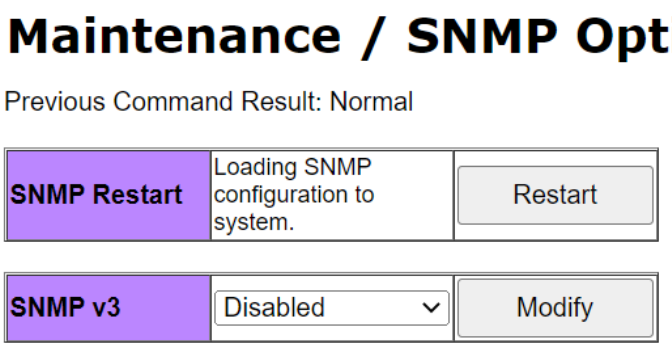
2.5.16 User Administration



Operation	Create: 1. Click “Create” button to create new user. 2. Fill user name, access level, password, confirm password and comment fields. 3. Click “Apply” to create setting data or click “Cancel” to cancel it. Delete: 1. Select one row data for delete.

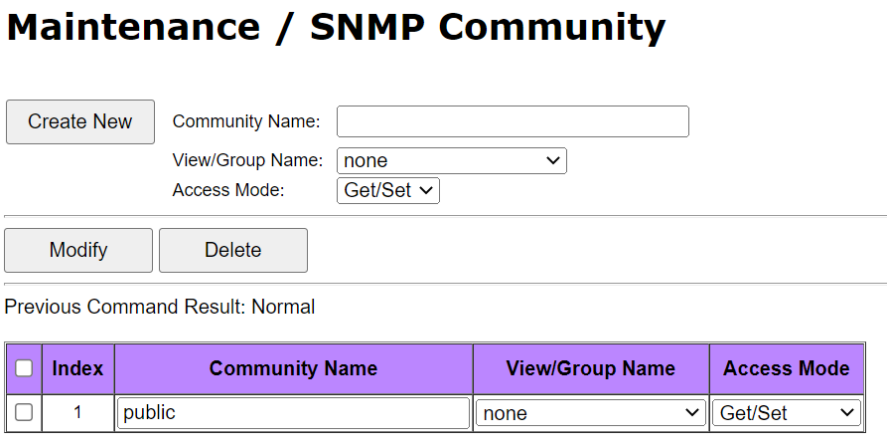
	2. Click “Delete” to delete selected data. Modify: 1. Click “Modify” button to modify user account. 2. Select “Change Password” checkbox if you want to change password. 3. Fill user name, access level, New Password, Retry Password and comment fields. 4. Click “Apply” to apply change or click “Cancel” to cancel it.
Field	Description
User Name	Shows the user name (up to 31 characters).
Access Level	Show the access level of the user: Super User - The user can access to all functions. Engineer - The user can access to all functions except user account management. Guest - The user can access to basic display functions.
Password	Enter a login password of 1-31 characters.
Confirm Password	Enter the login password of previous field again.
Comment	Description of the user account (up to 31 characters).

2.5.17 SNMP - Options



Operation	Restart: After any SNMP setting changed, only configuration is changed, but not apply to the system yet. All SNMP changed configuration could work after restart SNMP. It will not reboot system, but may take several seconds to load SNMP setting. Modify SNMP Version: This button is used to set whether SNMP v3 is enabled or not. If SNMP V3 switch is set to disable, the system would use SNMP v2c only. If SNMP V3 switch is set to enable, the system would use SNMP v3 setting. Changing this will restart SNMP automatically. The SNMP v3 parameters would be valid only if SNMP v3 is enabled.

