



See every bit, byte, and packet®

The EdgeLens® In-Line Security Packet Broker System

INT10G2SRBP10SFP
INT10G2LRBP10SFP
INT10G8SRBP16SFP
INT10G8LRBP16SFP

Graphical User Guide

Firmware Rev Level: **n280X_8.28-20** Ver-4

Garland Technology, LLC
New York | Texas | Germany
Office: 716-242-8500
support@garlandtechnology.com
www.garlandtechnology.com

TITLE: INT10GXXXBP GRAPHICAL USER INTERFACE GUIDE	Garland Technology Confidential & Proprietary	REV: 2.0	PAGE 1 OF 70
---	---	----------	--------------

Copyright © 2016 Garland Technology LLC. All Rights Reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of Garland Technology.

TRADEMARKS GARLAND TECHNOLOGY and THE GARLAND TECHNOLOGY LOGO are trademarks of Garland Technology LLC. in the U.S. and other countries. The use of any of these trademarks without Garland Technology prior written consent is strictly prohibited. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Garland Technology LLC. disclaims any proprietary interest in the trademarks and trade names other than its own.

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Garland Technology. Information in this document is subject to change without notice.

REQUESTS For information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Garland Technology on www.garlandtechnology.com

DOCUMENT No.: n280X_8.28-20

TITLE: INT10GXXXBP GRAPHICAL USER INTERFACE GUIDE	Garland Technology Confidential & Proprietary	REV: 2.0	PAGE 2 OF 70
---	---	----------	--------------

Table of Contents

1. OVERVIEW.....	9
2. SERIAL CONSOLE CONFIGURATION	9
3. MANAGEMENT INTERFACE.....	10
3.1 MANAGEMENT CONFIGURATION.....	10
3.2 LOGIN.....	10
4. SYSTEM CONFIGURATION	11
4.1 FIRST SCREEN THAT OPENS.....	11
4.2 SYSTEM SETTINGS	12
4.3 SYSTEM RESOURCES.....	13
4.4 NVRAM SETTINGS	14
4.5 FIRMWARE UPGRADE (TFTP).....	15
4.6 FIRMWARE UPGRADE (HTTP)	16
4.7 REBOOT	16
4.8 LOAD BALANCER POLICY	17
4.8.1 VIRTUAL TRUNK BALANCING POLICY.....	17
4.9 IP CONFIGURATION	18
4.10 GATEWAY CONFIGURATION.....	18
4.11 SAVE CONFIGURATION.....	19
4.12 ERASE CONFIGURATION.....	20
4.13 RESTORE SETTINGS.....	21
4.14 REMOTE RESTORE	22
4.15 TAG SETTINGS.....	22
4.16 DISPLAY CONFIGURATION	23
5. RMON CONFIGURATION.....	24
5.1 RMON BASICS	24
5.2 RMON ALARMS.....	24
5.3 RMON ETHERNET STATISTICS.....	25
5.4 RMON EVENT	25
5.5 RMON EVENT LOGS.....	26
5.6 RMON HISTORY	26
6. USER	27
6.1 USER CONFIGURATION.....	27
6.2 USER GROUP CONFIGURATION	27
6.3 USER CHANGE PASSWORD.....	28
7. TACACS.....	29
7.1 TACACS CONFIGURATION.....	29
7.2 TACACS SERVER CONFIGURATION	30
8. RADIUS.....	31
8.1 RADIUS CONFIGURATION	31

9.	SYSLOG	32
9.1	SYSLOG LOGGING	32
9.2	SYSLOG FORWARD.....	33
9.3	SYSLOG DISPLAY LOG.....	34
10.	SNMP	34
10.1	SNMP COMMUNITY.....	34
10.2	SNMP GROUP	35
10.3	SNMP GROUP ACCESS	37
10.4	SNMP VIEW	38
10.5	SNMP TARGET ADDRESS.....	39
10.6	SNMP TARGET PARAMETER	40
10.7	SNMP USER	41
10.8	SNMP TRAP MANAGER	43
10.9	SNMP FILTER CONFIGURATION	44
11.	SNTP	45
11.1	SNTP UNICAST	45
11.2	SNTP BROADCAST	46
11.3	SNTP MULTICAST	47
11.4	SNTP SCALARS	48
12.	STATISTICS.....	49
12.1	PORT STATISTICS.....	49
12.2	CLEAR PORT STATISTICS.....	50
12.3	RMON STATISTICS	50
12.4	TRAFFIC RATE STATISTICS.....	51
13.	INT10GXXXX-BPAC CONFIGURATION.....	52
12.1	CONFIGURATION MAPS.....	52
13.1.1	<i>New Configuration Map.....</i>	<i>53</i>
13.1.2	<i>Multiple Port Selection.....</i>	<i>54</i>
13.1.3	<i>Graph.....</i>	<i>54</i>
13.1.4	<i>Port/Filter Statistics.....</i>	<i>55</i>
13.1.5	<i>Ports.....</i>	<i>56</i>
13.1.6	<i>Egress Filters.....</i>	<i>57</i>
13.1.7	<i>Ports – Advanced Options.....</i>	<i>57</i>
13.2	PORT GROUPS	59
13.2.1	<i>New Port Groups.....</i>	<i>59</i>
13.3	FILTER TEMPLATES	60
13.4	FILTER TEMPLATES PAGE	61
13.5	NEW FILTER TEMPLATES.....	62
13.6	NEW FILTER TEMPLATE.....	62
13.7	ADVANCED	63

14.	BYPASS CONFIGURATION	64
14.1	BYPASS SEGMENTS.....	64
14.2	CONFIG MAP LIST.....	64
14.3	CONFIG MAPS.....	65
14.4	SEGMENT CONFIGURATION	66
14.5	SEGMENT PACKET FLOW	67
14.6	SEGMENT GENERAL SETTINGS	68
14.7	SEGMENT ADVANCED SETTINGS	69

Table of Figures

Figure 1: Login Screen	10
Figure 2: Opening Screen	11
Figure 3: System Information.....	12
Figure 4: System Resources	13
Figure 5: NVRAM Settings	14
Figure 6: Firmware Upgrade (tftp).....	15
Figure 7: Firmware Upgrade (http).....	16
Figure 8: Reboot	16
Figure 9: Load Balancer Policy	17
Figure 10: Virtual Trunk Balancing Policy	17
Figure 11: IPv4 Interface Settings.....	18
Figure 12: IP Gateway Configuration	18
Figure 13: Save Configuration	19
Figure 14: Erase Configuration.....	20
Figure 15: Restore Settings.....	21
Figure 16: Remote Restore	22
Figure 17: Tagging Mode.....	22
Figure 18: System Configuration.....	23
Figure 19: RMON Basics.....	24
Figure 20: RMON Alarms	24
Figure 21: RMON Ethernet Statistics	25
Figure 22: RMON Events	25
Figure 23: RMON Event Logs.....	26
Figure 24: RMON History	26
Figure 25: User Configuration.....	27
Figure 26: Group Configuration	27
Figure 27: Change Password	28
Figure 28: TACACS Configuration.....	29
Figure 29: TACACS Server Configuration.....	30

Figure 30: Radius Configuration	31
Figure 31: Syslog Logging.....	32
Figure 32: Syslog Forward Table.....	33
Figure 33: Syslog Display Log	34
Figure 34: SNMP Community	34
Figure 35: SNMP Group.....	35
Figure 36: SNMP Group Access.....	37
Figure 37: SNMP View	38
Figure 38: SNMP Target Address.....	39
Figure 39: SNMP Target Parameter	40
Figure 40: SNMP User	41
Figure 41: SNMP Trap Manager.....	43
Figure 42: Filter Configuration	44
Figure 43: SNTP Unicast Table	45
Figure 44: SNTP Broadcast Configuration	46
Figure 45: SNTP Multicast Configuration	47
Figure 46: SNTP Scalars Configuration	48
Figure 47: Port statistics.....	49
Figure 48: RMON Statistics	50
Figure 49: Traffic Rate Statistics.....	51
Figure 50: Configuration Maps	52
Figure 51: Configuration Maps	53
Figure 52: Multiple Port Selection	54
Figure 53: Port/Filter Statistics.....	55
Figure 54: Ports	56
Figure 55: Egress Filters	57
Figure 56: Advanced Options	57
Figure 57: CRC Load Balancing Policy.....	58
Figure 58: Port SFP Information	58
Figure 59: Port Groups.....	59

Figure 60: New Ports Group	59
Figure 61: Filter Templates Page.....	61
Figure 62: New Filter Template (General Tab)	62
Figure 63: New Filter Criteria (Filter Criteria Tab).....	62
Figure 64: Advanced	63
Figure 65: Bypass Segments	64
Figure 66: Config Map List	64
Figure 67: Config Map.....	65
Figure 68: Segment Configuration	66
Figure 69: Segment Packet Flow	67
Figure 70: Segment General Settings.....	68
Figure 71: Segment Advanced Settings.....	69

1. OVERVIEW

The EdgeLens INT10GXXXBPXXSFP Bypass System supports two very important features necessary to protect critical networks links. The EdgeLens can support in-line without any danger of losing the link in case of an appliance failure and has the ability of connecting the critical links to a variety of analysis and security tools to assure the integrity of even the most sensitive data.

