AVCOMM Media Converter
6003GX/6003GX-POE
User Manual

AVCOMM Technologies Inc.
333 West Loop North, Suite 460 Houston, TX 77024, USA | info@avcomm.us | www.avcomm.us

AVCOMM Technologies Inc.

6003GX/6003GX-POE

Industrial 3-port Full Gigabit Managed Media Converter

User Manual

About This Manual

This user manual is intended to guide a professional installer to install and to configure the Avcomm 6003GX/6003GX-POE. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this switch.

Disclaimer

Avcomm reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required, or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to Avcomm. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. Avcomm assumes no responsibility for its use by the third parties.

AVCOMM Online Technical Services

At Avcomm, you can use the online service forms to request the support. The submitted forms are stored in server for Avcomm team member to assign tasks and monitor the status of your service. Please feel free to write to www.avcomm.us if you encounter any problems.

CONTENTS

1. Introductions

1.1 Using the Web Interface

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

1.1.1 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

1.1.2 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:

- **Configuration**
- **Monitor**
- **Diagnostics**
- **Maintenance**

1.1.3 Title Bar Icons

Home Button 

Click Home Button, and the web page will return to Port State Overview page.

Help Button 

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

Logout Button 

Click Logout Button, the system will be logged out successfully.

1.1.4 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.

1.2 Using the Online Help

Each screen has a Help button  that invokes a page of information relevant to the 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

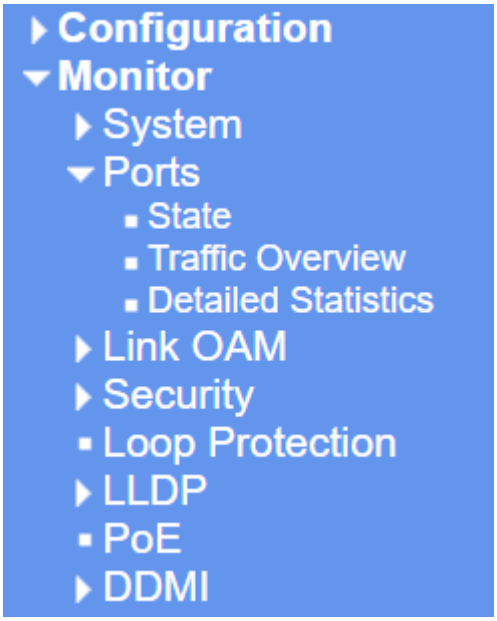
Operation	1. Fill Username and Password 2. Click “OK”
Field	Description
Username	Login user name. The allowed string length is 1 to 31. Default: adpro
Password	Login user password. The allowed string length is 0 to 31. Default: none

2.2 Tree View

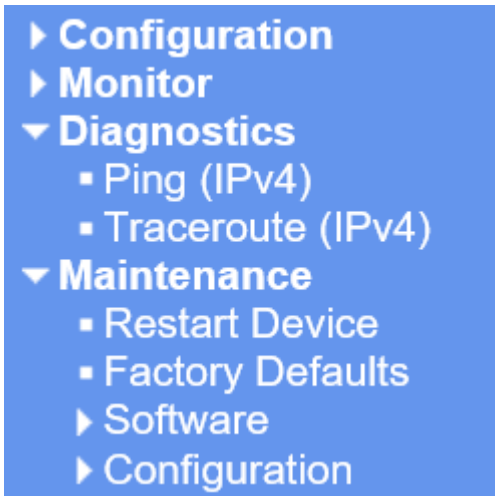
The tree view is a menu of the web. It offers user quickly to get the page for expected data or configuration.

2.2.1 Configuration Menu

2.2.2 Monitor Menu



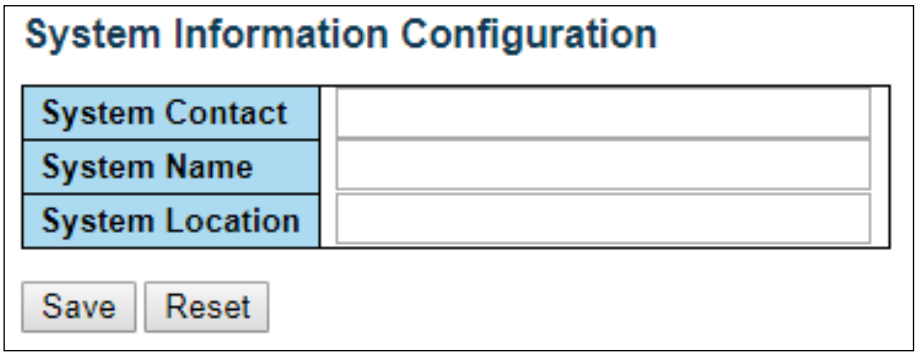
2.2.3 Diagnostics & Maintenance Menu



2.3 Configuration

2.3.1 System Information

The system information is provided here.



Object	Description
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified name. The name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 63.
System Location	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.2 System IP

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

IP Configuration

IP Interfaces

DHCPv4								IPv4	
Enable	Client ID				Hostname	Fallback	Current Lease	Address	Mask Length
	Type	IfMac	ASCII	HEX					
☐	Auto	Port USER				0		10.83.55.124	8

IP Routes

Delete	Network	Mask Length	Gateway
Delete			

Add Route

Save Reset

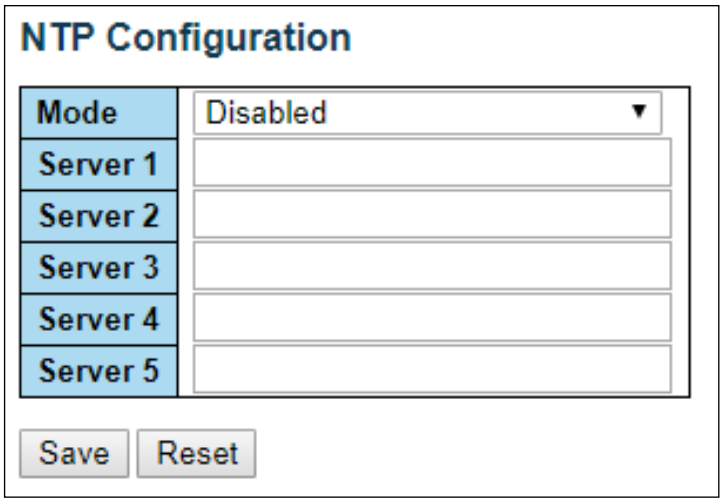
Object	Description
IP Interfaces	
IPv4 DHCP Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.
IPv4 DHCP Client Identifier Type	The Type of Client Identifier is selectable, option: Auto, IF_MAC, ASCII, HEX. Default is Auto, when type is Auto and hostname is configured (not empty), then the hostname will be used in the DHCP option 61 field. But if hostname is empty, then system MAC address will be used, in format xx-xx-xx-xx-xx-xx. Note: in either one of above 2 cases, there is an extra byte 00 appended in front of the option 61 field. For example: xx-xx-xx-xx-xx-xx, option 61 value length would be 18. 0x00 stands for Not HW Address.
IPv4 DHCP Client Identifier IfMac	The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field. For example: Port 2 is selected, option 61 value would be system's MAC plus 2. Note: In this case, there is an extra byte 01 appended in front of the option 61 field, like 01aabbcc010203, length 7. The 0x01 stands for Hardware type Ethernet.
IPv4 DHCP Client Identifier ASCII	The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field. Note: In this case, there is an extra byte 00 appended in front of the option 61 field. 0x00 stands for Not HW Address. And always uses lower-case character.
IPv4 DHCP Client Identifier HEX	The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field. Note: In this case, the option 61 value would be exact the same as HEX without any extra byte.

IPv4 DHCP Hostname	The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the option 12 field uses system mac.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If **DHCP** is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv4 Mask	The IPv4 network mask, in number of bits (*prefix length*). Valid values are between 0 and 30 bits for an IPv4 address. If **DHCP** is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IP Routes	
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation. A default route can use the value **0.0.0.0**.
Mask Length	The destination IP network or host mask, in number of bits (*prefix length*). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits. Only a default route will have a mask length of **0** (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation.

Buttons	
Add Interface	Click to add a new IP interface. A maximum of 8 interfaces is supported.
Add Route	Click to add a new IP route. A maximum of 32 routes is supported.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.3 System NTP

Configure NTP on this page.



Object	Description
Mode	Indicates the NTP mode operation. Possible modes are: **Enabled**: Enable NTP client mode operation. **Disabled**: Disable NTP client mode operation.
Server #	Provide the IPv4 address of a NTP server.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.4 System Time

This page allows you to configure the Time Zone

Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC+09:00) Osaka, Sapporo, Tokyo ▼
Hours	9 ▼
Minutes	0 ▼
Acronym	JST (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled ▼

Start Time settings	
Month	Jan ▼
Date	1 ▼
Year	2014 ▼
Hours	0 ▼
Minutes	0 ▼
End Time settings	
Month	Jan ▼
Date	1 ▼
Year	2097 ▼
Hours	0 ▼
Minutes	0 ▼
Offset settings	
Offset	1 (1 - 1439) Minutes

Date/Time Configuration

Date/Time settings	
Year	2019 (2000 - 2037)
Month	Oct ▼
Date	21 ▼
Hours	12 ▼
Minutes	41 ▼
Seconds	35 ▼

Save Reset

Object	Description
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' options is used for the specific time zone which is excluded from the options list.
Hours	Number of hours offset from UTC. The field only available when time zone manual setting.

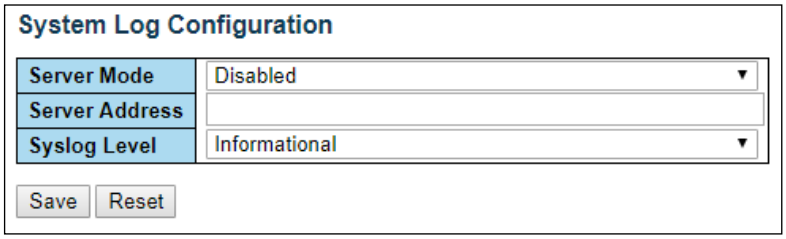
Minutes	Number of minutes offset from UTC. The field only available when time zone manual setting.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters) Notice the string '' is a special syntax that is reserved for null input.
Daylight Saving Time Configuration	
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)
Recurring Configurations	
Start time settings	
Week	Select the starting week number.
Day	Select the starting day.
Month	Select the starting month.
Hours	Select the starting hour.
Minutes	Select the starting minute
End time settings	
Week	Select the ending week number.
Day	Select the ending day.
Month	Select the ending month.
Hours	Select the ending hour.
Minutes	Select the ending minute
Offset settings	
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)
Non Recurring Configurations	
Start time settings	
Month	Select the starting month.
Date	Select the starting date.
Year	Select the starting year.
Hours	Select the starting hour.
Minutes	Select the starting minute
End time settings	
Month	Select the ending month.
Date	Select the ending date.
Year	Select the ending year.
Hours	Select the ending hour.
Minutes	Select the ending minute

Offset settings	
Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)
Date/Time Configuration	
Date/Time Settings	
Year	Year of current datetime. (Range: 2000 to 2037)
Month	Month of current datetime.
Date	Date of current datetime.
Hours	Hour of current datetime.
Minutes	Minute of current datetime.
Seconds	Second of current datetime.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.5 System Log

Configure System Log on this page.



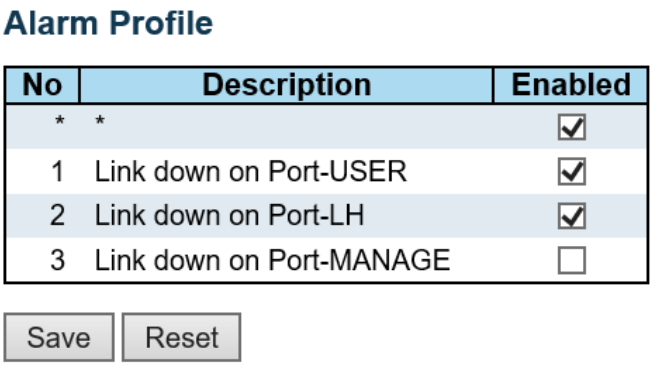
Object	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: `Enabled`: Enable server mode operation. `Disabled`: Disable server mode operation.
Server Address	Indicates the IPv4 host address of syslog server.
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are:

	Error: Send the specific messages which severity code is less or equal than Error(3). **Warning**: Send the specific messages which severity code is less or equal than Warning(4). **Notice**: Send the specific messages which severity code is less or equal than Notice(5). **Informational**: Send the specific messages which severity code is less or equal than Informational(6).

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.6 System Alarm Profile

Alarm Profile is provided here to enable/disable alarm



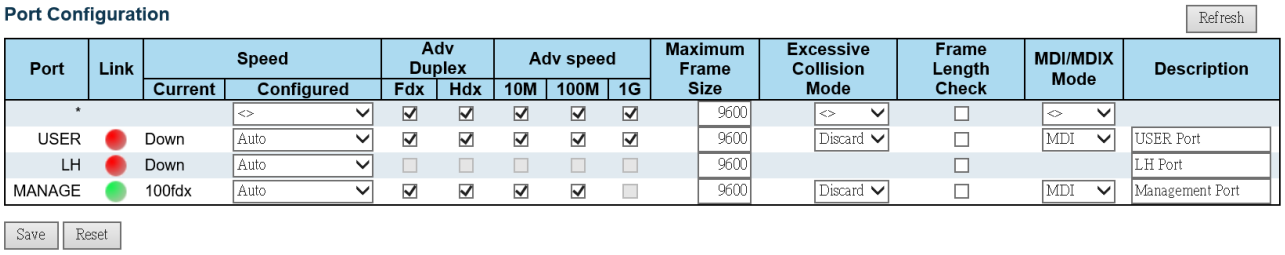
Object	Description
No	Index of the Alarm Profile entry.
Description	Alarm Type Description.
Enabled	If alarm entry is Enabled, then alarm will be shown in alarm history/current when it occurs. Alarm LED (ALM LED) will be turned on with Red. SNMP trap will be sent if any SNMP trap entry exists and enabled.
Disabled	If alarm entry is Disabled, then alarm will not be generated or shown in alarm history/current when alarm occurs; then it will not trigger the Alarm LED change,

	SNMP trap either.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.7 Ports

This page displays current port configurations. Ports can also be configured here.