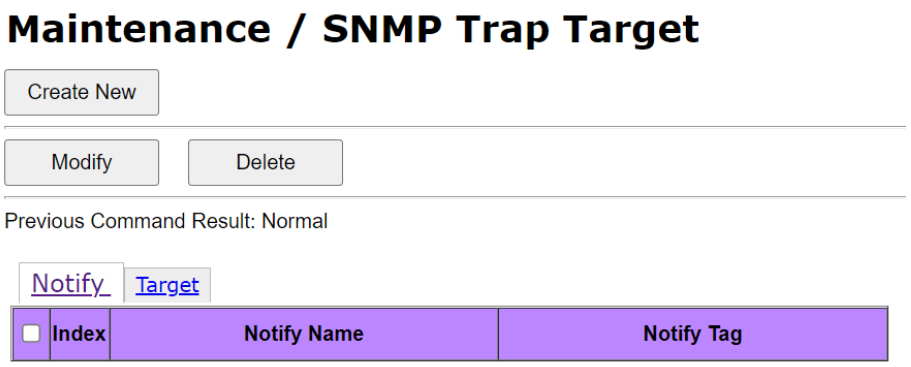
2.5.18 SNMP - Community



Operation	Create: 1. Fill the Community name. 2. Click "Create New" button to create new Community. Modify community entry: 1. Select entry by check up the check box 2. Modify field data: 3. Click "Modify" button to apply the change Delete community entry: Select entry by check box, then click "Delete". Note: This page supports multi-selection, click one or more row items to delete. User also could click "select all" to delete all target items.
Field	Description
Index	SNMP Community index, the system supports up to 32 Community data.
Community Name	SNMP Community name, for SNMP v1/v2c. Only if community name match, the SNMP request would be received. Community Name max size is 31 characters.
View/Group Name	View and Group are used for SNMP v3 only. A community is allowed to bind one of the view or group name. If it does not take any group or view, it will be a v1/v2c community. If it takes a view or a group name, the community will be treated as a v3 community. The v2c and v3 communities could exit in the community table concurrently. It will display "unknown(name)" when view/group name doesn't exist in view/group table.
Access Mode	Choice access right. Allow Get operation only, or allow both Get and Set.

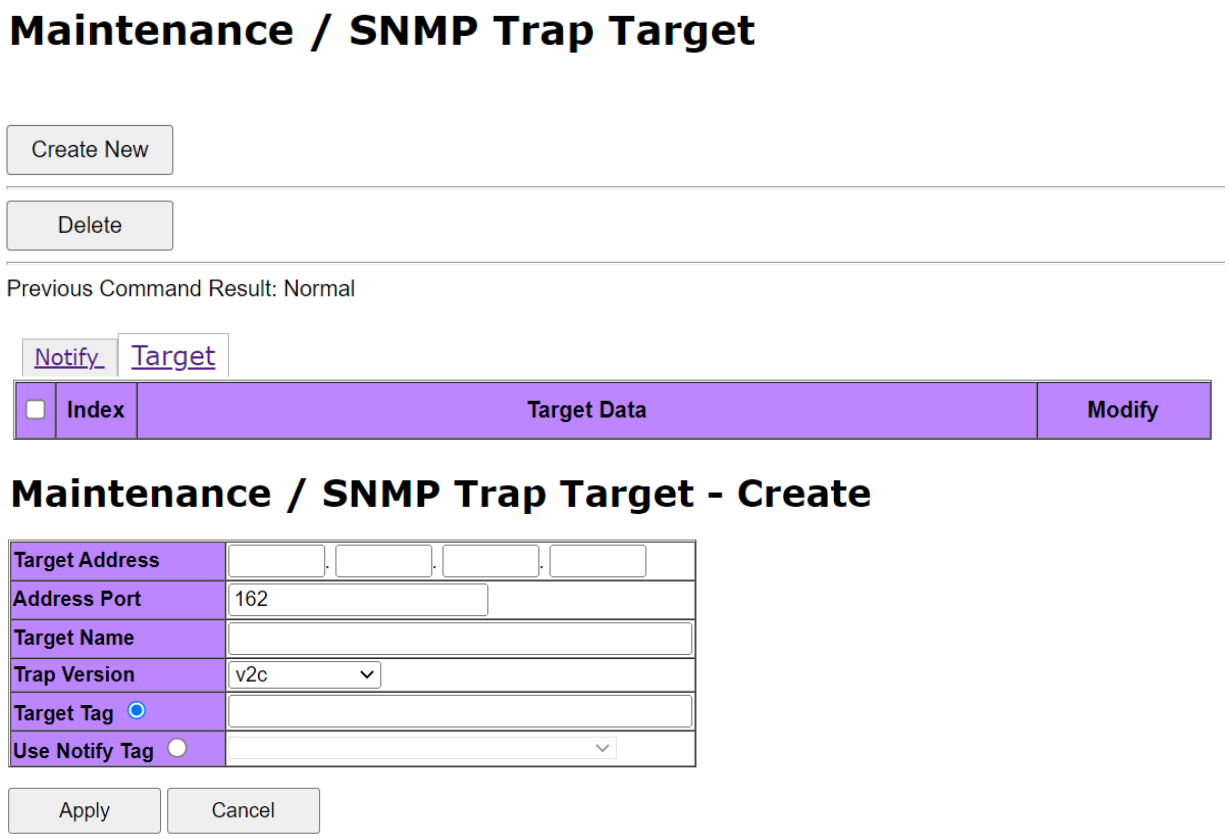
2.5.19 SNMP - Trap Target

SNMP Notify:



Operation	Create: 1. Click "Create New" button to create new notify tag. 2. Fill the notify name and notify tag. 3. Click "Apply" to create, "Cancel" to abort. Modify: 1. Select entry by check box 2. Modify field data 3. Click "Modify" button to apply change. Delete: 1. Select entry by check box 2. Click "Delete" button to delete Notify Tag item.
Field	Description
Index	SNMP notify tag index, The system supports up to 32 notify tags.
Notify Name	Name of Notify entry. Notify Name max size is 31 characters.
Notify Tag	Notify Tag string. If tag of Target entry matches any tag from tags of Notify Table, then SNMP trap function would work. Notify Tag max size is 31 characters.

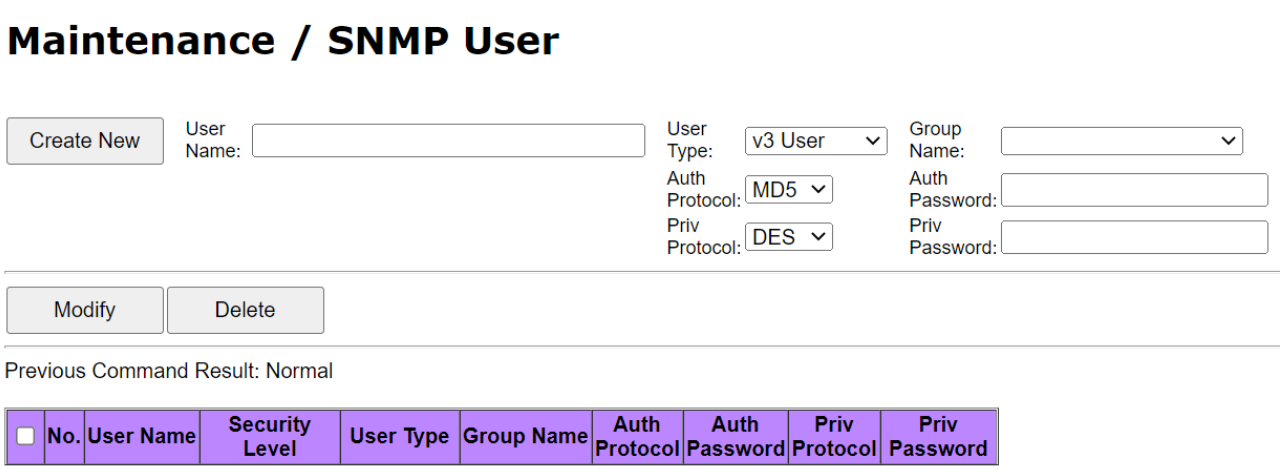
SNMP Target:



Operation	Create: 1. Click "Create New" button to create new target data 2. Fill the target IP address, name, port number, and trap version. Give a new tag name or select an existing notify tag name as target name 3. Click "Apply" to create, "Cancel" to abort. Modify: Click row item "modify" button to modify existence target data. Delete: Select entry by check box, then click "Delete". Note: This page supports multi-selection, click one or more row items to delete. User also could click "select all" to delete all target items.
Field	Description
Index	SNMP target index, the system supports up to 32 target entries.
Target Address	Target IP address, the host IP address of trap receiver. Value range 0.0.0.0 ~ 255.255.255.255

Address Port	Target Address port number. TCP Port number of Trap receiver. Range: 0 ~ 65535, Default is 162
Target Name	Name of target. Target Name max size is 31 characters.
Trap Version	Select SNMP trap version. Supports v1/v2c
Target Tag	Add a target tag, or pick up existing notify tag from Notify Table.