The active bypass enables plug and play connectivity, includes an auto heartbeat and does not require additional drivers to be installed on connected appliances and provides seamless failover in the case of a software crash, link loss or hardware failure. The unit possesses management functionality that can be utilized via an extensive web GUI or CLI which enables flexibility and multiple configurations. The EdgeLens Bypass System has passive bypass support that provides an additional layer of protection in the case of a power failure, preserving network connectivity.

This documentation will serve as a guide to the devices Graphical User Interface (GUI). It will include the following features:

- System configurations
- RMON configurations
- User Configurations
- TACACS configurations
- Radius Configurations
- Syslog configurations
- SNMP configurations
- SNTP configurations
- Statistics
- FAB Configurations
- Bypass Configuration

2. SERIAL CONSOLE CONFIGURATION

The settings to connect to the Serial Console are the following.

Bits per second: 115200

Data bits: 8

Parity: None

Stop: 1

Flow Control: None

Users may login with user “root” and password “gtroot1”.

TITLE: INT10GXXXBP GRAPHICAL USER INTERFACE GUIDE	Garland Technology Confidential & Proprietary	REV: 2.0	PAGE 9 OF 70
---	---	----------	--------------

3. MANAGEMENT INTERFACE

3.1 Management Configuration

The default management, also known as `cpu0`, IP is 10.10.10.200. Users are able to configure the management IP on the CLI using following commands.

end

`configure terminal`

`interface cpu0`

`ip address { <ip_address> <subnet_mask> }`

Users can set the gateway IP address with the following commands.

end

`configure terminal`

`ip route 0.0.0.0 0.0.0.0 <gateway_ip>`

Accessing GUI

Users may access the GUI, through the latest Mozilla Firefox or Google Chrome with the following address.

http://<ip_address>

3.2 Login

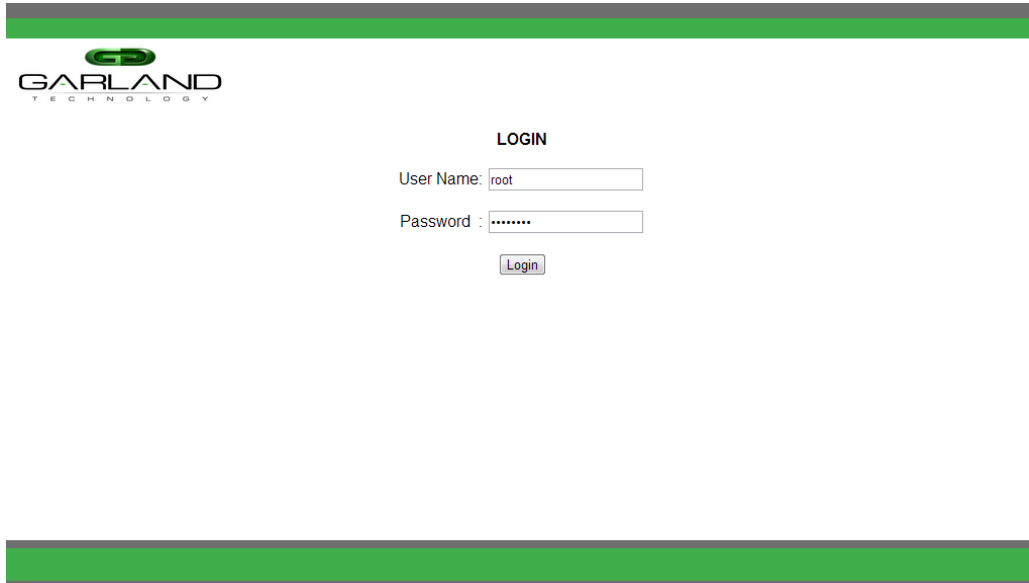


Figure 1: Login Screen

Users will be prompted with the login screen. Users can login with user '**root**' and password '**gtroot1**'.

4. SYSTEM CONFIGURATION

The settings under system configuration are globally applied to the unit. This is the place where users can configure the following.

System settings

NVRAM settings

Firmware Upgrade (tftp)

Firmware Upgrade (http)

Reboot

IP Configuration

Management IP

Gateway IP

Save, erase and restore configuration

Tagging settings

In Addition to this user guide, a help page is available for each individual page of the WEB UI. These help pages can be accessed by clicking the “help” button located at the top right of each configuration page of the WEB UI.

4.1 FIRST SCREEN THAT OPENS



Figure 2: Opening Screen

More information:

Users are able to create the configuration maps on this page; this will include load balancing, filtering, aggregation and mirroring.

Multiple configuration maps can be made on the system. Users will have the capability to disable or enable each configuration map.

When multiple configuration maps are made, users can set the priority of each to determine which rule should be looked at first.

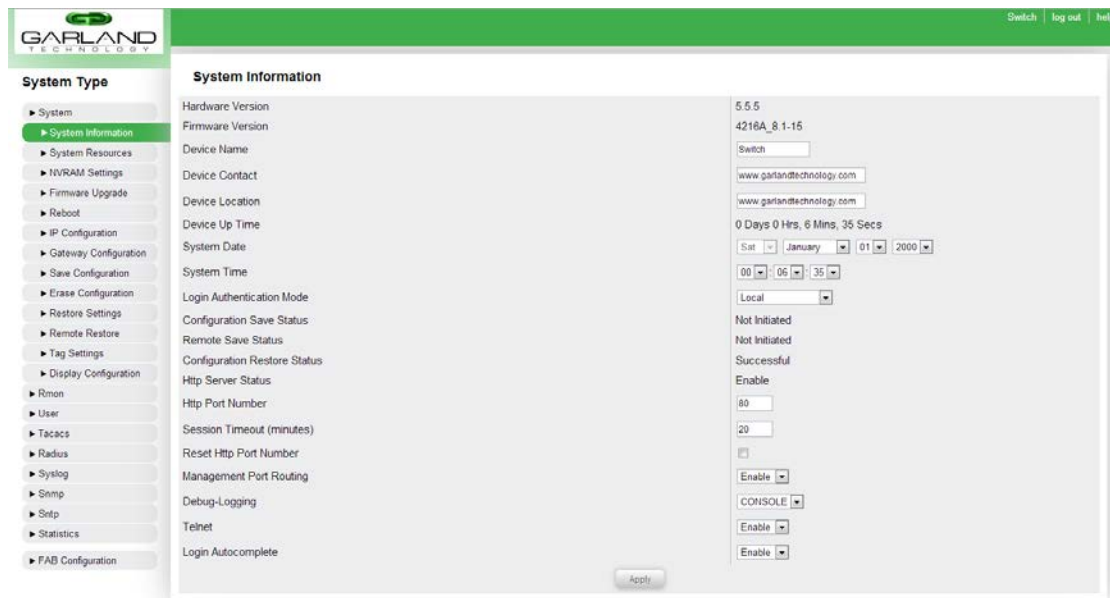
Garland Technology EdgeLens

The "Show All" option in the configuration maps interface will truncate and display all configuration maps on a single page. Users can edit a specific configuration map in this view by clicking on it.

1. This is the ports tab which updates what shows in section 4. A green colored bubble shows that a link has been established while a red colored bubble signifies that no link has been established.
2. This is the port groups tab which updates what shows in section 4. By default, it will be empty as there is no default port channels created.
3. This is the filter templates tab which updates what shows in section 4. Users can create filter templates and use them in the configuration map.
4. This area refreshes itself when tabs are changed between sections 1-3. Users can drag these icons to sections 6-8.
5. This section allows users to name and write a description for the configuration map without looking into detail.
6. Users can drag ports from section 4 when they are under the ports tab to this section. This will be the input port where traffic comes in.
7. Users can drag rules/filters from section 4 when they are under the filters tab to this section. This is the rule which will determine whether the type of traffic that is allowed to flow through to the output port or deny all traffic.
8. Users can drag ports and port groups from section 4 when they are under the ports or groups tab. This will be the output port(s).*

*If no port groups are created and user wishes to create a port group, users can drag ports on top of each other. A new window will pop up allowing the user to create a port group or virtual trunk for load balancing purposes.

4.2 SYSTEM SETTINGS



The screenshot displays the 'System Information' configuration page in the Garland Technology EdgeLens interface. The left sidebar contains a 'System Type' menu with options like System, System Information (selected), System Resources, INVRAM Settings, Firmware Upgrade, Reboot, IP Configuration, Gateway Configuration, Save Configuration, Erase Configuration, Restore Settings, Remote Restore, Tag Settings, Display Configuration, Rmon, User, Tacacs, Radius, Syslog, Snmp, Setp, Statistics, and FAB Configuration. The main content area is titled 'System Information' and includes the following fields and settings:

- Hardware Version: 5.5.5
- Firmware Version: 4218A_8.1-15
- Device Name: Switch
- Device Contact: www.garlandtechnology.com
- Device Location: www.garlandtechnology.com
- Device Up Time: 0 Days 0 Hrs, 6 Mins, 35 Secs
- System Date: Sat January 01 2000
- System Time: 00:06:35
- Login Authentication Mode: Local
- Configuration Save Status: Not Initiated
- Remote Save Status: Not Initiated
- Configuration Restore Status: Successful
- Http Server Status: Enable
- Http Port Number: 80
- Session Timeout (minutes): 20
- Reset Http Port Number: []
- Management Port Routing: Enable
- Debug-Logging: CONSOLE
- Telnet: Enable
- Login Autocomplete: Enable

An 'Apply' button is located at the bottom right of the configuration area.