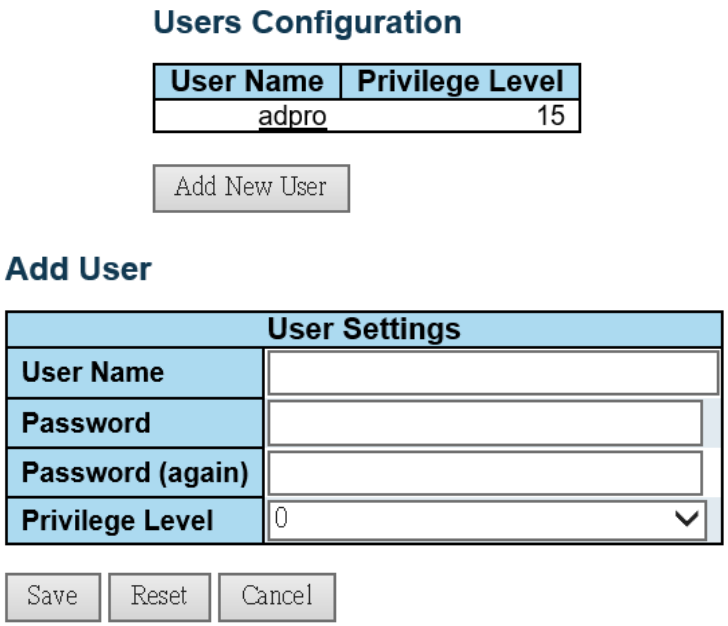
Object	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Selects any available link speed for the given system port. Only speeds supported by the specific port is shown. Possible speeds are: **Disabled** - Disables the system port operation. **Auto** - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **10Mbps HDX** - Forces the cu port in 10Mbps half duplex mode. **10Mbps FDX** - Forces the cu port in 10Mbps full duplex mode. **100Mbps HDX** - Forces the cu port in 100Mbps half duplex mode. **100Mbps FDX** - Forces the cu port in 100Mbps full duplex mode. **1Gbps FDX** - Forces the port in 1Gbps full duplex .
Unidirectional mode method	The 6003GX(POE) sends link-oam frames and use unidirectional mode method even if the LH port is link down. It is divided into two cases, one case is default and the other case is use unidirectional mode method as the following.

	Case 1 - When LH Port set auto negotiation at default, the unidirectional mode should be disable. Case 2 - When LH port change speed and set Fixed 1Gbps FDX, the unidirectional mode should be enable. (Note: Not set Fix 100Mbps FDX is limitation, and only set Fix 1Gbps FDX)
Advertise Duplex	When duplex is set as auto i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default port will advertise all the supported duplexes if the Duplex is Auto.
Advertise Speed	When Speed is set as auto i.e auto negotiation, the port will only advertise the specified speeds (**10M** **100M** **1G**) to the link partner. By default port will advertise all the supported speeds if speed is set as Auto.
Maximum Frame Size	Enter the maximum frame size allowed for the system port, including FCS. The range is 1518-9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. **Discard**: Discard frame after 16 collisions (default). **Restart**: Restart backoff algorithm after 16 collisions.
Frame Length Check	Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch
MDI/MDI-X Mode	Specify fix MDI or MDI-X mode for copper port. MDI: Fix MDI mode. MDI-X: Fix MDI-X mode.
Description	Port Description, max length 255 characters.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

2.3.8 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



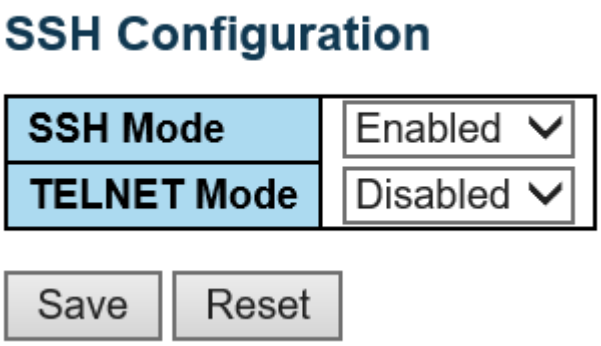
Object	Description
User Configuration	
User Name	The name identifying the user. This is also a link to Add/Edit User.
Privilege Level	The privilege level of the user. The allowed range is `0` to `15`. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the system. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.
Add User	
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.
Password	The password of the user. The allowed string length is 0 to 31. Any printable characters including space is accepted.
Password (again)	Type the password again for confirmation.
Privilege Level	The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or

	greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons	
Add New User	Click to add a new user. The maximum number of users is **20**.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and return to the Users.
Delete User	Delete the current user. This button is not available for new configurations (Add new user)

2.3.9 SSH/TELNET

Configure SSH/TELNET on this page.



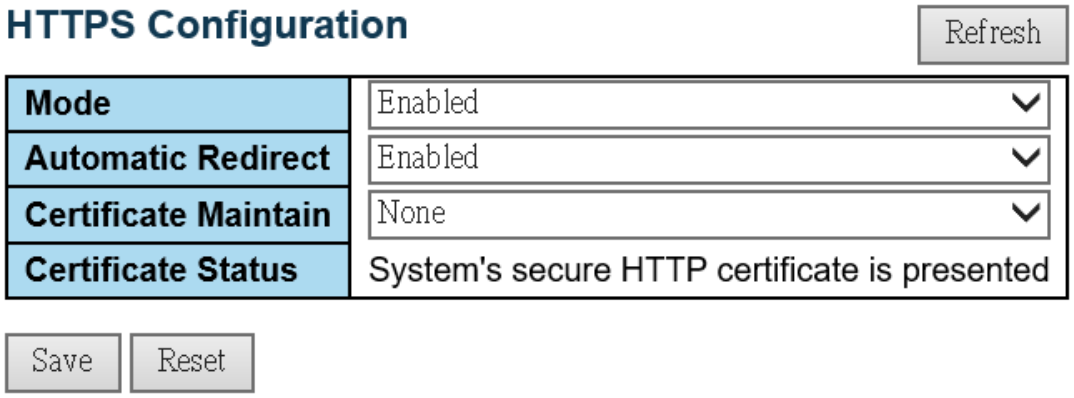
Object	Description
Mode	Indicates the SSH and TELNET mode operation. Possible modes are: Enabled: Enable SSH / TELNET mode operation. Disabled: Disable SSH / TELNET mode operation. (TELNET is Disabled by Default.)

Buttons

Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.10 HTTPS

This page allows you to configure the HTTPS settings and maintain the current certificate on the system.



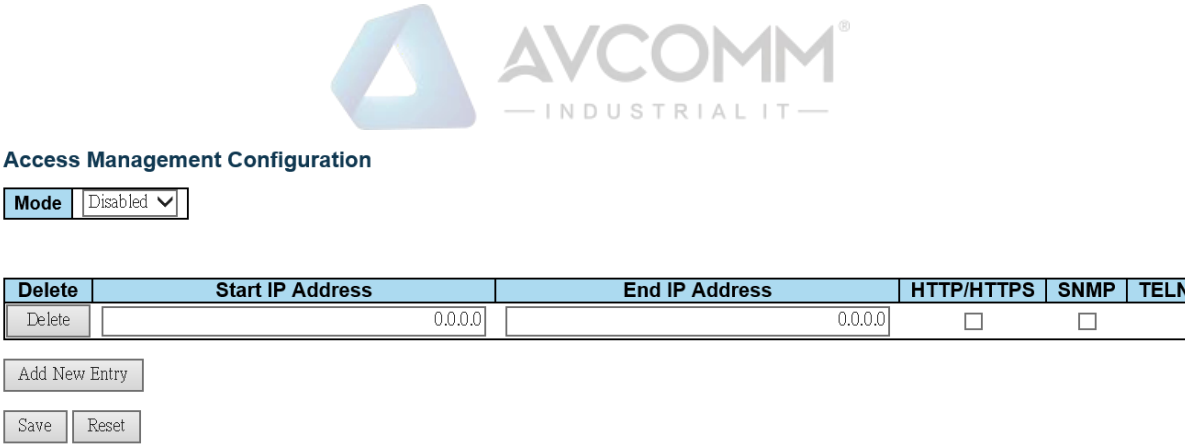
Object	Description
Mode	Indicate the HTTPS mode operation. Possible modes are: **`Enabled`**: Enable HTTPS mode operation. **`Disabled`**: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It is only significant when "HTTPS mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Notice that the browser may not allow the redirect operation due to the security consideration unless the system certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: **`Enabled`**: Enable HTTPS redirect mode operation. **`Disabled`**: Disable HTTPS redirect mode operation.
Certificate Maintain	The operation of certificate maintenance. Possible operations are: **`None`**: No operation. **`Delete`**: Delete the current certificate.

	Upload: Upload a certificate PEM file. Possible methods are: **Web Browser** or **URL**. **Generate**: Generate a new self-signed RSA certificate.
Certificate Pass Phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.
Certificate Upload	Upload a certificate PEM file into the system. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: **Web Browser**: Upload a certificate via Web browser. **URL**: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Z, a-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
Certificate Status	Display the current status of certificate on the system. Possible statuses are: **System's secure HTTP certificate is presented**. **System's secure HTTP certificate is not presented**. **System's secure HTTP certificate is generating ...**.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Refresh	Click to refresh the page. Any changes made locally will be undone.

2.3.11 Access Management

Configure access management table on this page. The maximum number of entries is **16**. If the application's type match any one of the access management entries, it will allow access to the system.

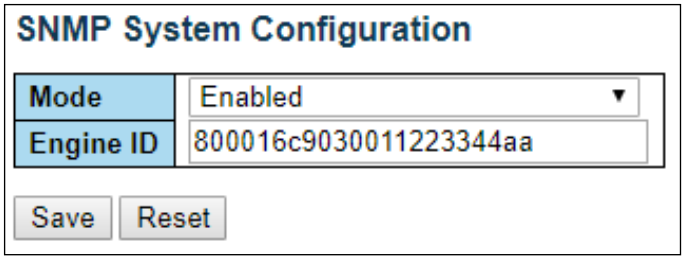


Object	Description
Mode	Indicates the access management mode operation. Possible modes are: `Enabled`: Enable access management mode operation. `Disabled`: Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next save.
Start IP address	Indicates the start IP address for the access management entry.
End IP address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the system from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the system from SNMP interface if the host IP address matches the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the system from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons	
Add New Entry	Click to add a new access management entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.12 SNMP System Configuration

Configure SNMP on this page.

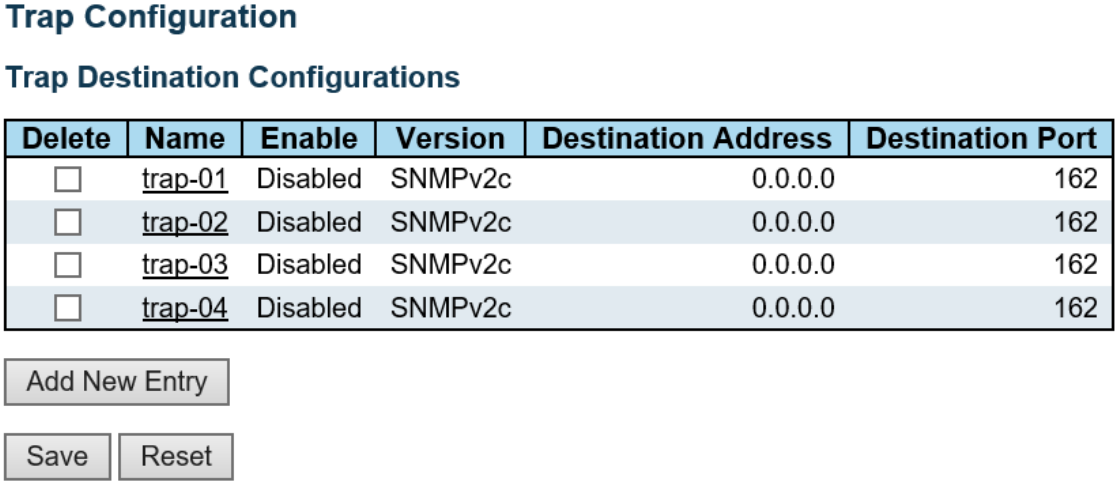


Object	Description
Mode	Indicates the SNMP mode operation. Possible modes are: `Enabled`: Enable SNMP mode operation. `Disabled`: Disable SNMP mode operation.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Only users on this Engine ID can access the system (local users), so changing the Engine ID will revoke access for all current local users.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

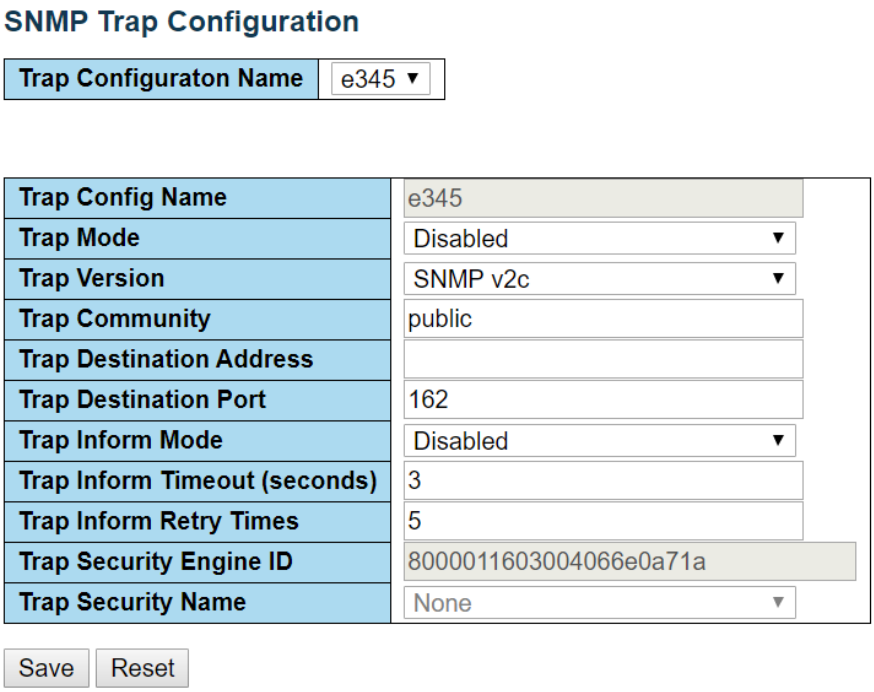
2.3.13 SNMP Trap Destination

Configure trap destinations on this page.



Object	Description
Trap Destination Configurations	
Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Enable	Indicates the trap destination mode operation. Possible modes are: `Enabled`: Enable SNMP trap mode operation. `Disabled`: Disable SNMP trap mode operation.
Version	Indicates the SNMP trap supported version. Possible versions are: `SNMPv1`: Set SNMP trap supported version 1. `SNMPv2c`: Set SNMP trap supported version 2c. `SNMPv3`: Set SNMP trap supported version 3.
Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').
Destination port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

The SNMP Trap Configuration page includes the following fields:



Object	Description
SNMP Trap Detailed Configuration	
Trap Config Name	Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Trap Mode	Indicates the SNMP trap mode operation. Possible modes are: `Enabled`: Enable SNMP mode operation. `Disabled`: Disable SNMP mode operation.
Trap Version	Indicates the SNMP trap supported version. Possible versions are: `SNMP v1`: Set SNMP trap supported version 1. `SNMP v2c`: Set SNMP trap supported version 2c. `SNMP v3`: Set SNMP trap supported version 3.
Trap Community	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.
Trap Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').
Trap Destination port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: `Enabled`: Enable SNMP trap inform mode operation. `Disabled`: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is `0` to `2147`.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is `0` to `255`.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons	
Add New Entry	Click to add a new user.
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

SNMP Trap Sources

This page provides SNMP trap source configurations. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches.