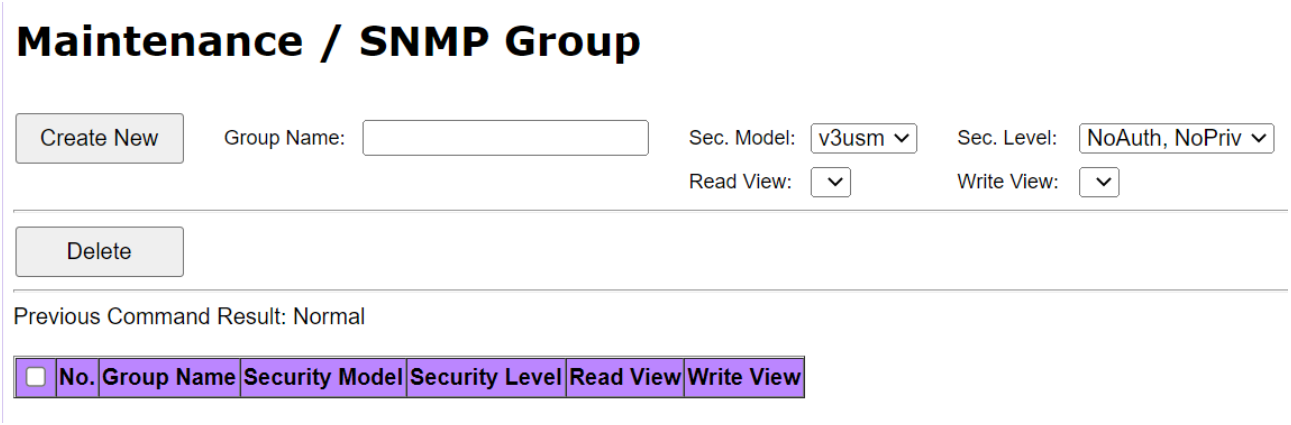
2.5.20 SNMP - User



Operation	Create new: 1. Fill "User Name" and select "User Type", "Auth Protocol" and "Priv Protocol". 2. Click "Create New" button to create new user. Delete: 1. Select a row data in user account table (also support multi-select). 2. Click "Delete" button to delete user account.
Field	Description
User Name	User name, length 1~31. Accept any characters except space, quote mark and "?".

User Type	SNMPv3 user type. Options: 1. Read Only 2. Read Write 3. v3 User If "User type" is "v3 User", the "Group Name" should be provided. No matter which User Type is selected, the authentication and Privacy options are allowed.
Group Name	Access Group name, length 1~15. Accept any characters except space, quote mark and "?". If user type is "Read Only" or "Read Write", then this field is not needed.
Auth Protocol	User authentication protocol. Works only if SNMPv3 is enabled. Options: 1. None 2. MD5 3. SHA If "Auth Protocol" is "None", "Priv Protocol" always is "None". If "Auth Protocol" is MD5 or SHA, "Auth Password" should be input.
Auth Password	Authentication password, length 8~15. Works only if SNMPv3 is enabled. Accept any characters except space, quote mark and "?". If Authentication Protocol is "None", then Privacy options are not needed.
Priv Protocol	User Privacy protocol. Works only if SNMPv3 is enabled. If "Priv Protocol" is not "None", "Priv Password" should be input. Options: 1. None 2. DES
Priv Password	Privacy password, length 8~15. Works only if SNMPv3 is enabled. Accept any characters except space, quote mark and "?". If "Priv Protocol" is "None" the field not needed.