Figure 3: System Information

Users can view and set the device information such as the switch name, contact and location as well as setting the date and time. They can change database to authenticate users from the locally defined users in the system to a remote authentication tool such as TACACS. Users can change the http port number, management port routing, debug-logging, and commit items.

4.3 SYSTEM RESOURCES

The screenshot shows the 'System Resources' configuration page in the Garland EdgeLens interface. The sidebar on the left lists various system configuration options, with 'System Resources' currently selected. The main area displays a table of system resources with their current and maximum usage percentages, and power supply status.

System Resource	Current Value	Maximum Value
Maximum CPU Usage(%)	100	100
Current CPU Usage(%)	2	100
Maximum RAM Usage(%)	100	100
Current RAM Usage(%)	44	100
Max Flash Usage(%)	100	100
Current Flash Usage(%)	36	100
Power Supply Unit 0	ON	ON/OFF
Power Supply Unit 1	OFF	ON/OFF

Buttons: Apply, Refresh

Figure 4: System Resources

Users can view the current hardware status of various hardware from this page as well as set the maximum usage limits for the hardware.

Maximum CPU Usage (%): This field allows the user to specify the maximum amount of CPU power the device is allowed to use. This option should not be modified except for debugging purposes.

Current CPU Usage (%): This field displays the current CPU usage of the device. This field cannot be modified.

Maximum RAM Usage (%): This field allows the user to specify the maximum amount of volatile memory the device is allowed to use. This option should not be modified except for debugging purposes.

Current RAM Usage (%): This field displays the current RAM usage of the device. This field cannot be modified.

Max Flash Usage (%): This field allows the user to specify the maximum amount of non-volatile memory the device is allowed to use. This option should not be modified except for debugging purposes.

Current Flash Usage (%): This field displays the current flash memory usage of the device. This field cannot be modified.

Power Supply Unit 0: This field displays the status of the first power supply of the device. This field cannot be modified.

Power Supply Unit 1: This field displays the status of the second power supply of the device. This field cannot be modified.

4.4 NVRAM SETTINGS

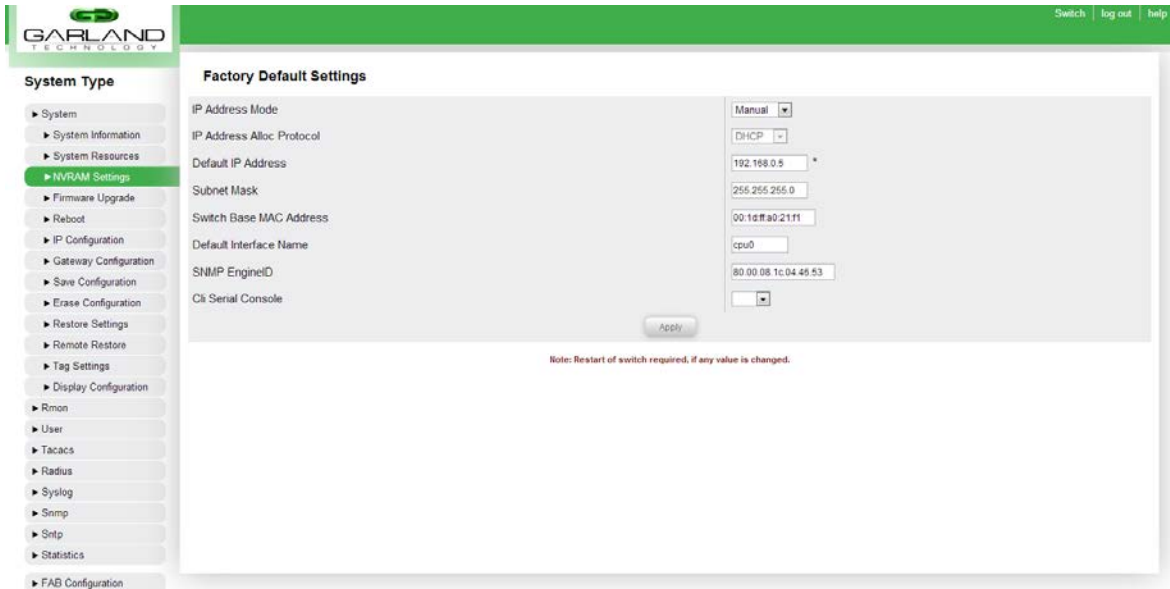


Figure 5: NVRAM Settings

The NVRAM settings page allows user to configure a default IP address. If users did not save the IP address configured under "IP Configuration", the unit will be configured with IP address based on this setting. Since specifying gateway in NVRAM is not applicable, it is recommended to configure IP address using IP configuration and gateway using Gateway configuration page.

Note: Settings from the "IP Configuration" page will take precedence over settings configured in "NVRAM Settings".

IP Address Mode: This drop-down list allows the user to select whether the management port will have a static (manual) IP address or a dynamic IP address.

IP Address Alloc Protocol: This drop-down list allows the user to select the allocation protocol used when the "IP Address Mode" field is set to "Dynamic". The options in this list are as follows:

1. **-RARP:** If the IP address allocation protocol used on the network is "Reverse Address Resolution Protocol", select this option.
2. **-DHCP:** If the IP address allocation protocol used on the network is "Dynamic Host Configuration Protocol", select this option.
3. **-BOOTP:** If the IP address allocation protocol used on the network is "Bootstrap Protocol", select this option.

Default IP Address: This field allows the user to specify the default IP address of the management port. If the "IP Address Mode" field is set to "Manual", the device will use the IP address specified in this field.

Subnet Mask: This field allows the user to specify the subnet mask of the management port. If the "IP Address Mode" field is set to "Manual", the device will use the subnet mask specified in this field.

Switch Base MAC Address: This field displays the base MAC address of the device used for the management port as well as the data ports. This field cannot be modified.

Default Interface Name: This field displays the default name of the management port interface. This field cannot be modified.

SNMP EngineID: This field allows the user to set the SNMP EngineID of the device. The EngineID is used when SNMPv3 functionality is enabled on the device to uniquely identify the agent in the device. This option should not be modified except for debugging purposes.

CLI Serial Console: This option allows the user to enable or disable the CLI serial console. The CLI should only be disabled for debugging purposes.

4.5 FIRMWARE UPGRADE (TFTP)

Figure 6: Firmware Upgrade (tftp)

Users will need to specify a server IP address with the firmware to upgrade the unit. The firmware should be placed in tftp server folder. After clicking apply, please wait few minutes for image download to be successful.

TFTP:

Upgrade From: This drop-down list allows the user to select the source of the firmware upgrade. Currently, the only option present is "TFTP".

Address Type: This drop-down list allows the user to select the address type of the TFTP server. Currently, the only option present is "IPv4".

Server IP Address: This field allows the user to specify the IP address of the TFTP server where the firmware file is located.

Firmware Name: This field allows the user to specify the name of the firmware located on the TFTP server from where the firmware will be upgraded. The filename must be in the format of "vmlinux.64_rXXXX_XXXX_*.gz".

After the "Server IP Address" and "Firmware Name" fields are specified, the user may click the "Submit" button to initiate the firmware upgrade. After the firmware upgrade is completed, the page will display the result of the upgrade. After the firmware upgrade is completed, it is necessary to reboot the device for the changes to take effect.

4.6 FIRMWARE UPGRADE (HTTP)

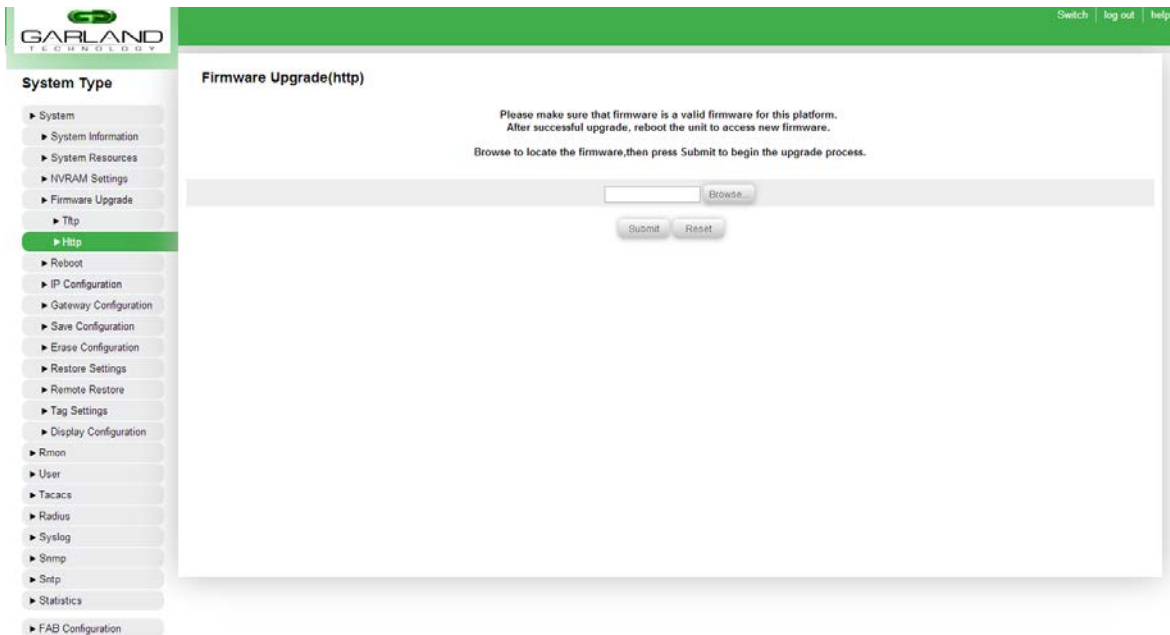


Figure 7: Firmware Upgrade (http)

HTTP:

To perform a firmware upgrade via HTTP, the user must click the **"Choose File"** button from the Http Firmware Upgrade page. The firmware file must be present on the host where the web UI is being accessed from. After clicking the **"Choose File"** button, the user will be able to navigate and choose the correct firmware file. The filename must be in the format of "vmlinux.64_rXXXX_XXXX_*.gz". After the firmware upgrade is completed, it is necessary to reboot the device for the changes to take effect.