Trap Configuration

Trap Source Configurations

Delete	Name	Type	Subset OID
Delete	coldStart	included	

Add New Entry

Save Reset

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Name	Indicates the name for the entry.
Type	The filter type for the entry. Possible types are: `included`: An optional flag to indicate a trap is sent for the given trap source is matched. `excluded`: An optional flag to indicate a trap is not sent for the given trap source is matched.
Subset OID	The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIndex is the subset OID of linkUp and linkDown, 1000001 stands for port 1. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin withasterisk(*) and the maximum of OID count must not exceed 63.

Buttons	
Add New Entry	Click to add a new community entry. The maximum entry count is `32`.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.14 SNMP Communities

Configure SNMPv3 community table on this page. The entry index key is **`Community`**.

SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
☐	public	public	0.0.0.0	0
☐	private	private	0.0.0.0	0
Delete				

Add New Entry | Save | Reset

Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community Name	Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Community Secret	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source prefix.
Source Prefix	Indicates the SNMP access source address prefix.

Buttons	
Add New Entry	Click to add a new community entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Users

Configure SNMPv3 user table on this page. The entry index keys are **`Engine ID`** and **`User Name`**.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	80000116030040660a0b0c		Auth, Priv	MD5		DES	

Add New Entry | Save | Reset

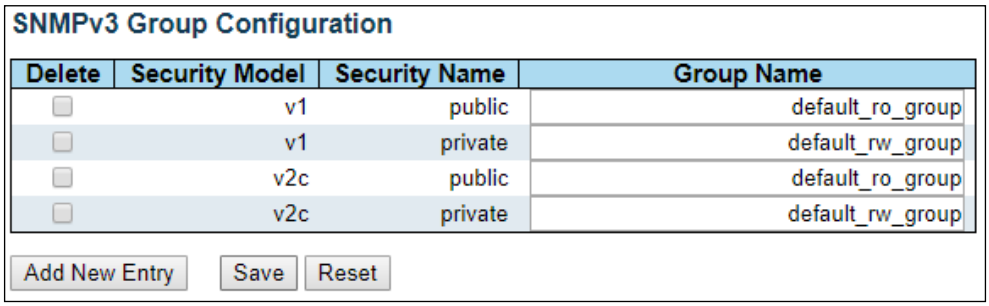
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: **`NoAuth, NoPriv`**: No authentication and no privacy. **`Auth, NoPriv`**: Authentication and no privacy. **`Auth, Priv`**: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: **`None`**: No authentication protocol. **`MD5`**: An optional flag to indicate that this user uses MD5 authentication protocol. **`SHA`**: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.
Authentication Password	A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: **`None`**: No privacy protocol. **`DES`**: An optional flag to indicate that this user uses DES authentication protocol. **`AES`**: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
Add New Entry	Click to add a new user entry.

Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

SNMP Groups

Configure SNMPv3 group table on this page. The entry index keys are **`Security Model`** and **`Security Name`**.

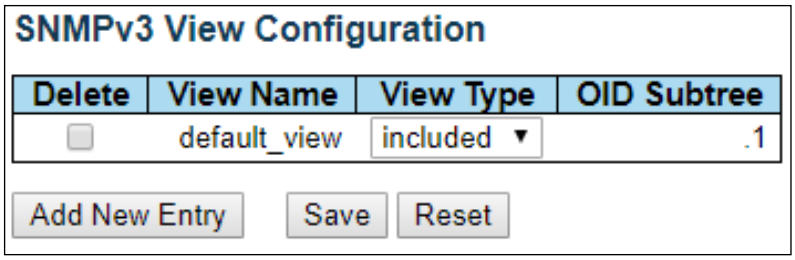


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: **`v1`**: Reserved for SNMPv1. **`v2c`**: Reserved for SNMPv2c. **`usm`**: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
Add New Entry	Click to add a new group entry
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

SNMPv3 Views

Configure SNMPv3 view table on this page. The entry index keys are **View Name** and **OID Subtree**.

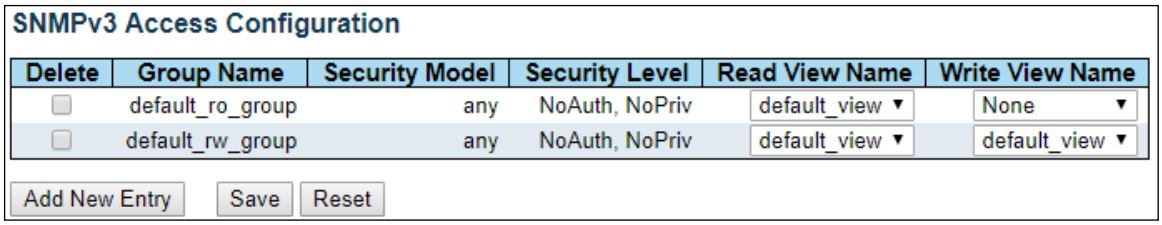


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 64. The allowed string content is digital number or asterisk(*).

Buttons	
Add New Entry	Click to add a new view entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.15 SNMP Access

Configure SNMPv3 access table on this page. The entry index keys are **Group Name**, **Security Model** and **Security Level**.

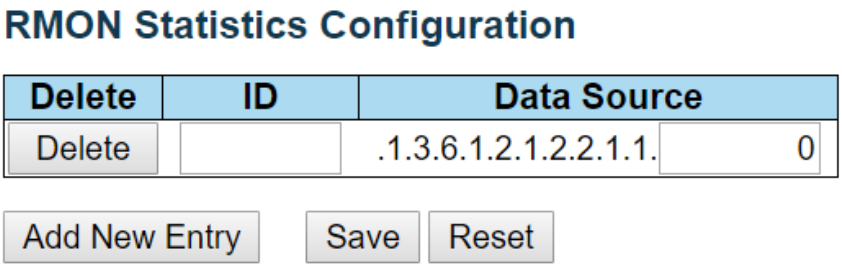


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: **any**: Any security model accepted(v1|v2c|usm). **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv**: No authentication and no privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons	
Add New Entry	Click to add a new access entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.16 RMON Statistics

Configure RMON Statistics table on this page. The entry index key is ID.

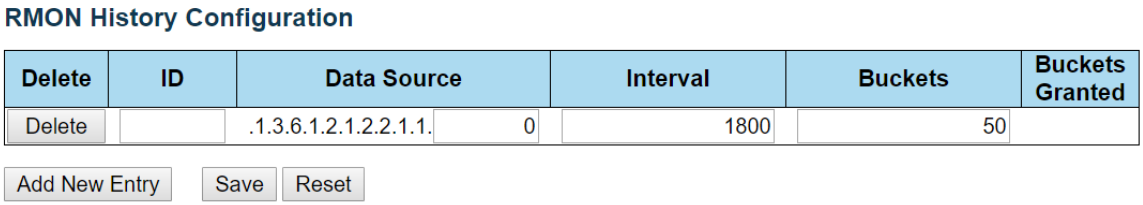


Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. For example 1000001~1000003.

Buttons	
Add New Entry :	Click to add a new RMON statistics entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.17 RMON History

Configure RMON History table on this page. The entry index key is ID.



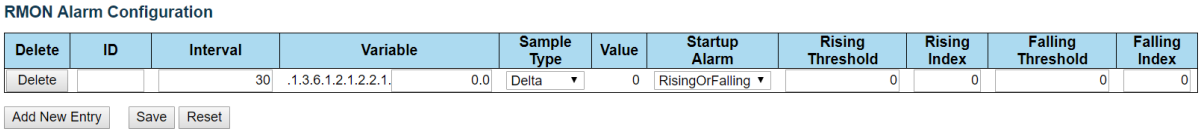
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID which wants to be monitored. For example 1000001~1000003.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 65535, default value is 50.
Buckets Granted	The number of data shall be saved in the RMON.

Buttons

Add New Entry :	Click to add a new RMON history entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.18 RMON Alarm

Configure RMON Alarm table on this page. The entry index key is ID.



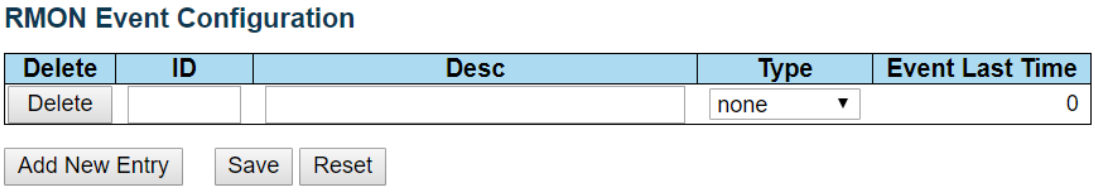
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: InOctets: The total number of octets received on the interface, including framing characters. InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol. InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded even the packets are normal. InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol. OutOctets: The number of octets transmitted out of the interface , including framing characters. OutUcastPkts: The number of uni-cast packets that request to transmit. OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit. OutDiscards: The number of outbound packets that are discarded event the packets is normal. OutErrors: The The number of outbound packets that could not be transmitted because of errors. OutQLen: The length of the output packet queue (in packets). The range of xxx is 10~21, and the range of yyy is 1000001~1000003.

	For example, 10.1000001 represents InOctets of USER port.
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: Absolute: Get the sample directly. Delta: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: Rising: Trigger alarm when the first value is larger than the rising threshold. Falling: Trigger alarm when the first value is less than the falling threshold. RisingOrFalling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

Buttons	
Add New Entry :	Click to add a new RMON alarm entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.19 RMON Event

Configure RMON Event table on this page. The entry index key is ID.



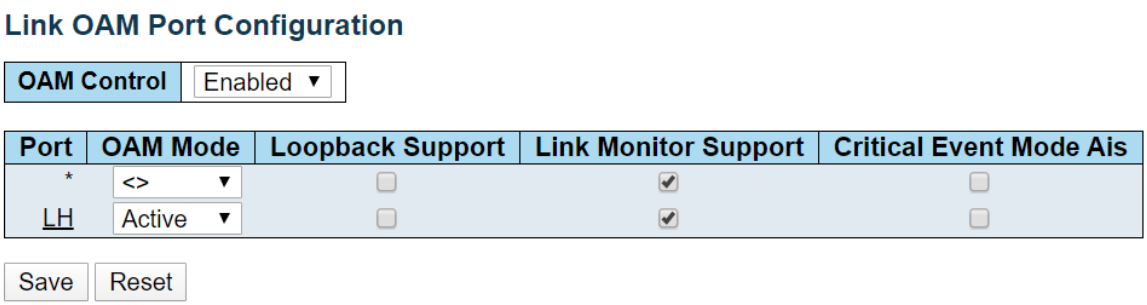
Object	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates this event, the string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event, the possible types are:

	none: No SNMP log is created, no SNMP trap is sent. log: Create SNMP log entry when the event is triggered. snmptrap: Send SNMP trap when the event is triggered. logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons	
Add New Entry :	Click to add a new RMON event entry.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.20 Link OAM Port Configuration

This page allows the user to inspect the current Link OAM port configurations, and change them as well.



Object	Description
OAM Control	Controls whether Link OAM is enabled or disabled in whole system. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions. OAM LED: LED light on with red when Remote OAM Alarm is received. Whenever DTE receives OAMPDU frame with any one flag including critical event / link fault/ dying gasp is set (true), then it is considered as Remote OAM Alarm. Note: LPT function works only if Link OAM function enabled.
Port	Link OAM is supported to LH Port only.
OAM Mode	Configures the OAM Mode as Active or Passive. The default mode is Passive. **Active mode** DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are

	permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer. **Passive mode** DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.
Loopback Support	Controls whether the loopback support is enabled for the port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.
Link Monitor Support	Controls whether the Link Monitor support is enabled for the port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.
Critical Event Mode Ais	[topology] (USER_PORT_A) [6003GX1] (LH) ------- (LH) [6003GX2] (USER_PORT_B) "6003GX2" outputs an efm-oam frame with critical event bit 0 when the user port is linkup "6003GX2" outputs an efm-oam frame with critical event bit 1 when the user port is linkdown. [Case 1] The "critical-event-mode ais" setting is diable in "6003GX1. The "show link-oam status" command shows the status in the critical event item for critical event bit and the "user-port status" item is always "-". [Case 2] The "critical-event-mode ais" setting is enable in "6003GX1. The "show link-oam status" command shows the status in the user-port status item for critical event bit and the "critical event" item is always "-".

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.21 Link OAM Event Configuration

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

Link Event Configuration for Port LH

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Save Reset

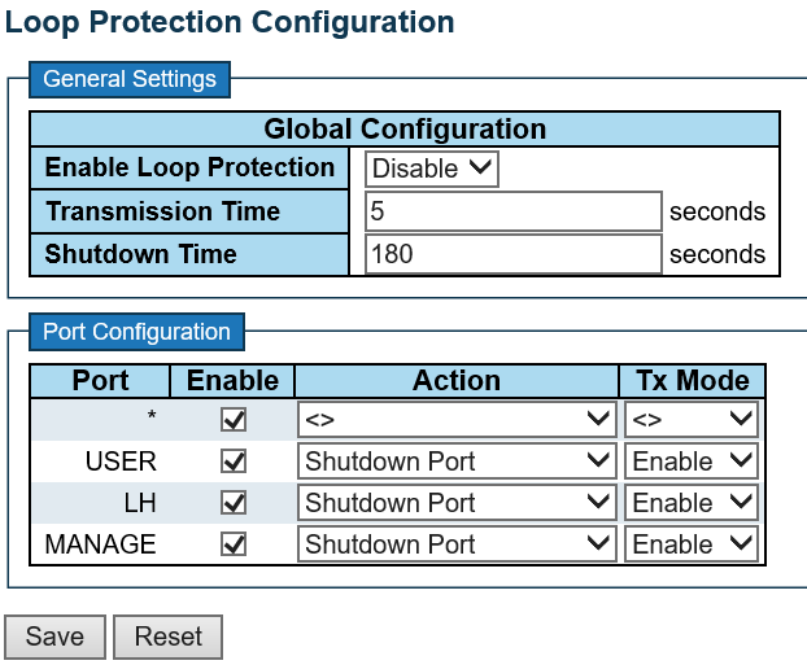
Object	Description
Event Name	Name of the Link Event which is being configured.
Error Window	Represents the window period in the order of 1 sec for the observation of various link events.
Error Threshold	Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.
Error Frame Event	The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.
Symbol Period Error Event	The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.
Seconds Summary Event	The Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 0-65535 and its default value is '1'.