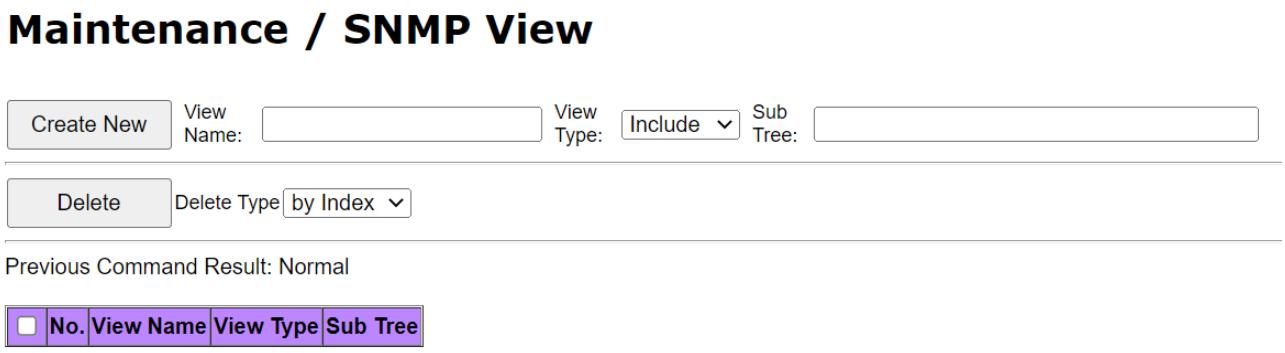
2.5.21 SNMP - Group



Operation	<u>To create new SNMP v3 user:</u> 1. Fill "User Name" and select "User Type", "Auth Protocol" and "Priv Protocol". 2. Click "Create New" button to create new user. <u>To modify SNMP user:</u> 1. Select row(s) in user account table (support multi-select), and modify data as expected. 2. Click "Modify" button to modify user account. <u>To delete SNMP user:</u> 1. Select row(s) in user account table (support multi-select). 2. Click "Delete" button to delete user account.
Field	Description
Group Name	Group name, length 1~15. Accept any characters except space, quote mark and "?".
Security Model	SNMP security model. Options: - v1 supports read/write view. - v2c supports read/write view. - v3usm supports read/write view & security level.

Security Level	User security level. If "Security Model" is "v1" or "v2c", the field is not used, it will be show as "--". States as below: - NoAuth, NoPriv (No authentication and no Privacy) - Auth, NoPriv (Authentication and no Privacy) - Auth, Priv (Authentication and Privacy)
Read View	Access View for Read (snmp-get) Select from the view list. If list is empty, create access view with page "SNMP View" first. It will display "unknown(xxxx)" when the name of xxxx doesn't exist in view name.
Write View	Access View for Write (snmp-set) Select from the view list. If list is empty, create access view with page "SNMP View" first. It will display "unknown(xxxx)" when the name of xxxx doesn't exist in view name.

2.5.22 SNMP - View



Operation	Create new: 1. Fill "View Name", "Sub Tree" and select "View Type". 2. Click "Create New" button to create new view. Note: max group entry: 32 Delete: 1. Select a row data in VACM view table (also support multi-select). 2. Click "Delete" button to delete user account. VACM View can be delete by Name or by Index. Note that if delete by name, all entries with the same name would be deleted together.
Field	Description
View Name	View name, length 1~15. Accept any characters except space, quote mark and "?".
View Type	Accessible/Not accessible of object (SNMP OID). Select down list box: 1. Include, allow access the subtree/oid; 2. Exclude, doesn't allow access the subtree/oid. Note: the oid is a prefix, no need to match it exactly. For example: 1.3.6.1.2.1 (include), it means 1.3.6.1.2.1.* are accessible. For example: 1.3.6.1.2.1 (exclude), it means 1.3.6.1.2.1.* are NOT accessible. An example of wildcard(*): 1.3.6.1.*.1 (include), it means that 1.3.6.1.4.1.* are accessible and 1.3.6.1.2.1.* are accessible.

Sub Tree	SNMP OID or Object Name of MIB Input format is OID, char length 1~31. Accept MIB object name "iswitch" OID or wildcard (*). iswitch represents 1.3.6.1.4.1.XXXX.XXXX (this is just an example, please reference to actual OID designed for product.) For example: 1.3.6.1.2.1 1.3.6.1.4.1.XXXX.XXXX iswitch.1 iswitch.2.6.1.1.*.4

2.6 Diagnostics

2.6.1 VeriPHY

Diagnostics /VeriPHY

Start

Previous Command Result: Normal

	Port	Pair A		Pair B		Pair C		Pair D	
		Result	Length to Fault	Result	Length to Fault	Result	Length to Fault	Result	Length to Fault
☐	G1	--	0	--	0	--	0	--	0
☐	G2	--	0	--	0	--	0	--	0
☐	G3	--	0	--	0	--	0	--	0
☐	G4	--	0	--	0	--	0	--	0
☐	G5	--	0	--	0	--	0	--	0
☐	G6	--	0	--	0	--	0	--	0

Operation	Start: Push "Start" button to start cable diagnostics. Display "Success" when previous operation succeed. Display "Fail" when previous operation is failure.
Field	Description
Port	Specify the port identifier.
Pair X	Each copper port requires one 4-pair RJ-45 cables to establish link with link-partner. This displays the diagnostic result for per pair, include result and estimated distance to failure point. Support result, include : "Ok" - It means cable good for this pair. "Open" - Lack of continuity between the pins at each end of the twisted-pair cable. "SP Short" - Two or more conductors are short-circuited together on same pair. "CP Short" - Two or more conductors are short-circuited together on Crossed pair. "Busy" - The circuit is busy for this pair when diagnostics event occur. "Invalid" - Other fault but above ones. It estimates the distance that self to failure point for the failure pair. This length is calculated in unit of 0.1m. Its accuracy is about +/- 2-meter.