4.7 REBOOT

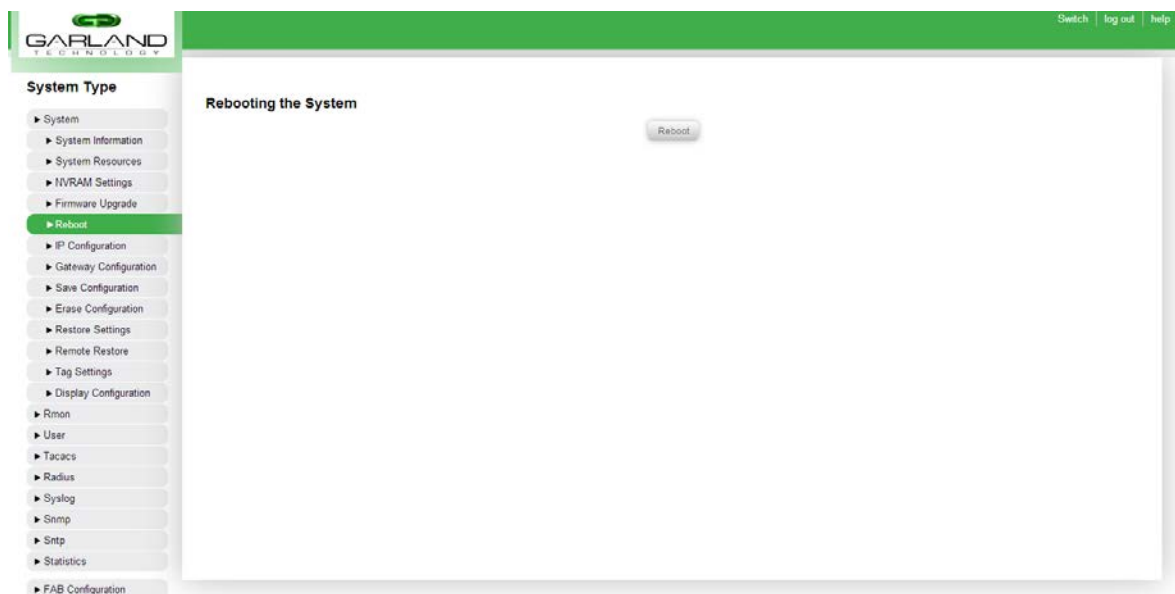


Figure 8: Reboot

The system can be soft rebooted through this page. Users can reconnect in 1-2 minutes.

Users may initiate a soft reboot of the device from this page. Clicking the "Reboot" button will prompt the user to reboot. Upon confirmation by the user, the device will reboot.

4.8 LOAD BALANCER POLICY

The screenshot shows the 'LA Load Balancing Policy' configuration page. On the left is a 'System Type' sidebar with a tree view including System, Rmon, User, Tacacs, Radius, Syslog, Snmp, Sntp, Statistics, FAB Configuration, Ports, Port Groups, Filter Templates, Load Balancer Policy (highlighted), Show All Configurations, and Configuration Maps. The main area is titled 'LA Load Balancing Policy' and contains a table with columns: Select, Hash Index Type, and Selection Policy. The table has three rows: 'XOR Based' (selected), 'CRC Based', and 'CRC-16 Based'. The 'XOR Based' row shows a list of selection criteria: MAC Source, MAC Destination, IP Source, Byte0-Byte2, Byte1-Byte3, IP Destination, Byte0-Byte2, and Byte1-Byte3. The 'CRC Based' and 'CRC-16 Based' rows have a text input field labeled 'Enter the seed value'. A 'Apply' button is at the bottom right of the table.

Select	Hash Index Type	Selection Policy
<input checked="" type="radio"/>	XOR Based	<input checked="" type="checkbox"/> MAC Source <input checked="" type="checkbox"/> MAC Destination <input checked="" type="checkbox"/> IP Source <input checked="" type="checkbox"/> Byte0-Byte2 <input checked="" type="checkbox"/> Byte1-Byte3 <input checked="" type="checkbox"/> IP Destination <input checked="" type="checkbox"/> Byte0-Byte2 <input checked="" type="checkbox"/> Byte1-Byte3
<input type="radio"/>	CRC Based	Enter the seed value
<input type="radio"/>	CRC-16 Based	Enter the seed value

Figure 9: Load Balancer Policy

The load balancing parameters will only be available once a port group has been created. Once created, users can apply one or any combination of the available options. Configuring the load balancing policy is global for the whole device.

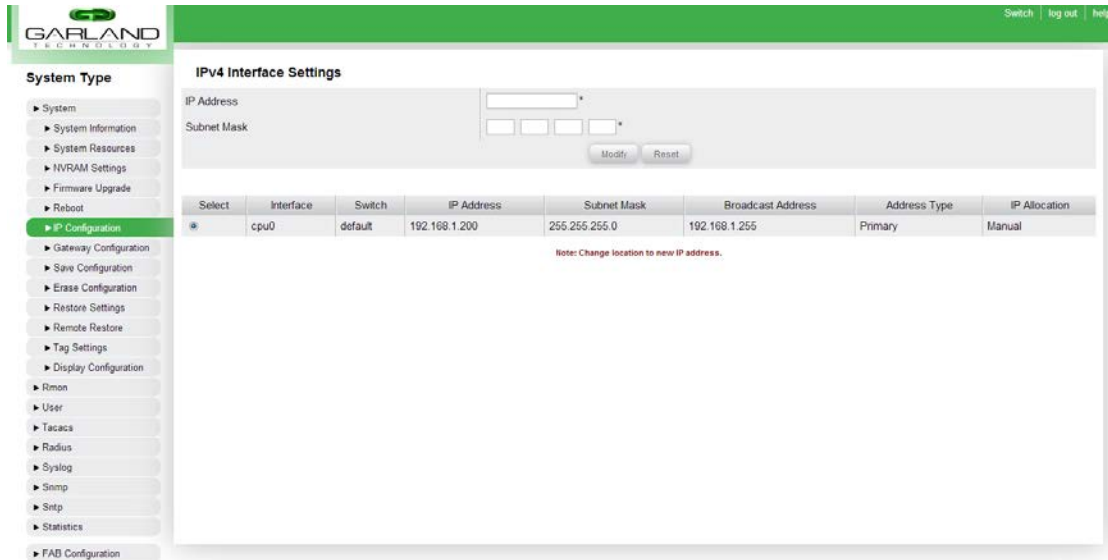
4.8.1 VIRTUAL TRUNK BALANCING POLICY

The screenshot shows the 'Port Group Properties » New Port Group' dialog box. It has two tabs: 'General' and 'Privilege'. The 'General' tab is active. It contains a 'Type' dropdown menu set to 'Virtual Trunk' and a 'Value' dropdown menu set to 'Source-IP'. Below these are 'Advanced Options' with four checkboxes: 'Byte 0', 'Byte 1', 'Byte 2', and 'Byte 3', all of which are currently unchecked. 'Cancel' and 'Save' buttons are at the top right.

Figure 10: Virtual Trunk Balancing Policy

When creating a virtual trunk by dragging and dropping ports in the Configuration Maps interface, the balancing policy is set individually for each virtual trunk during its creation process.

4.9 IP CONFIGURATION



IPv4 Interface Settings

IP Address:
 Subnet Mask:

Select	Interface	Switch	IP Address	Subnet Mask	Broadcast Address	Address Type	IP Allocation
<input checked="" type="radio"/>	cpu0	default	192.168.1.200	255.255.255.0	192.168.1.255	Primary	Manual

Note: Change location to new IP address.