Buttons	
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.22 Loop Protection

This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.



Object	Description
General Settings	
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next system restart). Default value is 180 seconds.
Port Configuration	
Port	The system port number.
Enable	Controls whether loop protection is enabled on this system port.
Action	Configures the action performed when a loop is detected on a port. Valid values are **Shutdown Port** or **Shutdown Port and Log**.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is

	just passively looking for looped PDU's.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.23 LLDP (For PoE Model Only)

This page allows the user to inspect and configure the current LLDP interface settings.

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Interface Configuration

				Optional TLVs				
Interface	**Mode**	**CDP aware**	**Trap**	**Port Descr**	**Sys Name**	**Sys Descr**	**Sys Capa**	**Mgmt Addr**
*	<>	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Disabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled	☐	☐	☑	☑	☑	☑	☑
FastEthernet 1/1	Disabled	☐	☐	☑	☑	☑	☑	☑

Save Reset

Object	Description
LLDP Parameters	
Tx Interval	The system periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the system is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signalling that the LLDP information isn't valid anymore. **Tx Reinit** controls the amount of seconds between the

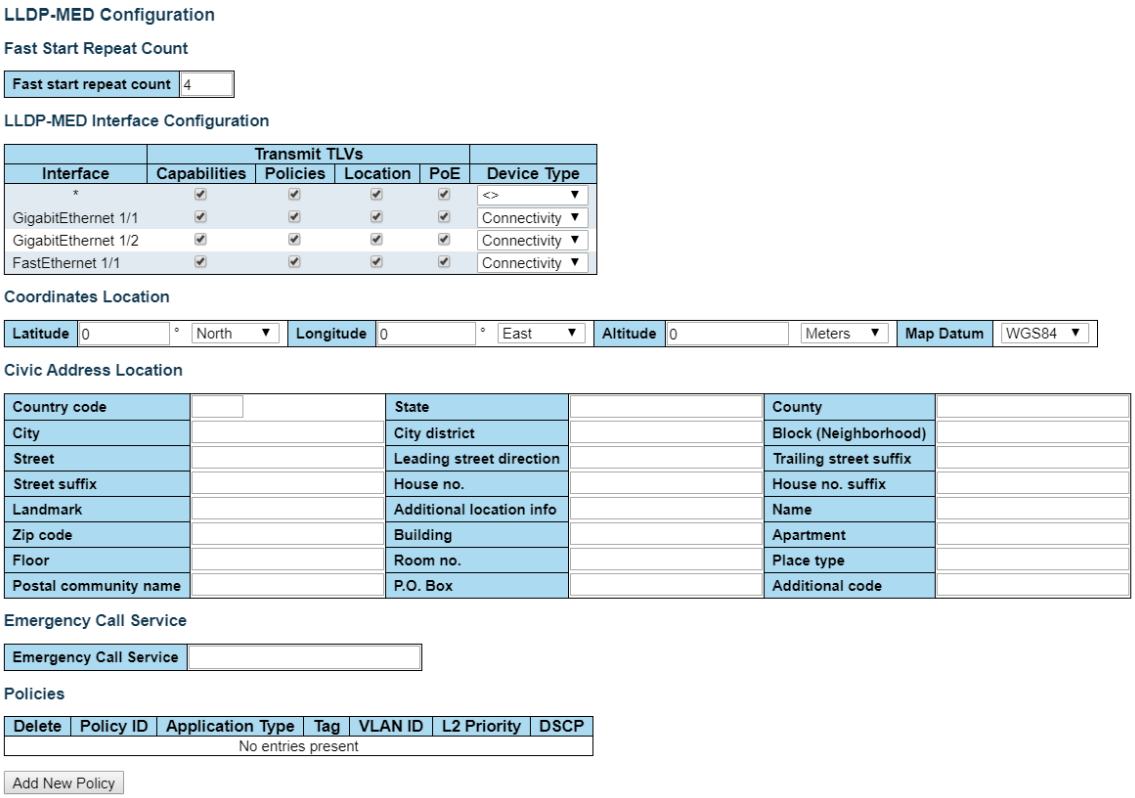
	shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
LLDP Interface Configuration	
Interface	The system interface name of the logical LLDP interface.
Mode	Select LLDP mode. `Rx only` The system will not send out LLDP information, but LLDP information from neighbor units is analyzed. `Tx only` The system will drop LLDP information received from neighbors, but will send out LLDP information. `Disabled` The system will not send out LLDP information, and will drop LLDP information received from neighbors. `Enabled` The system will send out LLDP information, and will analyze LLDP information received from neighbors.
CDP Aware	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The system doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below. CDP TLV "System ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table. If all interfaces have CDP awareness disabled the system forwards CDP frames received from neighbor systems. If at least one interface has CDP awareness enabled all CDP frames are terminated by the system. Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.24 LLDP-MED (For PoE Model Only)

This page allows you to configure the LLDP-MED. This function applies to VoIP systems which support LLDP-MED.



Object	Description
Fast start repeat count	
Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space

	and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors. Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.
LLDP-MED Interface Configuration	
Interface	The interface name to which the configuration applies.
Transmit TLVs - Capabilities	When checked the system's capabilities is included in LLDP-MED information transmitted.
Transmit TLVs - Policies	When checked the configured policies for the interface is included in LLDP-MED information transmitted.
Transmit TLVs - Location	When checked the configured location information for the system is included in LLDP-MED information transmitted.
Transmit TLVs – PoE	When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.
Device Type	Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below. A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies : 1. LAN Switch/Router

	2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method. An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology. The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange. Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together)
Coordinates Location	
Latitude	**Latitude** SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either **North** of the equator or **South** of the equator.
Longitude	**Longitude** SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either **East** of the prime meridian or **West** of the prime meridian.
Altitude	**Altitude** SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters). **Meters:** Representing meters of Altitude defined by the vertical datum specified. **Floors:** Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The **Map Datum** is used for the coordinates given in these options: **WGS84**: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. **NAD83/NAVD88**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical

	Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). **NAD83/MLLW**: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
Civic Address Location	
Country code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Poppelvej.
Leading street direction	Leading street direction - Example: N.
Trailing street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House no.	House number - Example: 21.
House no. suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Flemming Jahn.
Zip code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.
Room no.	Room number - Example: 450F.
Place type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.
Additional code	Additional code - Example: 1320300003.
Emergency Call Service	
Emergency Call Service	**Emergency Call Service** ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
Policies	
Delete	Check to delete the policy. It will be deleted during the next save.

Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.
Application Type	Intended use of the application types: 1. **Voice** - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. **Voice Signalling** (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Voice** application policy. 3. **Guest Voice** - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. **Guest Voice Signalling** (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the **Guest Voice** application policy. 5. **Softphone Voice** - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. **Video Conferencing** - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. **Streaming** Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. **Video Signalling** (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the **Video Conferencing** application policy.

Tag	**Tag** indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. **Untagged** indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. **Tagged** indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.
VLAN ID	VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.
L2 Priority	**L2 Priority** is the Layer 2 priority to be used for the specified application type. **L2 Priority** may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	**DSCP** value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. **DSCP** may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Adding a new policy	Click Add New Policy to add a new policy. Specify the **Application type**, **Tag**, **VLAN ID**, **L2 Priority** and **DSCP** for the new policy. Click "Save". The number of policies supported is 32
Port Policies Interface Configuration	
Interface	The interface name to which the configuration applies.
Policy Id	The set of policies that shall apply to a given interface. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.25 PoE (For 6003GX-POE Only)

This page allows the user to inspect and configure the current PoE port settings.

Power Over Ethernet Configuration

Reserved Power determined by	◉ Class ○ Allocation ○ LLDP-MED
Power Management Mode	◉ Actual Consumption ○ Reserved Power

PoE Port Configuration

Port	Mode	Operation	Maximum Power [W]
*	<>	<>	30
1	Auto-Restart	PoE+	30

Save Reset

Object	Description
Reserved Power determined by	
Allocated mode	In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.
Class mode	In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
LLDP-MED mode	This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode In this mode the Maximum Power fields have no effect For all modes: If a port uses more power than the reserved power for the port, the port is shut down.
Power Management Mode	
Actual Consumption	In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
Reserved Power	In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
Port Configuration	
Port	This is the logical port number for this row.

	Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.
PoE Mode	
Disable	PoE disabled for the port.
Enable	Enables PoE for the port.
Schedule	Enables PoE for the port by scheduling.
Auto-Restart	Enables PoE for the port by scheduling, and also provides the ICMP Ping Detection for Auto-Restart PD in additional. Note: If ping failure event happen continue 3 times, PoE mode will change from Auto-Restart to Disabled.
Operation Mode	
PoE+	Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)
Maximum Power	
The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. The maximum allowed value is 30 W.	

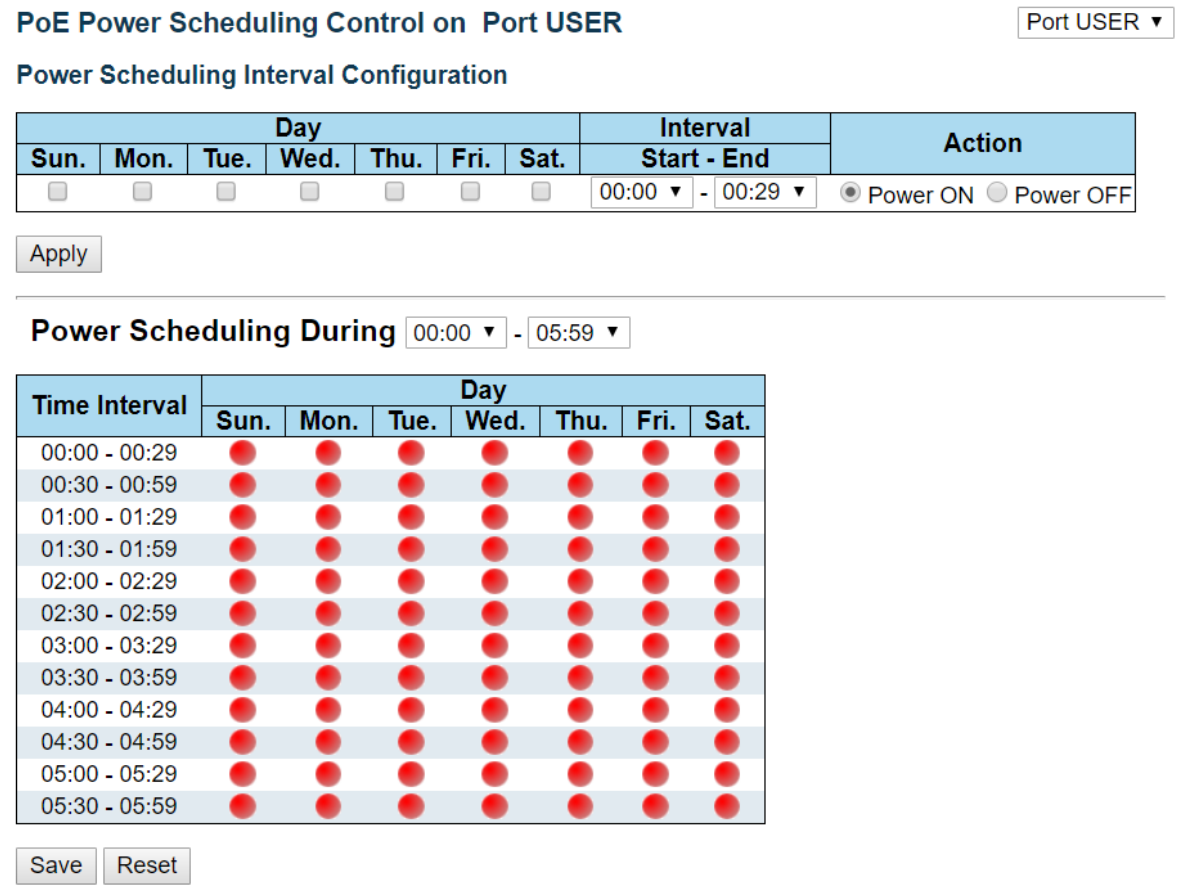
Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.26 PoE Power Scheduler (For 6003GX-POE Only)

This page provides power scheduling configurations.

The entry is used to control the power alive interval on PoE port.

It is allowed to set the specific interval to schedule power on/off in one week.



Object	Description
Power Scheduling Interval Configuration	
Day	Checkmarks indicate which day are members of the set.
Interval	Start - Select the start hour and minute. End - Select the end hour and minute.
Action	Power On - Select the radio button to apply power on during the interval. Power Off - Select the radio button to apply power off during the interval.
Power Scheduling During	
Time Interval	There are 48 time interval one day. Each interval have 30 minutes.
Day	The current scheduling state is displayed graphically during the week. Green indicates the power is on and red that it is off. Directly changes checkmarks to indicate which day are members of the time interval. Check or uncheck as needed to modify the scheduling table.

Buttons

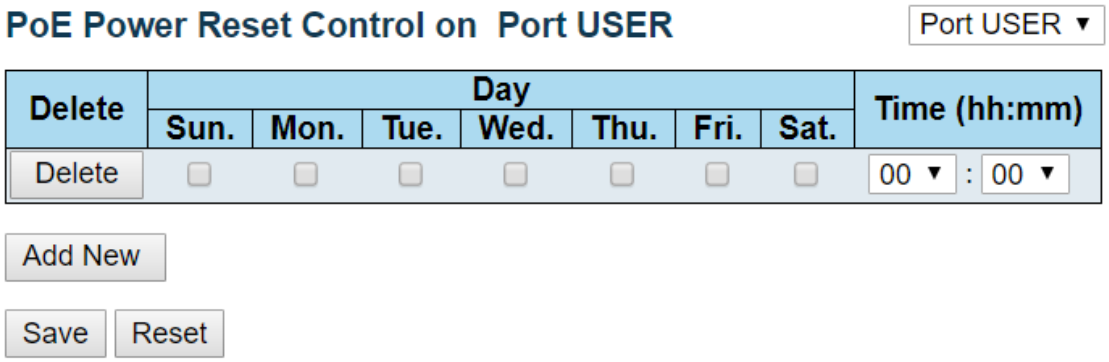
Apply	Click to apply the power scheduling interval.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.27 PoE Power Reset (For 6003GX-POE Only)

This page provides power reset entry configurations.

The entry is used to control the power reset time on PoE port.