Figure 11: IPv4 Interface Settings

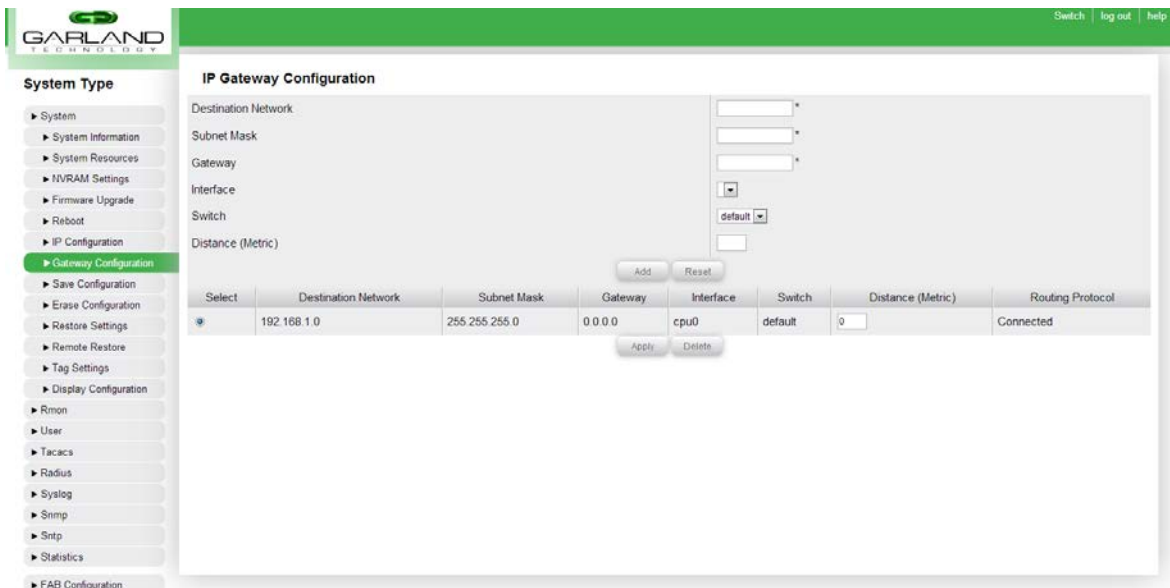
Note: Settings from the "IP Configuration" page will take precedence over settings configured in "NVRAM Settings".

IP Address: This field allows the user to specify a static IP address for the management port.

Subnet Mask: This field allows the user to specify the subnet mask for the management port.

The table shown at the bottom of the page shows the current settings of the management port.

4.10 GATEWAY CONFIGURATION



IP Gateway Configuration

Destination Network:
 Subnet Mask:
 Gateway:
 Interface:
 Switch:
 Distance (Metric):

Select	Destination Network	Subnet Mask	Gateway	Interface	Switch	Distance (Metric)	Routing Protocol
<input checked="" type="radio"/>	192.168.1.0	255.255.255.0	0.0.0.0	cpu0	default	0	Connected

Figure 12: IP Gateway Configuration

Configuring the gateway for the management port is made in this page.

Destination Network: This field allows the user to set a destination network for the gateway address specified above.

Subnet Mask: This field allows the user to set the subnet mask of the destination network specified in the "Destination Network" field above.

Gateway: This field allows the user to set the gateway address to be used to route traffic to the network specified in the "Destination Network" field above.

Interface: This field is not applicable on this platform.

Switch: This field is not applicable on this platform.

Distance (Metric): This field allows the user to specify the number of hops between the device and the gateway address specified in the "Gateway" field above. This field is optional.

Users are able to view a table on this page containing the current routing entries on the device. Users may modify the "Distance (Metric)" field of an existing routing entry in the table by changing the desired value and clicking the "Apply" button. Users may also delete specific route entries by selecting the radio button in the left-most column of the table and selecting the "Delete" button.

Note: Only static routes can be deleted or modified

4.11 SAVE CONFIGURATION

Figure 13: Save Configuration

The unit's configuration can be saved onto the flash or saved remotely to a host.

Save option: Users can select whether they would like to save the current configuration to the device's non-volatile flash memory or to a remote TFTP server.

-Flash Save: Selecting this option will save the device's current configuration to the on-board flash memory. If this option is selected, the user may skip to the bottom of the page and click the "Apply" button to save the configuration to the flash.

-Remote Save: Selecting this option will allow the user to save the device's current configuration to a remote TFTP server. If this option is selected, the user must specify the IP address of the TFTP server where the configuration will be saved.

TITLE: INT10GXXXBP GRAPHICAL USER INTERFACE GUIDE	Garland Technology Confidential & Proprietary	REV: 2.0	PAGE 19 OF 70
---	---	----------	---------------

Garland Technology EdgeLens

Transfer Mode: Specifies the protocol to be used to copy the device's current configuration to a remote server. Currently, only TFTP is supported.

Address Type: Specifies whether the IP address specified in the "IP Address" field below is of type IPv4 or IPv6.

IP Address: Allows the user to specify the IP address of the remote server where the device's current configuration will be saved.

File Name: Allows the user to specify configuration's file name to be written to the remote server. This field does not require modification.

After every mandatory field is filled out, a user may click the "Apply" button to write the device's current configuration to the local flash memory or to a remote server, depending on the specified "Save option" above.

4.12 ERASE CONFIGURATION

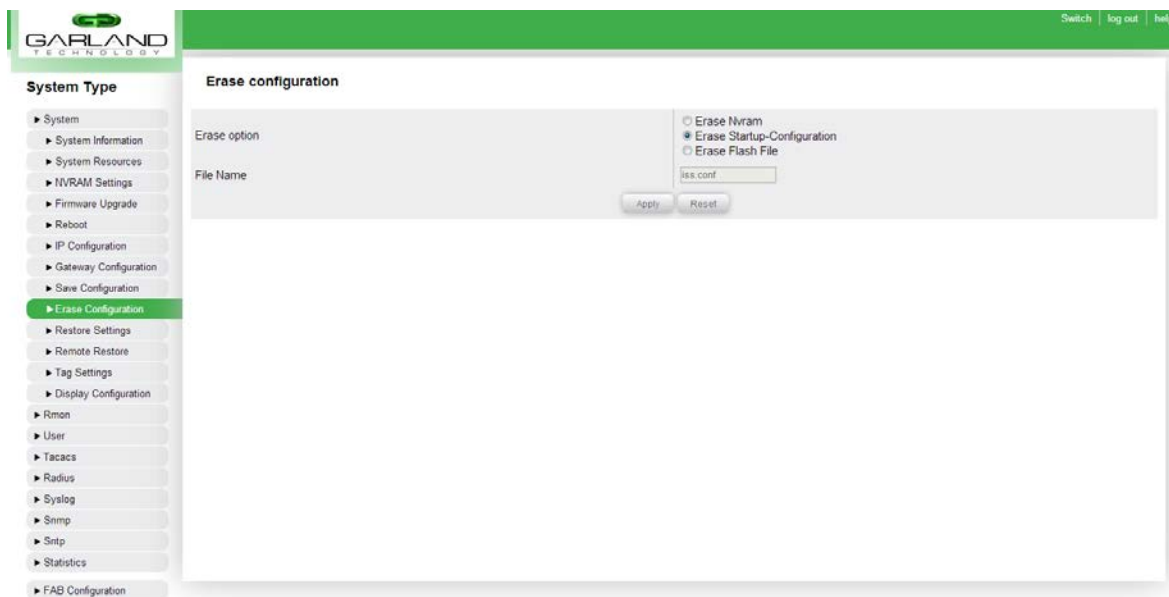


Figure 14: Erase Configuration

The unit's startup-configuration, NVRAM, and flash files can be erased through this page.

Erase option: This option allows the user to choose which configuration file they would like to erase. If "Erase Flash File" is chosen, a file name must be provided as well. By default, the file name is "switch.conf".

-Erase NVRAM: Selecting this option will reset the default settings of the device.

-Erase Startup-Configuration: Selecting this option will erase the existing startup-configuration that is written to the device's flash memory.

-Erase Flash File: Selecting this option will erase the flash file specified in the "File Name" text box below. By default, the file name is "switch.conf", which is the default startup-configuration file name.

-File Name: In this field, the user may specify the file name of the file to be erased. This field only becomes modifiable when the "Erase Flash File" option is chosen above. By default, the file name is "switch.conf", which is the default startup-configuration file name.

After specifying the desired erase option and file name (if "Erase Flash File" option was chosen), the user may click the "Apply" button to erase the specified file.

4.13 RESTORE SETTINGS

The screenshot displays the 'Restore configuration' page in the Garland Technology EdgeLens interface. On the left, a sidebar titled 'System Type' contains a list of configuration categories. The 'Restore Settings' category is currently selected and highlighted in green. The main panel, titled 'Restore configuration', contains two sections. The first section, 'Restore Option', features two radio button options: 'No Restore' and 'Flash Restore', with 'Flash Restore' being the selected option. The second section, 'File Name', includes a text input field that currently holds the value 'iss.conf'. At the bottom of this section are two buttons: 'Apply' and 'Reset'.

Figure 15: Restore Settings

The unit's configuration can be restored through the flash. Users will have the option to restore the configuration after reboot or not.

Restore Option: This option allows the user to choose whether the configuration file on the flash memory (if it exists) should be used in case the device is rebooted. If the configuration file is not present in the flash memory, and is instead present on a remote server, select the "Remote Restore" page. The user may pick one of the following options:

- No Restore: Users may select this option if they do not want the saved configuration to be restored upon boot.

- Flash Restore: Users may select this option if they would like to restore the saved configuration file present in the flash memory upon boot. Note: if this option is selected, the user must specify the file name of the configuration file in the "File Name" field below. The default specified file is "switch.conf".

- File Name: Users may specify the file name of the saved configuration file present in the flash memory. By default, this field is set to "switch.conf". This field is required only if the "Flash Restore" option is selected above.

After specifying the desired restore option and file name (if "Flash Restore" option was chosen), the user may click the "Apply" button to save the restoration preferences.