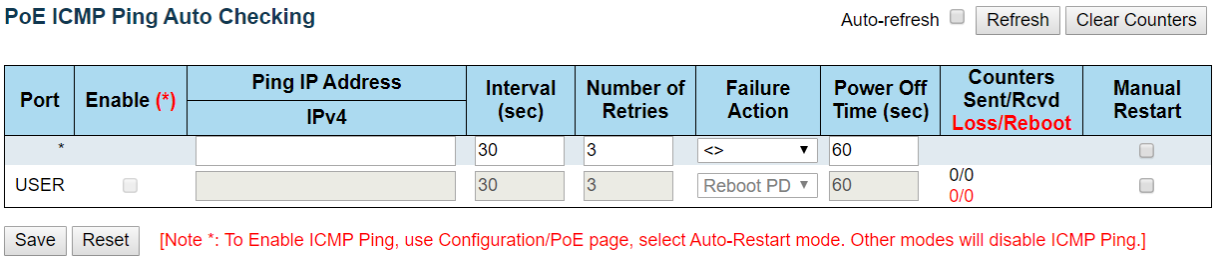
It is allowed to create at maximum 5 entries for each PoE port.



Object	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Day	Checkmarks indicate which day are members of the entry. Check or uncheck as needed to modify the entry.
Time (hh:mm)	hh - Select the hour. mm - Select the minute.

Buttons	
Add New	Click to add new reset entry
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.28 PoE Ping Auto Checking (For PoE Model Only)



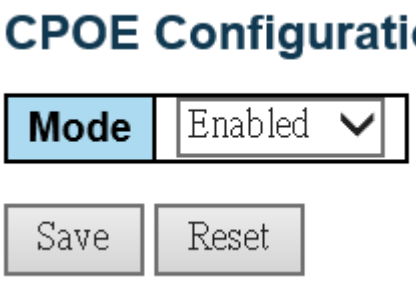
Object	Description
Port	This is the logical port number for this row. Ports not PoE-capable will not be available here.
Enable	ICMP Ping Checking function is Enabled/Disabled. In this page it is status for READ ONLY, to enable/disable it in PoE main configuration page. Select "Auto-Restart" option below the Schedule option. If Auto-Restart is selected, the Schedule still valid and works. So, if the Auto-Restart option is selected, PoE Schedule must be configured, otherwise, there could be no power output for PoE Ports. Note: There are 2 conditions that ping won't be started: 1. When IP is not valid, like 0.0.0.0. 2. When PoE port has no power output, it could be due to no PD connected, or power off per schedule configuration.
Ping IP Address IPv4	IPv4 address of PD for Ping detection per port. Default is ipv4 0.0.0.0.
Interval (sec)	Time interval in second per port, Ping starts when time waiting exceeds this interval since last round, but it would NOT be on time due to wait for other port. Range: 10 ~ 1800 seconds.
Number of Retries	Number of ping retry, system will run the ping repeatly. If retry number is 5, then ping 5+1 times. Range: 1 ~ 5.
Failure Action	If ping, including ping retry, has no any packet received, it is a ping failure event. If failure event happens, system can do nothing or reboot PD per this option. Reboot PD means poe port will stop power output, wait for Power-Off Time and start power output again. Note: If ping failure event happen continue 3 times, PoE mode will change from Auto-Restart to Disabled.
Power Off Time (sec)	Time of PD being power-off if ping failure event happens. If Failure Action is do nothing, this time parameter is not used. Range: 3 ~ 120sec.

Counters Sent/Rcvd/Loss/Reboot	Counters of ping packet sent/received/loss and reboot PD. Counters can be reset manually, if system reboot, counters reset also.
Manual Restart	Restart the PD immediately. PoE of this port will disabled and enabled in 3~5 seconds. But the restart will NOT count in the reboot number.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear Counters	Click to reset counters.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.29 CPOE Configuration (For PoE Model Only)

Configure CPOE on this page.



Object	Description
Mode	Indicates the CPOE mode operation. Possible modes are: Enabled: Enable CPOE mode operation. PoE power supply to PD won't be stopped even if system reboot (reload cold). Disabled: Disable CPOE mode operation.

Buttons	
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

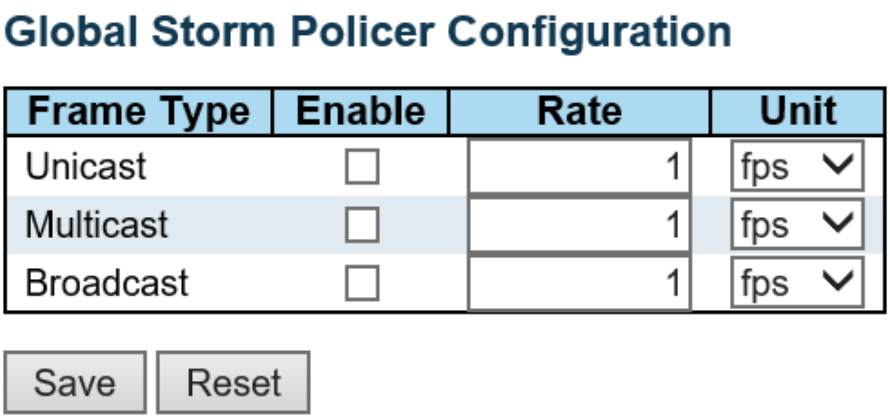
2.3.30 Storm Policing

Global storm policers for the system are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

The displayed settings are:



Object	Description
Frame Type	The frame type for which the configuration below applies.
Enable	Enable or disable the global storm policer for the given frame type.
Rate	Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.
Unit	Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons	
Save	Click to save changes.

Reset	Click to undo any changes made locally and revert to previously saved values.

2.3.31 LPT

Configure LPT on this page. (Link Fault Pass Through)

The LPT function should work as the following description between 2 MC systems, when LPT is enabled.

(USER_PORT_A) [MC_A] (LH) ------- (LH) [MC_B] (USER_PORT_B)

The notification between MC_A and MC_B would be the 802.3ah OAMPDU frame, while LH-Port link up between MC_A and MC_B.

Case 1:

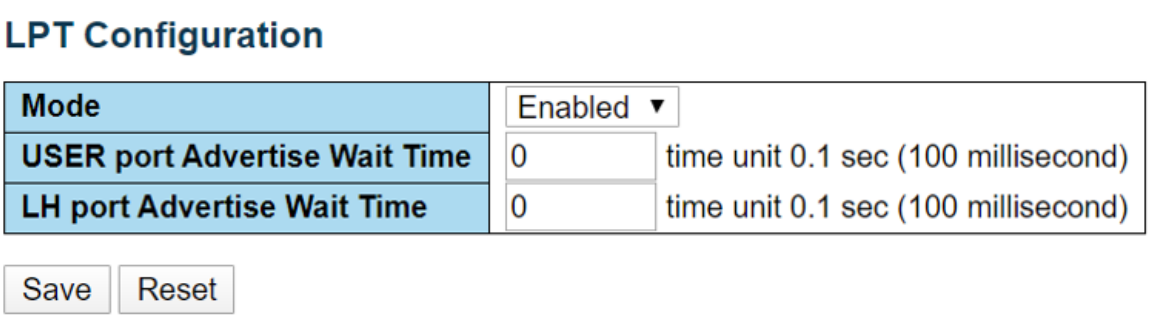
When USER_PORT_A link down, an 802.3ah OAMPDU with "critical event" flag true should be sent from MC_A to MC_B. In such case critical event received in MC_B, OAM LED should be turned on and then USER_PORT_B should be disabled.

Result: USER_PORT_A is in status Link Down , but the USER_PORT_B would be remarked as Link Down(LPT).

Case 2:

When USER_PORT_B link down, an 802.3ah OAMPDU with "critical event" flag true should be sent from MC_B to MC_A. In such case critical event received on MC_A, OAM LED should be turned on and then USER_PORT_A should be disabled.

Result: USER_PORT_B is in status Link Down , but the USER_PORT_A would be remarked as Link Down(LPT).



Object	Description
Mode	Indicates the LPT mode operation. Enabled: Enable LPT mode.

	Disabled: Disable LPT mode. Note: LPT function needs Link OAM function enabled. OAM LED: Turn on when remote Alarm detected, the remote alarm means critical event is true in OAMPDU packet sent by remote 6003GX(POE). Turned off when critical event Alarm cleared (critical event, flag:false).
USER port Advertise Wait Time	Indicates the guard time (delay time) before link fault message to be transmitted when the user port link down is detected, in local system. Valid values range from 0 - 20 (x 100 millisecond), that is 0-2 seconds in step of 0.1 second. default: 0 (no wait)
LH port Advertise Wait Time	Indicates the guard time (delay time) before link fault message to be transmitted when the lh port link down is detected, in local system. Valid values range from 0 - 20 (x 100 millisecond), that is 0-2 seconds in step of 0.1 second. default: 0 (no wait)

Buttons	
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

2.4 Monitor

2.4.1 System

2.4.2 System Information

The system information is provided here.

System Information

Auto-refresh ☐ Refresh

System	
Contact	
Name	
Location	
Hardware	
Product Name	6003GX-POE
MAC Address	00-40-66-e0-a7-1a
Serial Number	306830888
Temperature-PSE	69 C
Time	
System Date	2020-04-23 14:02:48+09:00
System Uptime	0days 01:13:03
Software	
Software Version	1.00.02
Software Date	2020-04-23 10:11:34+08:00
Acknowledgments	Details

Object	Description
Contact	The system contact configured in Configuration | System | Information | System Contact.
Name	The system name configured in Configuration | System | Information | System Name.
Location	The system location configured in Configuration | System | Information | System Location.
Product Name	The model name of the system.
MAC Address	The MAC Address of this system.
Serial Number	The system's serial number
Temperature-PSE (For PoE Model Only)	The temperature of PSE chip.
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the system, if any.
System Uptime	The period of time when the system has been operational.
Software Version	The software version of this system.
Software Date	The date when the system software was produced.
Acknowledgements	Display detailed license statement about CPU-load, MD5, NET-SNMP, NET-SNMP RMON, libcxx and libfetch.

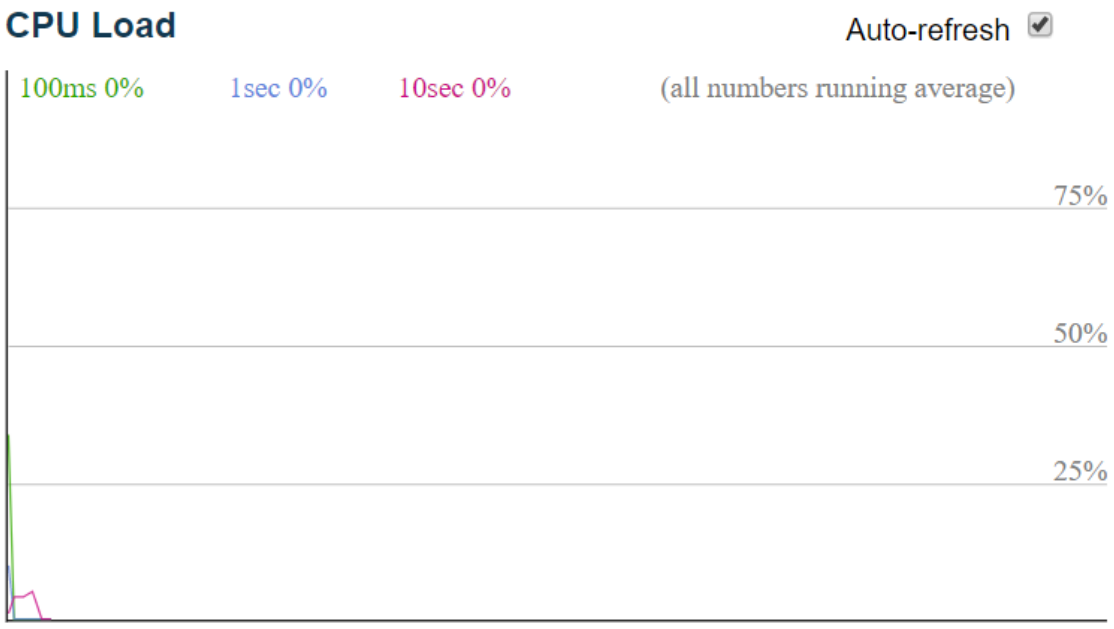
Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.3 CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well.

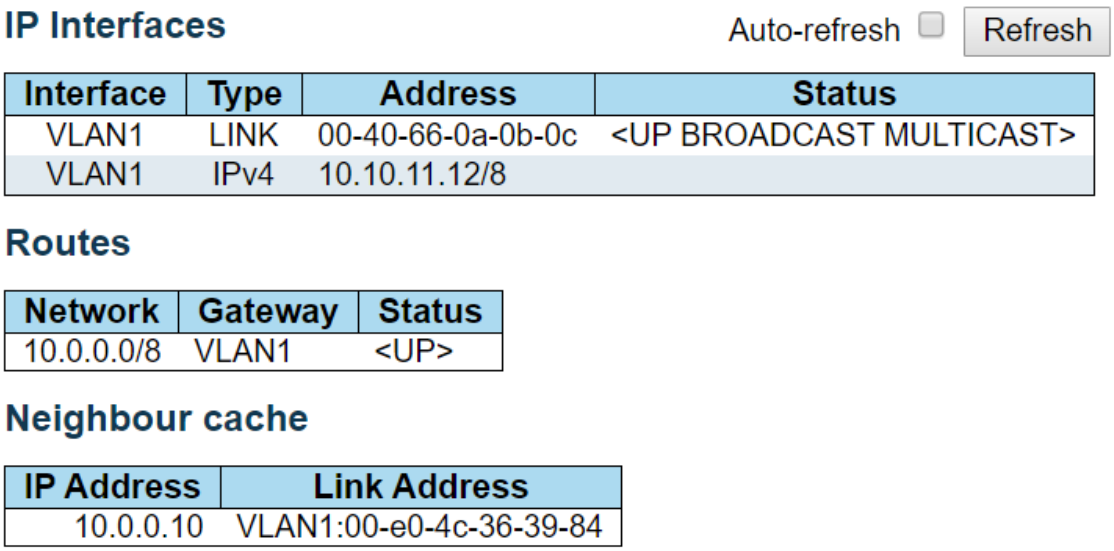
In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.



Buttons	
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.4 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbor cache (ARP cache) status.



Object	Description
IP Interfaces	
Interface	The name of the interface.
Type	The address type of the entry. This may be **LINK** or **IPv4**.
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address).
Routes	
Network	The destination IP network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route.
Neighbor cache	
IP Address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist.

Buttons	
Refresh	Click to refresh the page.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.5 System Log

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.
The "Clear Level" input field is used to specify which system log entries will be cleared.