4.14 REMOTE RESTORE

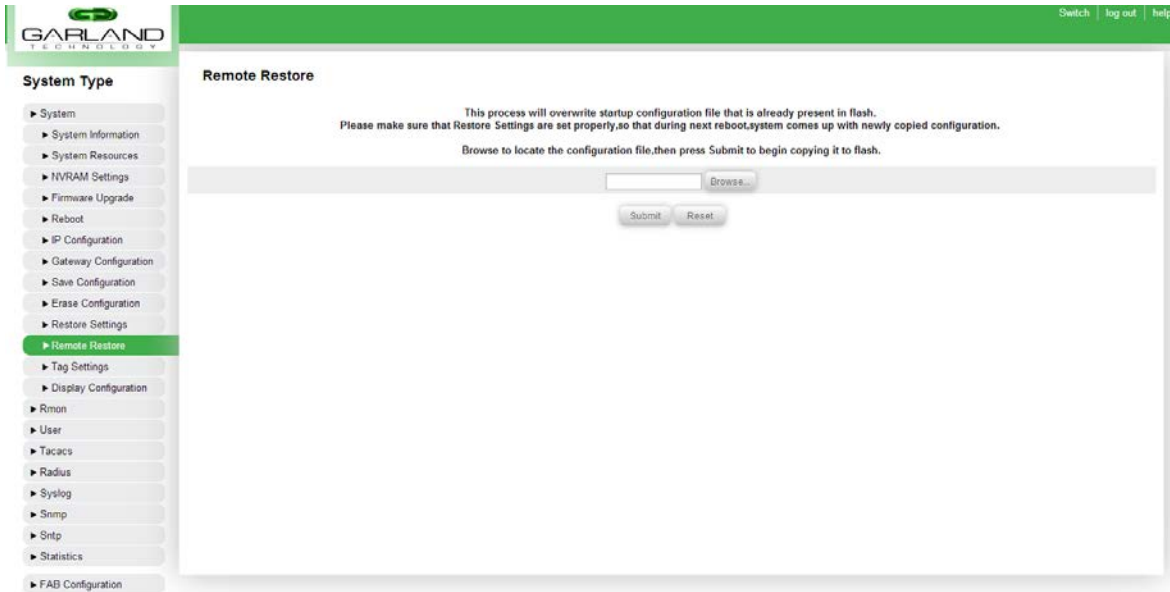


Figure 16: Remote Restore

If the configuration file is not present in the flash memory, and is instead present on the host from where the device is being accessed, the user may click the "Choose File" button to browse the contents of the host and select the desired configuration file.

After selecting the appropriate file, click on the "Submit" button to copy the configuration file from the host to the device's flash memory.

Note: this process will overwrite the current configuration file present in the unit's flash memory (if any).

4.15 TAG SETTINGS

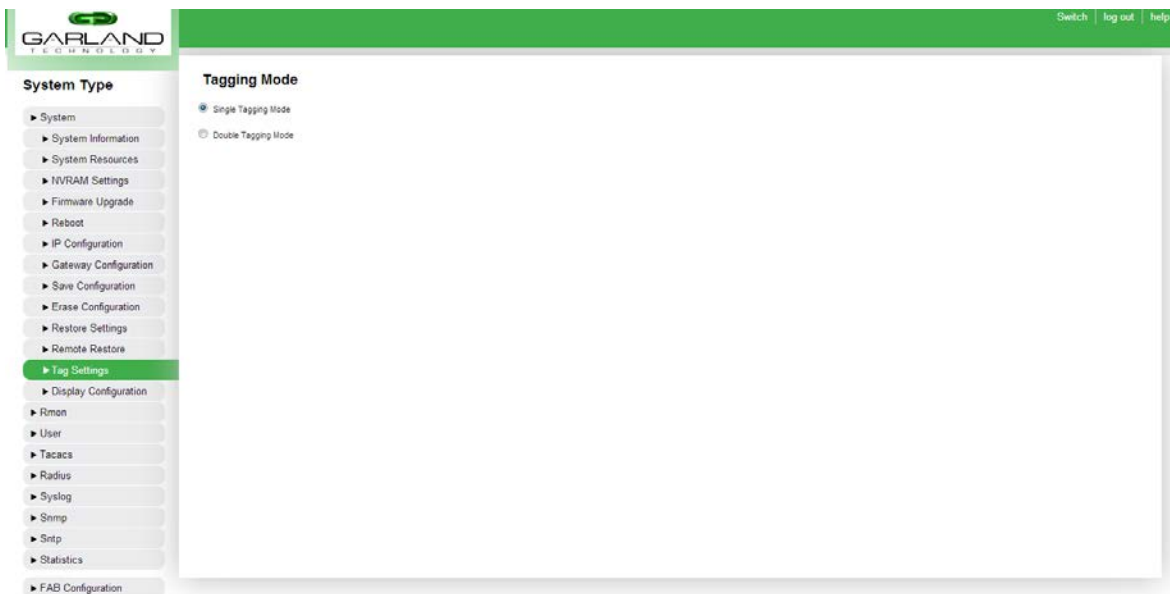


Figure 17: Tagging Mode

The unit can be configured to remove a single VLAN tag or two VLAN tags.

Single Tagging Mode: When this option is selected, any filters that use the "Strip vlan" advanced action (see screenshot above) will strip one VLAN tag per packet.

Double Tagging Mode: When this option is selected, any filters that use the "Strip vlan" advanced action will strip two VLAN tags per packet.

Note: There is no "Save" button on this page. Settings are automatically saved when an option is selected.

4.16 DISPLAY CONFIGURATION

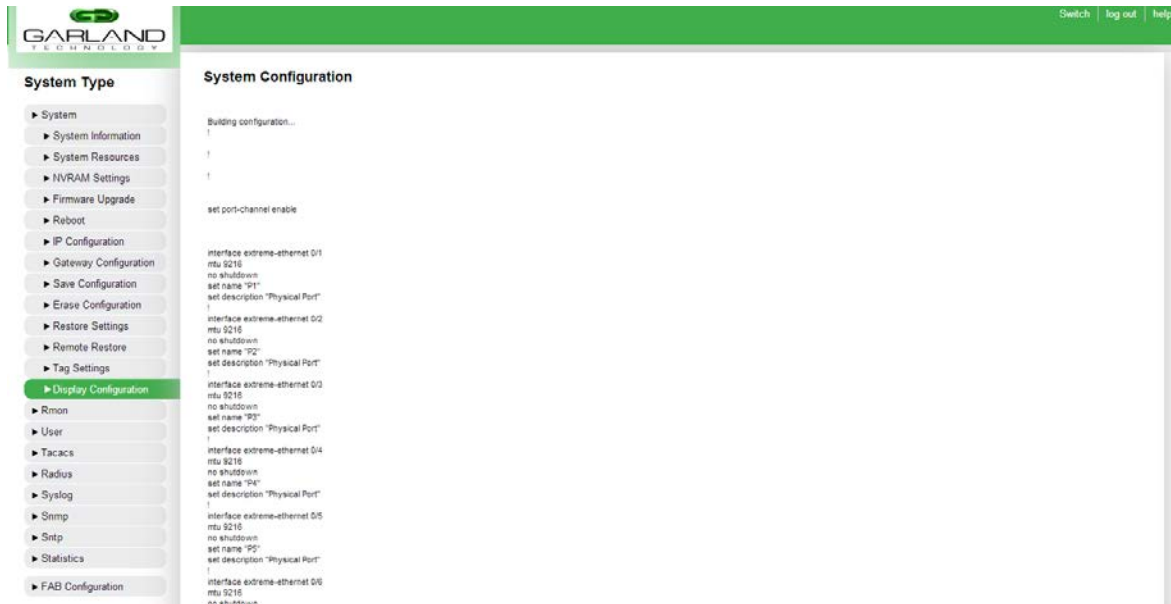


Figure 18: System Configuration

The entire running configuration is now viewable in the web GUI. This is equivalent to "show running-config" in the CLI.

Web GUI: System ---> Display Configuration

5. RMON CONFIGURATION

The unit supports Remote networking Monitoring (RMON). This section will guide users in the configuration of RMON.

5.1 RMON BASICS

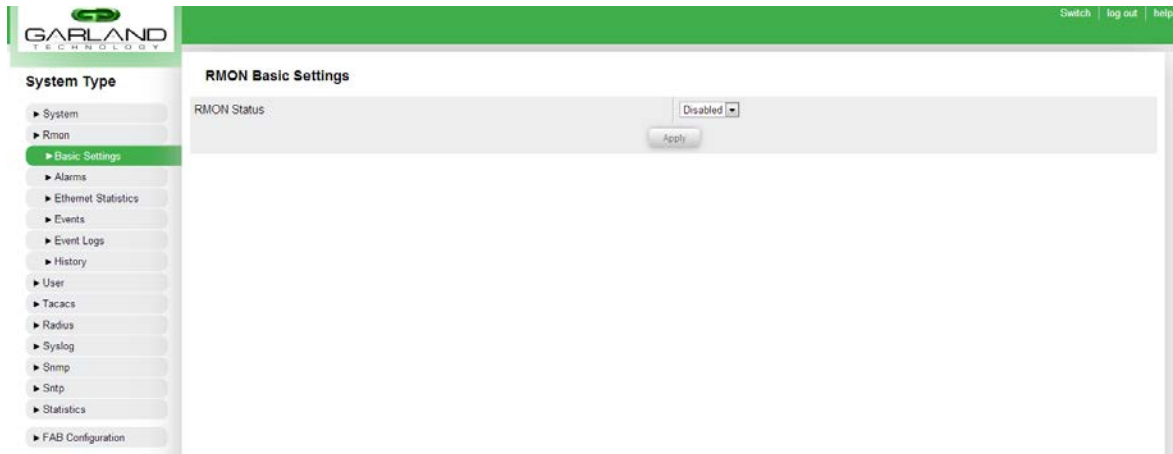


Figure 19: RMON Basics

Enabling and disabling RMON can be done through RMON basics page.