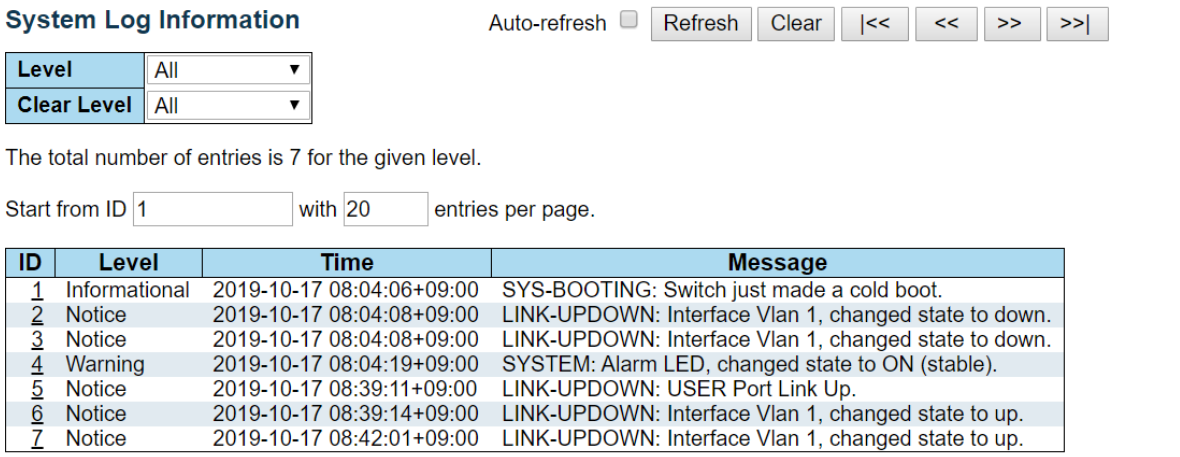
To clear specific system log entries, select the clear level first then click the Clear button.

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the Refresh button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The >> will use the last entry of the currently displayed table as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



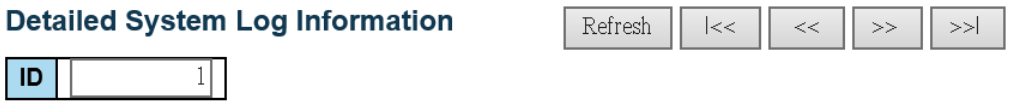
Object	Description
ID	The identification of the system log entry.
Level	The level of the system log entry. **Info**: The system log entry is belonged information level. **Warning**: The system log entry is belonged warning level.

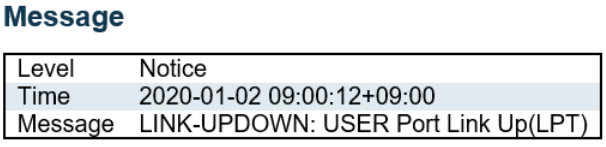
	Error: The system log entry is belonged error level.
Time	The occurred time of the system log entry.
Message	The detail message of the system log entry.

Buttons	
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Updates the table entries, starting from the current entry.
Clear	Flushes the selected entries.
|<<	Updates the table entries, starting from the first available entry.
<<	Updates the table entries, ending at the last entry currently displayed.
>>	Updates the table entries, starting from the last entry currently displayed.
>>|	Updates the table entries, ending at the last available entry.

2.4.6 System Detailed Log

The system detailed log information is provided here.



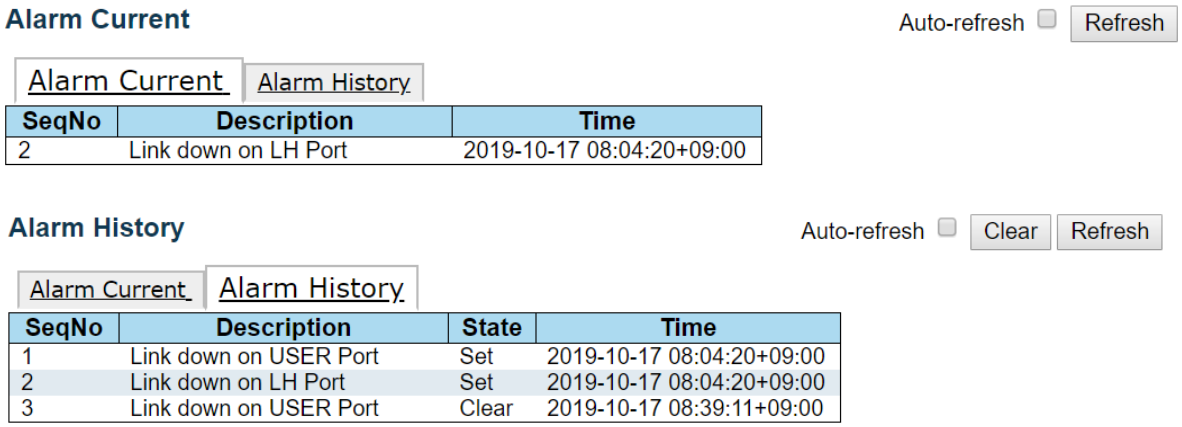


Object	Description
Level	The severity level of the system log entry.
ID	The ID (>= 1) of the system log entry.
Message	The detailed message of the system log entry.

Buttons	
Refresh	Updates the system log entry to the current entry ID.
|<<	Updates the system log entry to the first available entry ID.
<<	Updates the system log entry to the previous available entry ID.
>>	Updates the system log entry to the next available entry ID.
>>|	Updates the system log entry to the last available entry ID.

2.4.7 System Alarm

Current & History Alarm is provided on this page.



Object	Description
Alarm Current	
SeqNo	Alarm Sequence Number.
Description	Alarm Type Description..
Time	Alarm occurrence date time.
Alarm History	
SeqNo	Alarm Sequence Number.
Description	Alarm Type Description..
State	Alarm State. Set stands for alarm occurs; Cleared stands for alarm disappear.
Time	Alarm occurrence/cleared date time

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh	Click to refresh data.
Clear	Click to Clear data.

2.4.8 Ports State

This page provides an overview of the current system port states.

The port states are illustrated as follows:

RJ45 ports			
SFP ports			
State	Disabled	Down	Link

PWR		Light on with Green when system gets Power.
LOOP		Light on with Red when system detects loop condition.
ALM		Light on with Red when system has alarm happened.
LINK/ACT		Light on with green when LH Port link up, flash when traffic pass through.
PoE (For 6003GX-POE Only)		PoE status indicator (Supported depends on HW): - Off (dark green): No power ouput. - Green: PoE port is connected to PoE device, has power output. - Amber: PoE port is connected but with abnormal status.
OAM		Light on with Red when system detects EFM-OAM events, including Link Fault, Critical Event, Dying Gasp.

Buttons

Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.9 Trafice Overview

This page provides an overview of general traffic statistics for all system ports.

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
USER	7719	5838	1218817	1474279	0	0	0	0	2364
LH	0	1	0	68	0	0	0	0	0
MANAGE	0	0	0	0	0	0	0	0	0

Object	Description
Port	The logical port for the settings contained in the same row.
Packet	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

Buttons	
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for all ports.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.10 Detailed Statistics

This page provides detailed traffic statistics for a specific system port. Use the port select box to select which system port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Port Statistics Port USER

Port USER ▾ Auto-refresh ☐ Refresh Clear

Receive Total		Transmit Total	
Rx Packets	8336	Tx Packets	6526
Rx Octets	1340261	Tx Octets	1725070
Rx Unicast	5458	Tx Unicast	6519
Rx Multicast	2372	Tx Multicast	0
Rx Broadcast	506	Tx Broadcast	7
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3455	Tx 64 Bytes	2039
Rx 65-127 Bytes	3294	Tx 65-127 Bytes	2228
Rx 128-255 Bytes	272	Tx 128-255 Bytes	435
Rx 256-511 Bytes	7	Tx 256-511 Bytes	1037
Rx 512-1023 Bytes	1264	Tx 512-1023 Bytes	197
Rx 1024-1526 Bytes	44	Tx 1024-1526 Bytes	590
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	8336	Tx Q0	6521
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	5
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	2372		

Object	Description
Receive Total and Transmit Total	
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	
The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.	
Receive and Transmit Queue Counters	
The number of received and transmitted packets per input and output queue.	
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short[1] frames received with valid CRC.
Rx Oversize	The number of long[2] frames received with valid CRC.
Rx Fragments	The number of short[1] frames received with invalid CRC.
Rx Jabber	The number of long[2] frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Note: [1]Short frames are frames that are smaller than 64 bytes.	

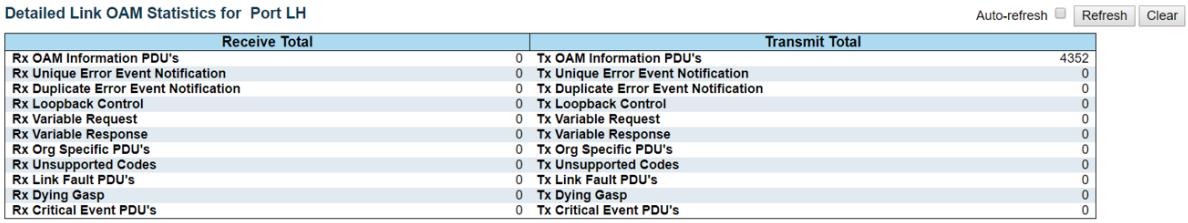
[2]Long frames are frames that are longer than the configured maximum frame length for this port.	
Transmit Error Counters	
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

Buttons	
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for the selected ports.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.11 Link OAM Statistics

This page provides detailed OAM traffic statistics for a specific system port. Use the port select box to select which system port details to display.

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.



Object	Description
Rx and Tx OAM Information PDU's	The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.
Rx and Tx Unique Error Event Notification	A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.
Rx and Tx Duplicate Error Event Notification	A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted

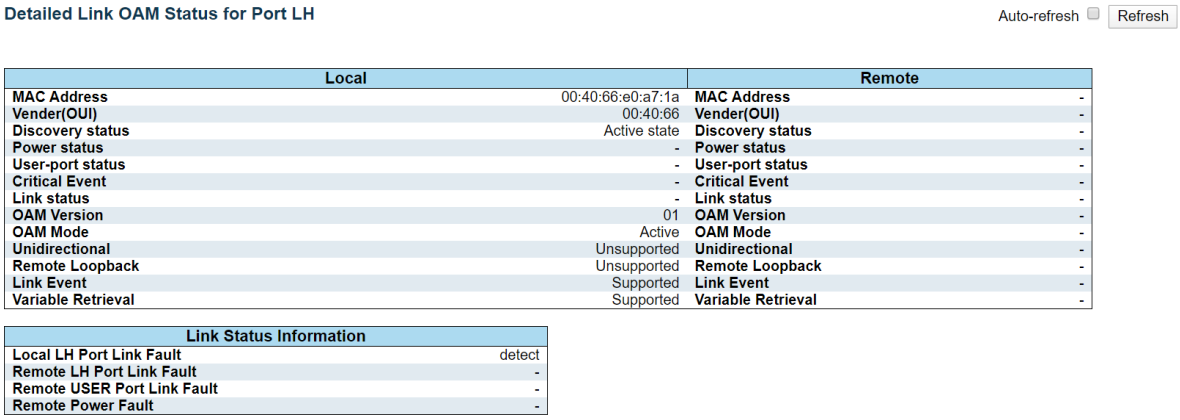
	Event Notification OAMPDU Sequence Number.
Rx and Tx Loopback Control	A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.
Rx and Tx Variable Request	A count of the number of Variable Request OAMPDUs received and transmitted on this interface.
Rx and Tx Variable Response	A count of the number of Variable Response OAMPDUs received and transmitted on this interface.
Rx and Tx Org Specific PDU's	A count of the number of Organization Specific OAMPDUs transmitted on this interface.
Rx and Tx Unsupported Codes	A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.
Rx and Tx Link fault PDU's	A count of the number of Link fault PDU's received and transmitted on this interface.
Rx and Tx Dying Gasp	A count of the number of Dying Gasp events received and transmitted on this interface.
Rx and Tx Critical Event PDU's	A count of the number of Critical event PDU's received and transmitted on this interface.

Buttons	
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for the selected ports.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.12 Link OAM Port Status

This page provides Link OAM configuration operational status.

The displayed fields show the active configuration status for the selected port.



Object	Description

Local/Remote	
MAC Address	MAC address.
Vender(OUI)	Vendor identifier(OUI).
Discovery Status	Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.
Power status	For local is always show dash(-); for remote field, it is status of device power as following. Up: Power up. Down: Power down (dying gasp frame is received).
User-Port Status	For local it always show dash(-); for remote field, it shows Up/Down depends on Critical Event Flag/Bit. (note: this status could be changed by 'link-oam critical-event-mode ais' of LH Port.). Up: OAM frame with critical event (false) is received. Down: OAM frame with critical event (true) is received.
Critical Event	For local, it always show dash(-); for remote field, it shows Up/Down depends on Critical Event Flag/Bit. (note: this status could be changed by 'link-oam critical-event-mode ais' of LH Port.). Up: Critical Event false (bit=0) is received. Down: Critical Event true (bit=1) is received.
Link status	LH Port status. For local, it always show dash(-); for remote field, Up/Down depends on EFM-OAM status or LH Port status. Up: Frame with Link Fault (bit=0) is received. Down: Frame with Link Fault (bit=1) is received. '-': When efm-oam of remote device is disabled or when LH port of this device is linkdown.
OAM Version	Link-OAM version.
OAM Mode	The Mode in which the Link OAM is operating, Active or Passive.
Unidirectional	This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.
Remote Loopback	If status is enabled, DTE is capable of OAM remote loopback mode.
Link Event	If status is enabled, DTE supports interpreting Link Events.
Variable Retrieval	If status ie enabled DTE supports sending Variable Response OAMPDUs.
Link Status Information	
Local LH Port Link Fault	It is local LH Port Link Fault status. If local LH Port is Link up, it shows dash("-"). If local LH Port is Link down, it shows "detect".
Remote LH Port Link Fault	It shows Link Fault status of Remote LH Port, accroding to EFM-OAM Link Fault flag. When 6003GX receives OAMPDU with Link Fault (bit=0), it shows dash("-"). When 6003GX receives OAMPDU frame with Link Fault (bit=1), it shows "detect".
Remote USER Port Link	It shows Link Fault status of Remote User Port, according to EFM-OAM Critical Event

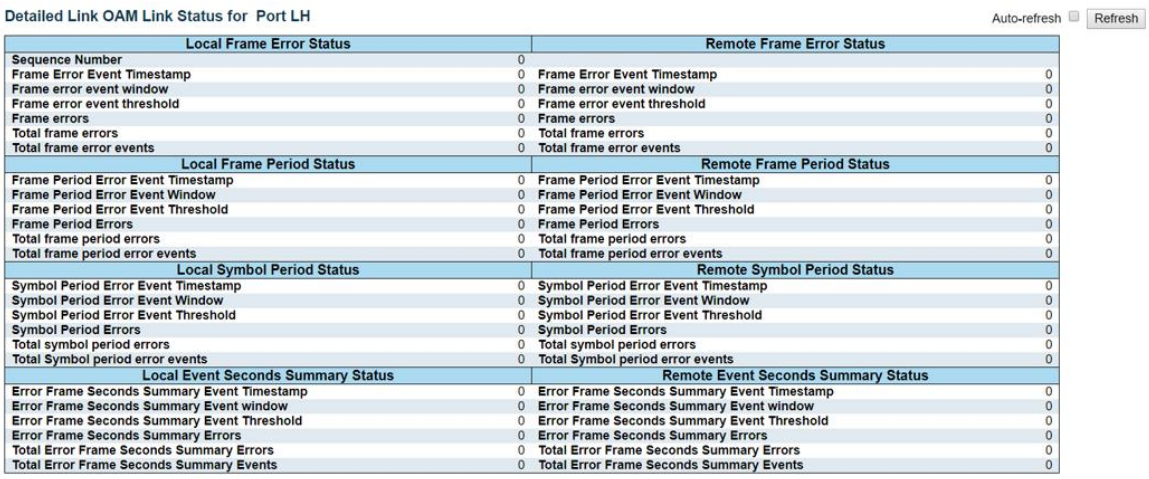
Fault	flag. When 6003GX receives OAMPDU with critical event (bit=0), it shows dash("-"). When 6003GX receives OAMPDU with critical event (bit=1), it shows "detect".
Remote Power Fault	It is Power status of Remote device. When no Dying Gasp is received in local, it shows dash("-"). When Dying Gasp frame is received in local and it shows "detect" which means remote device could be power off.