5.2 RMON ALARMS

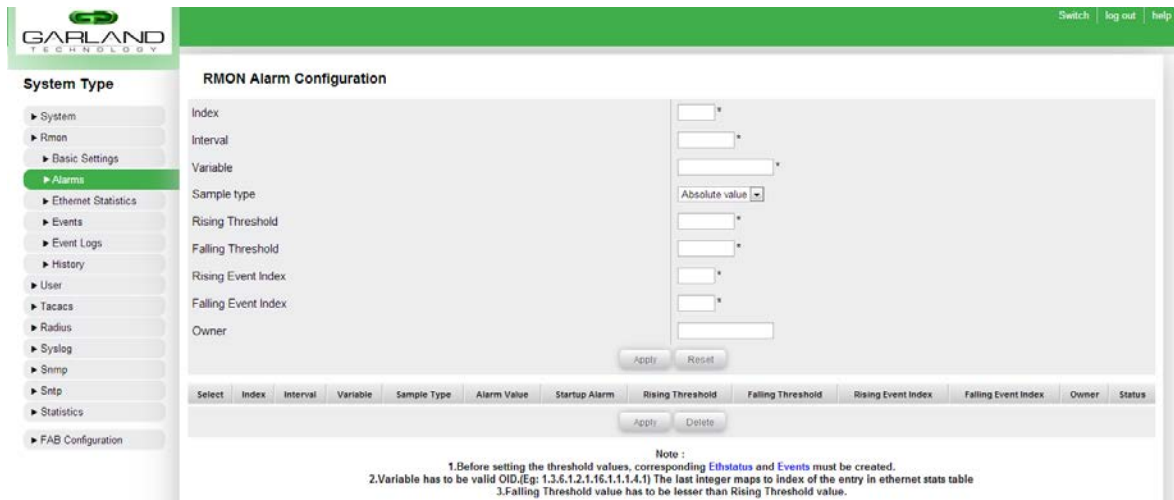


Figure 20: RMON Alarms

5.3 RMON Ethernet Statistics

The screenshot shows the 'Ethernet Statistics Configuration' page. On the left is a 'System Type' sidebar with a tree view containing: System, Rmon, Basic Settings, Alarms, Ethernet Statistics (highlighted), Events, Event Logs, History, User, Tacacs, Radius, Syslog, Snmp, Sntp, Statistics, and FAB Configuration. The main content area has a green header with 'Switch', 'log out', and 'help' links. Below the header, the 'Ethernet Statistics Configuration' section includes input fields for 'Index', 'Data Source', and 'Owner', with 'Add' and 'Reset' buttons. A table below these fields has columns: Select, Index, Data Source, Drop Events, Octets, Packets, Broadcast Packets, Multicast Packets, Owner, and Status. An 'Apply' button is centered below the table. A note at the bottom states: 'Note: Data Source has to be valid OID. To collect statistics for port 1, use 1.3.6.1.2.1.2.2.1.1.1 as the data source. The last integer value in data source represents the port number.'

Figure 21: RMON Ethernet Statistics

This page allows user to view the statistics of the RMON rules created.

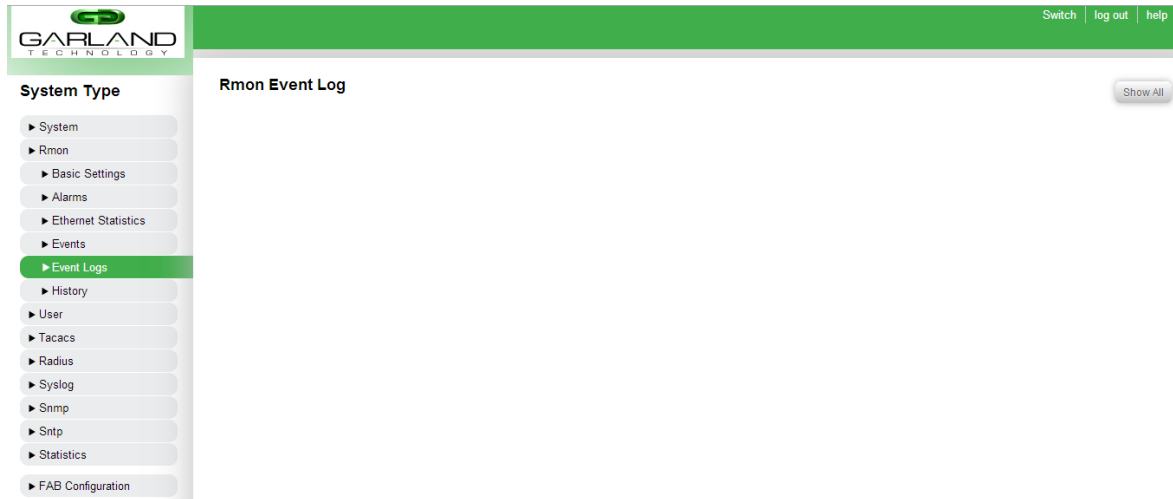
5.4 RMON Event

The screenshot shows the 'Event Configuration' page. It features the same 'System Type' sidebar as Figure 21, with 'Events' highlighted. The main content area has a green header with 'Switch', 'log out', and 'help' links. The 'Event Configuration' section includes input fields for 'Event Index', 'Description', 'Type' (a dropdown menu currently showing 'None'), 'Community', and 'Owner', with 'Add' and 'Reset' buttons. Below these fields is a table with columns: Select, Event Index, Description, Type, Community, Owner, Last Time Sent, and Status. 'Apply' and 'Delete' buttons are centered below the table.

Figure 22: RMON Events

This page allows the configuration of RMON events to be logged. The events include state changes, threshold, etc.

5.5 RMON Event Logs



Clicking the "Show All" button on this page will display the events that have been previously triggered via an RMON alarm.

Figure 23: RMON Event Logs

5.6 RMON History

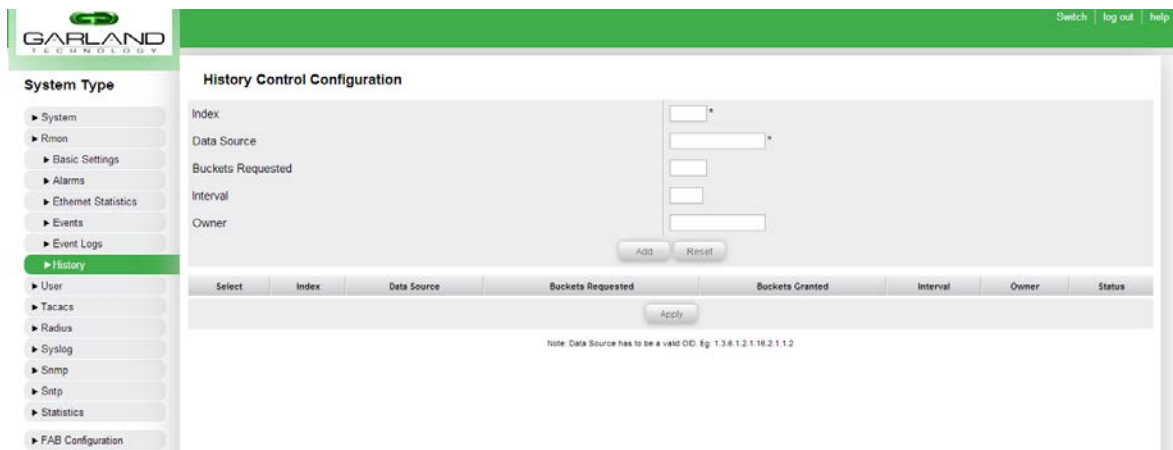


Figure 24: RMON History

Users can view the RMON history of the entries created on the system.

Index: Users must specify an index for the RMON History entry to be created.

Data Source: This field must be a valid OID. The device uses a standard OID scheme. For example: 1.3.6.1.2.1.16.2.1.1.2

Buckets Requested: This field specifies the time intervals in which to retrieve the RMON History for the entry to be created. Valid range is 1-65535.

Interval: Specifies the bucket interval in seconds. Valid range is 1-3600.

Owner: This field allows the user to specify the creator of the RMON History entry to be created.

After all required fields are entered, the user may click the "Add" button to add the entry into the RMON History table. After the entry is added, the user may modify portions of the entry by changing data in the relevant text fields and clicking the "Apply" button.

6. USER

User privilege policy defines the privilege for various users are allowed to access the objects in the FAB. The object can be configuration map, ports, port channel, filter template and system configuration

6.1 USER CONFIGURATION

Select	Username	Member Of
<input type="radio"/>	root	Administrator

Figure 25: User Configuration

New users may be created by entering the desired username and password and clicking the “Save” button. Note that users must also be assigned to a group to have their privilege level defined (it is inherited from the group privilege settings).

Administrators may modify the password of existing users by selecting the desired user from the existing list. Once the desired user is selected, the username will automatically be entered in the “Username” field and the new password may be entered in the “Password” and “Confirm Password” fields. Administrators may also delete custom users by selecting them from the list and selecting the “Delete” button. Note that the root user may not be deleted.