Buttons	
Refresh	Click to refresh the page immediately.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.13 Link OAM Event Status

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.



Object	Description
Sequence Number	This two-octet field indicates the total number of events occurred at the remote end.
Frame Error Event Timestamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
Frame error event window	This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.
Frame error event	This four-octet field indicates the number of detected errored frames in the period is

threshold	required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.
Frame errors	This four-octet field indicates the number of detected errored frames in the period.
Total frame errors	This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.
Total frame error events	This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.
Frame Period Error Event Timestamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
Frame Period Error Event Window	This four-octet field indicates the duration of period in terms of frames.
Frame Period Error Event Threshold	This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.
Frame Period Errors	This four-octet field indicates the number of frame errors in the period.
Total frame period errors	This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.
Total frame period error events	This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.
Symbol Period Error Event Timestamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.
Symbol Period Error Event Window	This eight-octet field indicates the number of symbols in the period.
Symbol Period Error Event Threshold	This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.
Symbol Period Errors	This eight-octet field indicates the number of symbol errors in the period.
Total symbol period errors	This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.
Total Symbol period error events	This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.
Error Frame Seconds Summary Event Timestamp	This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
Error Frame Seconds Summary Event window	This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.
Error Frame Seconds Summary Event Threshold	This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.
Error Frame Seconds	This two-octet field indicates the number of errored frame seconds in the period,

Summary Errors	encoded as a 16-bit unsigned integer.
Total Error Frame Seconds Summary Errors	This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.
Total Error Frame Seconds Summary Events	This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

Buttons	
Refresh	Click to refresh the page immediately.
Clear	Click to clear the data.
Auto-refresh ☑	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.4.14 Security

2.4.15 Accessment Management Statistics

This page provides statistics for access management.

Access Management Statistics Auto-refresh ☐ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Object	Description
Interface	The interface type through which the remote host can access the system.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh	Click to refresh the page immediately.
Clear	Clear all statistics.

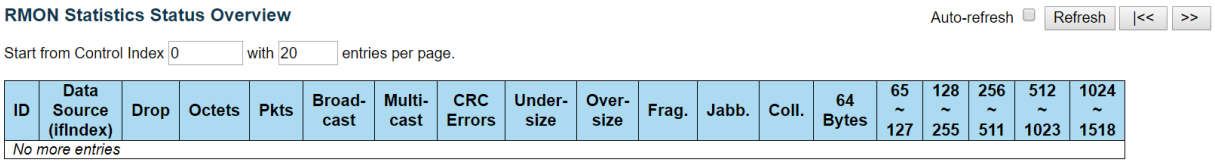
2.4.16 RMON Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

The displayed counters are:



Object	Description
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-Cast	The total number of good packets received that were directed to the broadcast address.
Multi-Cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad

	Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-Size	The total number of packets received that were less than 64 octets.
Over-Size	The total number of packets received that were longer than Max. Frame Size.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than Max. Frame Size and with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1518	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
|<<	Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

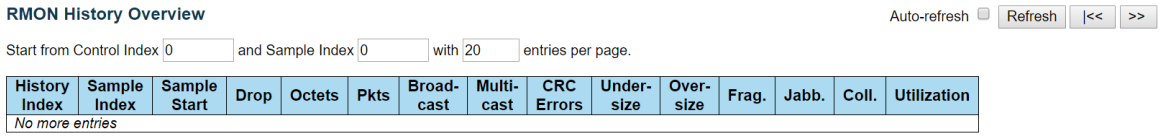
2.4.17 RMON History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

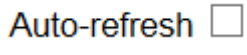
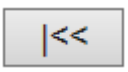
The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next

closest History table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



Object	Description
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.
CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than Max. Frame Size.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than Max. Frame Size and with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons	
	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
	Click to refresh the page immediately.
	Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.

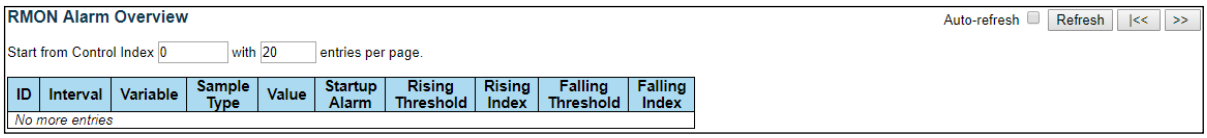
>>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.18 RMON Alarm

This page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the Refresh button will update the displayed table starting from that or the next closest Alarm table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



Object	Description
ID	Indicates the index of Alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled.
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
Startup Alarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	Rising threshold value.
Rising Index	Rising event index.
Falling Threshold	Falling threshold value.
Falling Index	Falling event index.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh	Click to refresh the page immediately.
|<<	Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
>>	Updates the table, starting with the entry after the last entry currently displayed.

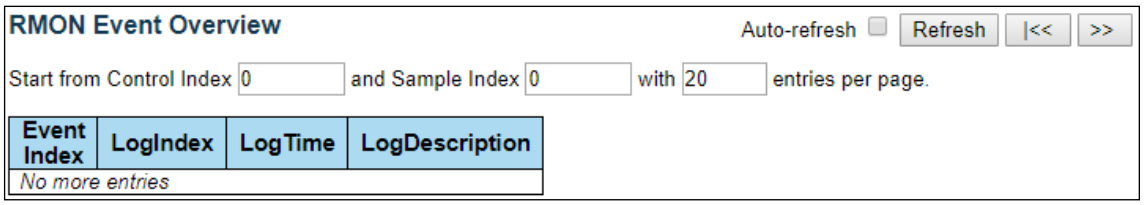
2.4.19 RMON Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "Start from Event Index and Log Index" allows the user to select the starting point in the Event table.

Clicking the Refresh button will update the displayed table starting from that or the next closest Event table match.

The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.



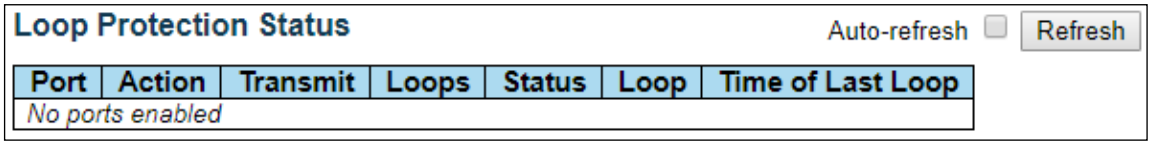
Object	Description
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
Log Time	Indicates Event log time.
LogDescription	Indicates the Event description.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.

|<<	Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
>>	Updates the table, starting with the entry after the last entry currently displayed.

2.4.20 Loop Protection

This page displays the loop protection port status the ports of the system.

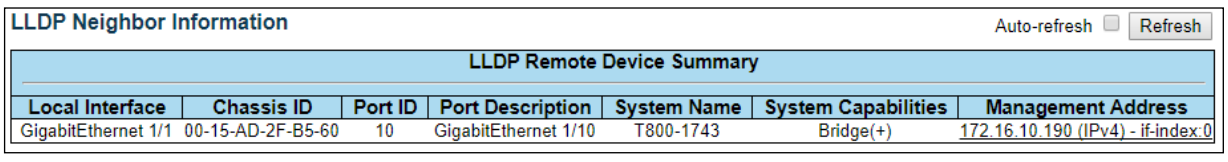


Object	Description
Port	The system port number of the logical port.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

Buttons	
Refresh	Click to refresh the page immediately.
Auto-refresh ☐	Check this box to enable an automatic refresh of the page at regular intervals.

2.4.21 LLDP Neighbors (For PoE Model Only)

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.



Object	Description
Local Interface	The Interface on which the LLDP frame was received.

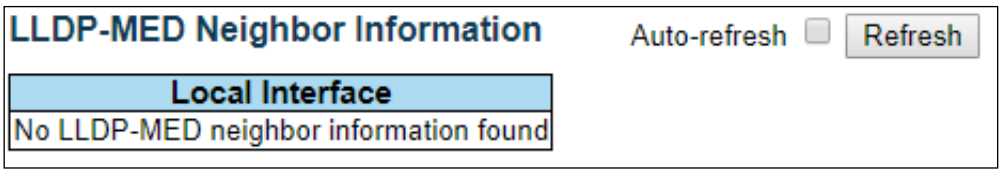
Chassis ID	The **Chassis ID** is the identification of the neighbor's LLDP frames.
Port ID	The **Port ID** is the identification of the neighbor port.
Port Description	**Port Description** is the port description advertised by the neighbor unit.
System Name	**System Name** is the name advertised by the neighbor unit.
System Capabilities	**System Capabilities** describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
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.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.22 LLDP-MED Neighbors (For PoE Model Only)

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. This function applies to VoIP devices which

support LLDP-MED.



Object	Description
Interface	The Interface on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary **Device Types**: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a

	Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I)** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II)** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III)** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.
LLDP-MED Capabilities	**LLDP-MED Capabilities** describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

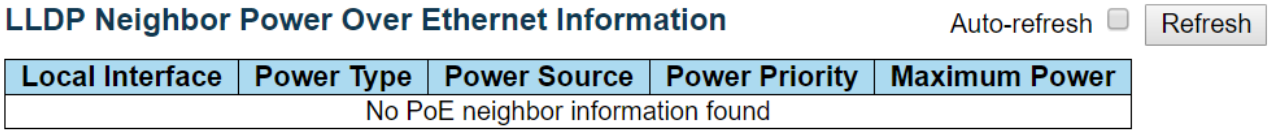
	1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
Application Type	**Application Type** indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media. 3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

	8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.
Policy	**Policy** indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown Unknown: The network policy for the specified application type is currently unknown. Defined: The network policy is defined.
TAG	**TAG** is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. Tagged: The device is using the IEEE 802.1Q tagged frame format.
VLAN ID	**VLAN ID** is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the system is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.
Priority	**Priority** is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP	**DSCP** is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto-Negotiation	**Auto-negotiation** identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-Negotiation Status	**Auto-negotiation status** identifies if auto-negotiation is currently enabled at the link partner. If **Auto-negotiation** is supported and **Auto-negotiation status** is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	**Auto-negotiation Capabilities** shows the link partners MAC/PHY capabilities.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.23 LLDP PoE (For PoE Model Only)

This page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected.



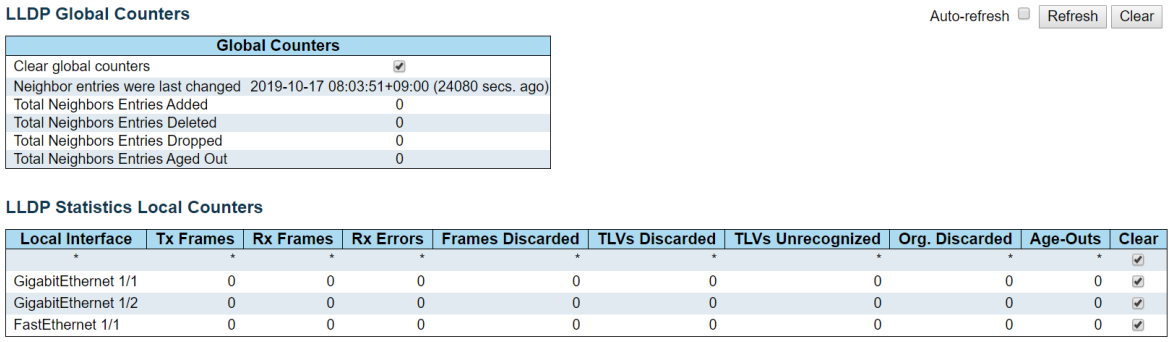
Object	Description
Local Interface	The interface for this system on which the LLDP frame was received.
Power Type	The Power Type represents whether the system is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".
Power Source	The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE system is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD system is using it is indicated as "Unknown"
Power Priority	Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as "Unknown"
Maximum Power	The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved"

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.24 LLDP Port Statistics (For PoE Model Only)

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole system, while local counters refer to per interface counters for the currently selected system.



Object	Description
Global Counters	
Clear global counters	If checked the global counters are cleared when Clear is pressed.
Neighbor entries were last changed	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since system reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since system reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.
Local Counters	
Local Interface	The interface on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the interface.
Rx Frames	The number of LLDP frames received on the interface.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If a LLDP frame is received on an interface, and the system's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface 's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.

Org. Discarded	If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the **Age-Out** counter is incremented.
Clear	If checked the counters for the specific interface are cleared when Clear is pressed.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.
Clear	Clears the counters which have the corresponding checkbox checked.

2.4.25 PoE (For 6003GX-POE Only)

This page allows the user to inspect the current status for all PoE ports.

Power Over Ethernet Status Auto-refresh ☐ Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

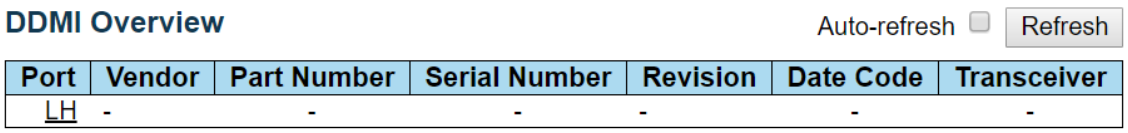
Object	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined: Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the system has allocated for the PD.
Power Used	The Power Used shows how much power the PD currently is using.

Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status. The status can be one of the following values: PoE turned ON - PoE port has power output. PoE not available - No PoE chip found - PoE not supported for the port. PoE turned OFF - PoE disabled: PoE is disabled by user. No PD detected - No PD detected for the port. PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down. PoE turned OFF - PD is off. Invalid PD - PD detected, but is not working correctly.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.4.26 DDMI Overview

Display DDMI overview information on this page.



Object	Description
Port	DDMI port.
Vendor	Indicates Vendor name SFP vendor name.
Part Number	Indicates Vendor PN Part number provided by SFP vendor.
Serial Number	Indicates Vendor SN Serial number provided by vendor.
Revision	Indicates Vendor rev Revision level for part number provided by vendor.
Date Code	Indicates Date code Vendor's manufacturing date code.
Transceiver	Indicates Transceiver compatibility.

2.4.27 DDMI Detailed

Display DDMI detailed information on this page.

Transceiver Information

Port LH ▾ Auto-refresh ☐ Refresh

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

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(dBm)	-	-	-	-	-
Rx Power(dBm)	-	-	-	-	-

Object	Description
Transceiver Information	
Vendor	Indicates Vendor name SFP vendor name.
Part Number	Indicates Vendor PN Part number provided by SFP vendor.
Serial Number	Indicates Vendor SN Serial number provided by vendor.
Revision	Indicates Vendor rev Revision level for part number provided by vendor.
Date Code	Indicates Date code Vendor's manufacturing date code.
Transceiver	Indicates Transceiver compatibility.
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.

Buttons	
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

2.5 Diagnostics

2.5.1 Ping(IPv4)

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.

After you press Start, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

PING 2001::01 (2001::1) from 2001::3: 56 data bytes

64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms

64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms

64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms

64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms

64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.845/2.138/2.869 ms

Ping (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
TTL Value	64	
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	☐	

Start

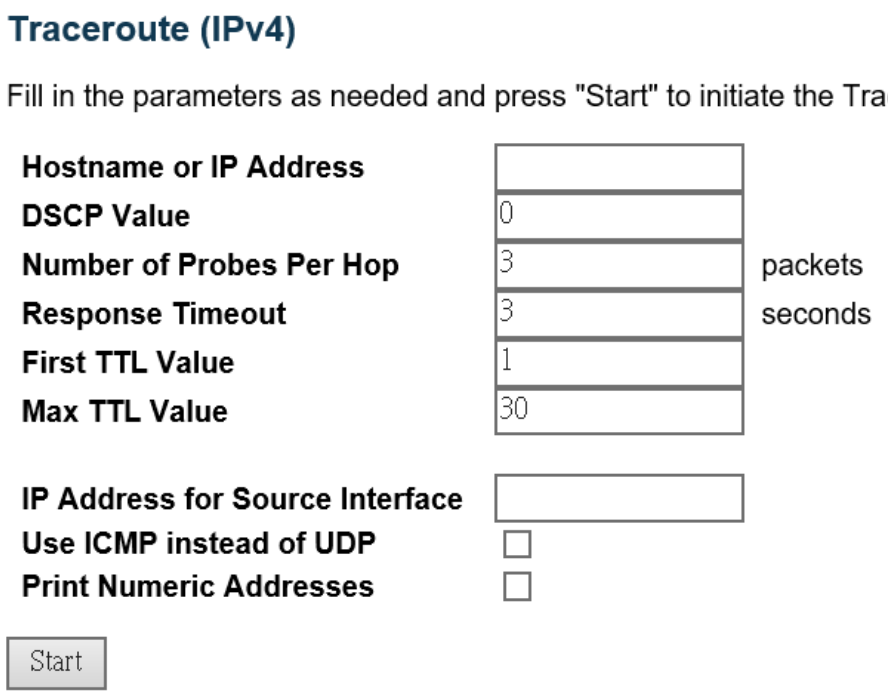
Object	Description
Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.
Packet Count	Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.
TTL Value	Determines the Time-To-Live /TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.
Source Port Number	This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Quiet (only print result)	Checking this option will not print the result of each ping request but will only show the final result.

Buttons

Start	Click to start transmitting ICMP packets.
New Ping	Click to re-start diagnostics with PING.

2.5.2 Traceroute (IPv4)

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.



Object	Description
Hostname or IP Address	The destination IP Address.
DSCP Value	This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.
Number of Probes Per Hop	Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.
Response Timeout	Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.
First TTL Value	Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.
Max TTL Value	Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

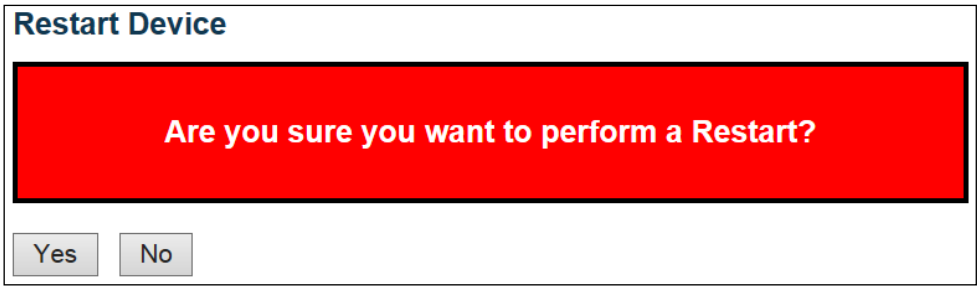
Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Use ICMP instead of UDP	By default the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.
Print Numeric Addresses	By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons	
Start	Click to perform a traceroute test.

2.6 Maintenance

2.6.1 Restart Device

You can restart the system on this page. After restart, the system will boot normally.

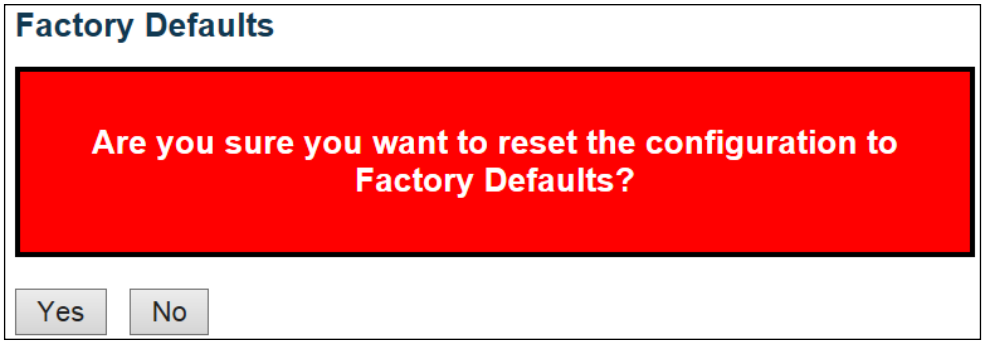


Buttons	
Yes	Click to restart system.
No	Click to return to the Port State page without restarting.

2.6.2 Factory Default

You can reset the configuration of the system.

The new configuration is available immediately, which means that no restart is necessary.

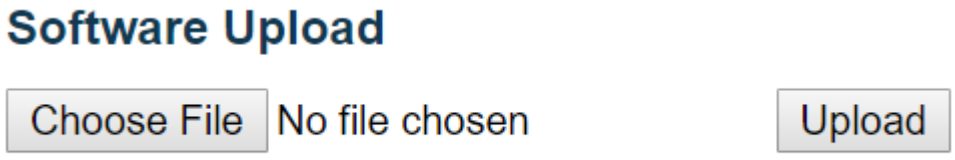


Buttons	
Yes	Click to reset the configuration to Factory Defaults.
No	Click to return to the Port State page without resetting the configuration.

2.6.3 Software

2.6.4 Software Upload

This page facilitates an update of the firmware controlling the system.



Buttons	
Choose File	Select the location of a software image and click Choose File.
Upload	Click to start the firmware upgrade process.

After the software image is uploaded, a page announces that the firmware update is initiated. After about a few minutes, the firmware is updated and the system restarts.

Warning: *While the firmware is being updated, Web access appears to be defunct. Do not restart or power off the system at this time or the system may fail to function afterwards.*

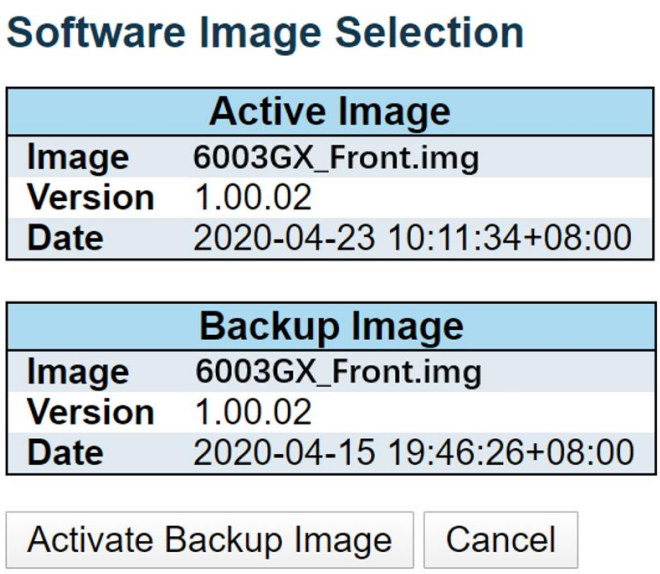
2.6.5 Image select

This page provides information about the active and backup firmware images in the system, and allows you to revert to the backup image.

The web page displays two tables with information about the active and backup firmware images.

Note:

1. In case the active firmware image is the backup image, only the "Active Image" table is shown. In this case, the `Activate Backup Image` button is also disabled.
2. If the backup image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the system will automatically use the primary image slot and activate this.
3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



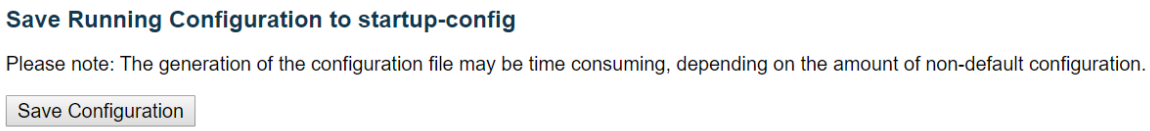
Object	Description
Image	The file name of the firmware image, from when the image was last updated.

Version	The version of the firmware image.
Data	The date where the firmware was produced.

Buttons	
Activate Backup Image	Click to use the backup image. This button may be disabled depending on system state.
Cancel	Cancel activating the backup image. Navigates away from this page.

2.6.6 Save Configuration

This copies running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.



2.6.7 Download Configuration

It is possible to download any of the files on the system to the web browser. Select the file and click

.

Download *running-config* may take a little while to complete, as the file must be prepared for download.

Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
running-config
.ca
default-config
shiftTime
history_cmd_log
startup-config

Download Configuration

2.6.8 Upload Configuration

It is possible to upload a file from the web browser to all the files on the system, except default-config which is read-only.

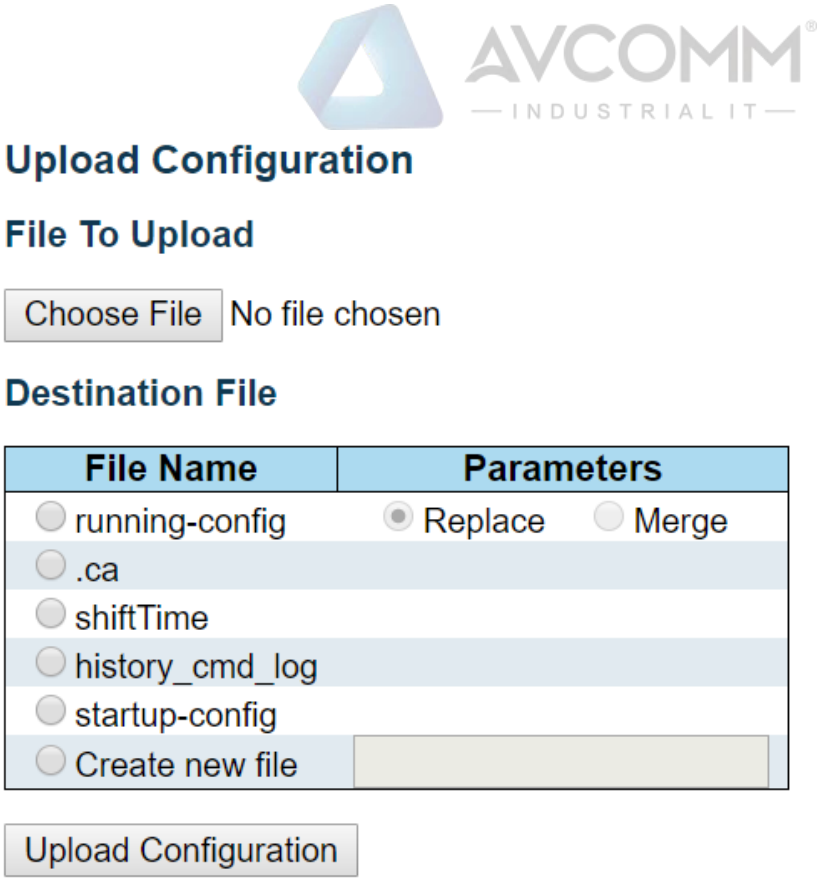
Select the file to upload, select the destination file on the target, then click Upload Configuration.

If the destination is running-config, the file will be applied to the system configuration. This can be done in two ways:

Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.

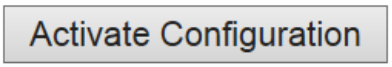
Merge mode: The uploaded file is merged into running-config.

If the flash file system is full (i.e. contains default-config and 32 other files, usually including startup-config), it is not possible to create new files. Instead an existing file must be overwritten or another file must be deleted.

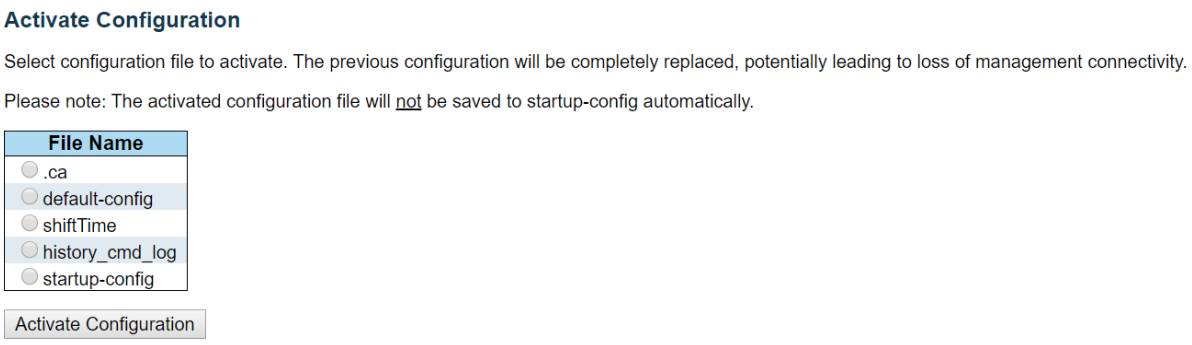


2.6.9 Activate Configuration

It is possible to activate any of the configuration files present on the system, except for running-config which represents the currently active configuration.

Select the file to activate and click 

. This will initiate the process of completely replacing the existing configuration with that of the selected file.



2.6.10 Delete Configuration

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done

and the system is rebooted without a prior Save operation, this effectively resets the system to default configuration.