6.2 USER GROUP CONFIGURATION

Select	Group Name	Description	Member	Port Privilege
<input type="radio"/>	Administrator		root	P1(F) P2(F) P3(F) P4(F) P5(F) P6(F) P7(F) P8(F) P9(F) P10(F) P11(F) P12(F) P13(F) P14(F) P15(F) P16(F)

Figure 26: Group Configuration

Administrators may add/edit/remove custom user name groups from the ‘Groups Configuration Screen’. New groups are created by entering a “group Name” and an optional “Description”. Next, the default privileges of the group are defined. The group will be added when the “Save” button is pressed.

Garland Technology EdgeLens

Available privilege levels are as follows:

- **Access** – User with access privilege can view the object and use the object in group. If it is a port or filter, it can be used in the configuration map or port channel. Port channel and configuration map access privilege are inherited from ports and filters.
- **Modify** – User with modify privilege can access, modify and delete the object.
- **Full** – in addition to the modify privilege, user also can add and remove group privilege of the object.
- **None** – object will be inaccessible and unavailable to the user.

Users

A user is a member of at least one user group who can login to the FAB. A user can be a local user, TACACS+ user, or RADIUS user. A user can belong to one or more user groups. Users with full privilege may change owner, group, and group privilege for the object.

User Groups

A user group is for grouping users with same privilege or purpose together. A user group consists of the following properties:

1. Name
2. Description
3. Default Privilege for each object

The minimum privilege level required to view objects is “access”.

The minimum privilege level required to edit or create objects is “modify”.

Only users with “full” privileges may access an object's privilege tab.

Port groups and configuration maps will inherit their privilege from ports.

Special Groups

1. Administrator – has full privilege to all objects
2. Everyone/Other – all users/all other users

6.3 User Change Password

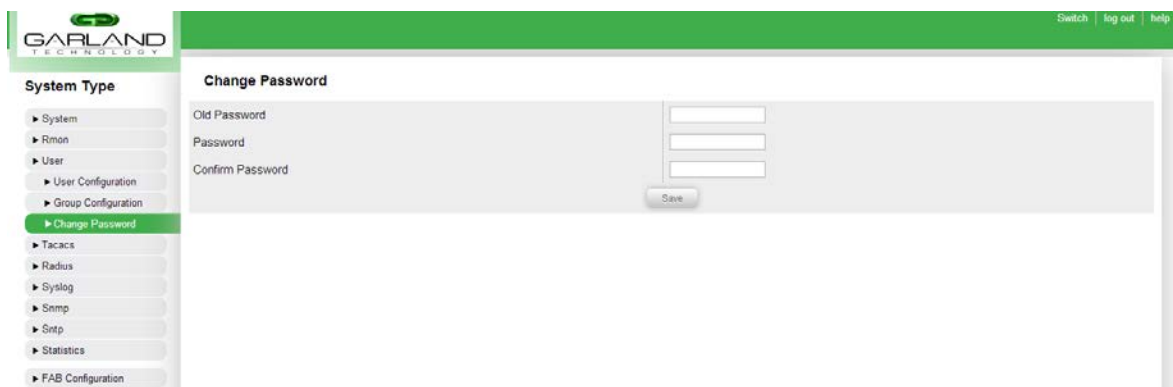


Figure 27: Change Password

Users may change the User Password of the current user on the Change Password Page.

7. TACACS

TACACS allows an external server to authenticate users to access the unit. The following will detail the configurations of TACACS on the GUI.

7.1 TACACS CONFIGURATION

Figure 28: TACACS Configuration

Users can configure the multiple TACACS server address, secret, port, and timeout. Important note: users must go to the System Information and change the Login Authentication Mode to TACACS to use this tool.

Server Address Type: Users may specify the address type of the TACACS server. Users may choose from IPv4 or IPv6 address types.

IP Address: Users may specify the IP address of the remote TACACS server to be used for authentication.

Shared Secret: Users may specify the shared secret of the TACACS server (if required).

Single Connection: Users may specify whether the the device and the remote TACACS server should use a single connection. When this option is set to "Yes", the device will maintain a constant connection to the TACACS server, avoiding the device opening and closing a TCP connection to the TACACS server every time it needs to communicate. Note: the remote TACACS server must support single connection mode in order for this setting to function.

Server Port: Users may specify the port number where the TACACS server is accessible.

Server Timeout: Users may specify the timeout period for communication between the TACACS server and the device. Units are in seconds.

After all required TACACS server fields have been entered, the user can click the "Add" button to add the server configuration to the existing list of TACACS servers. Users may also select an existing TACACS server from the table at the bottom of the page and click the "Delete" button to remove the chosen entry.

7.2 TACACS SERVER CONFIGURATION

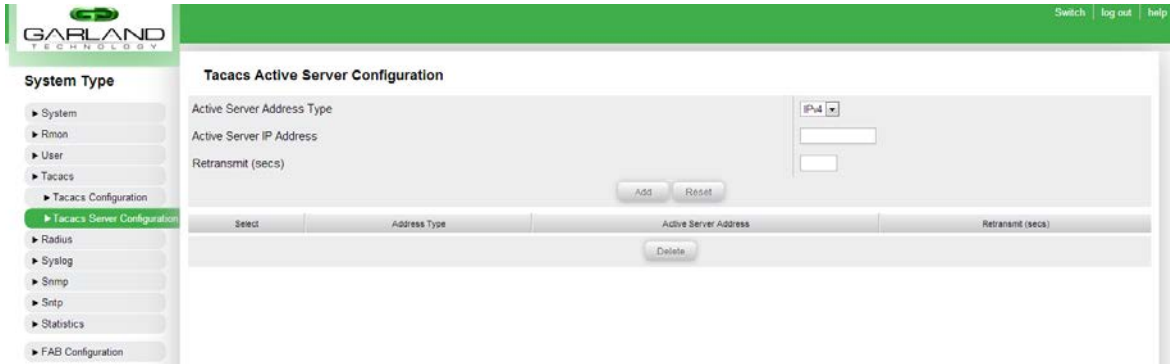


Figure 29: TACACS Server Configuration

Users may store multiple TACACS server onto the unit. Only one TACACS server may be active at a time.

Active Server Address Type: Users may select the address type of the active TACACS server entry to be added. Currently, only the IPv4 address type is supported.

Active Server IP Address: Users may specify the IP address of the remote TACACS authentication server in this field.

Retransmit: This field allows the user to specify how often the device will send an authentication request to the TACACS server if the server does not respond. Units are in seconds.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the TACACS active server configuration table at the bottom of this page.

The user may also select an active server configuration entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

8. RADIUS

8.1 RADIUS CONFIGURATION

Figure 30: Radius Configuration

Server Address Type: Users may specify the address type of the Radius server. Users may choose from IPv4 or IPv6 address types.

IP Address: Users may specify the IP address of the remote Radius server to be used for authentication or accounting.

Primary Server: Users may specify the Radius server as primary server.

Shared Secret: Users may specify the shared secret of the Radius server (if required).

Server Type: Users may specify whether the server for authentication or accounting or both.

Response Time: Users may specify the maximum response time for the Radius server. Units are in seconds.

Retry Count: Users may specify the maximum number of time to retry.

After all required Radius server fields have been entered, the user can click the "Add" button to add the server configuration to the existing list of Radius servers. Users may also select an existing Radius server from the table at the bottom of the page and click the "Delete" button to remove the chosen entry.

9. SYSLOG

9.1 SYSLOG LOGGING



The screenshot displays the 'Syslog Logging Settings' page. On the left, a 'System Type' menu lists various system components, with 'Syslog Logging' highlighted. The main content area contains the following settings:

- Number of Log Buffers:** A text input field containing the value '50'.
- Console Log:** A dropdown menu set to 'Enable'.
- Logging Facility:** A dropdown menu set to 'Local0(128)'.
- Logging Severity:** A dropdown menu set to 'Debug(7)'.
- Syslog Logging:** A section with an 'Enable' dropdown menu and a 'Clear' checkbox.

An 'Apply' button is located at the bottom right of the settings area.

Figure 31: Syslog Logging

Number of Log Buffers: This field specifies the number of syslog messages to be stored on the device's flash memory before the oldest entries become overwritten.

Console Log: This drop-down list specifies whether syslog messages will be output to the console.

Logging Facility: This field specifies which processes on the device should send the syslog messages. Options with higher values reflect higher priority messages.

Logging Severity: This field specifies which messages should be logged to the syslog daemon. Available options are as follows:

1. -Severity 0: Emergency Messages - Resource is unavailable.
2. -Severity 1: Alert Messages - Immediate action is needed.
3. -Severity 2: Critical Messages - Critical conditions.
4. -Severity 3: Error Messages - Error conditions.
5. -Severity 4: Warning Messages - Warning conditions.
6. -Severity 5: Notification Messages - Normal but significant conditions.
7. -Severity 6: Informational Messages - Informational messages only.
8. -Severity 7: Debugging Messages - Debugging messages only.

Logs: Users may select the "Clear" checkbox to clear the syslog messages currently stored on the device. To initiate the deletion process, the user must click the "Apply" button at the bottom of this page.

After setting the desired options on this page, the user may click the "Apply" button at the bottom of this page to apply the changes to the device.

9.2 SYSLOG FORWARD

Syslog Forward Table

Forward Priority:

Forward Address Type:

Server Ip Address:

Forward Port:

Forward Transition Type:

Add Reset

Select	Forward Priority	Forward Address Type	Server Ip Address	Forward Port	Forward TransType

Note :
1. Forward priority value is calculated by doing OR between Logging facility and Logging severity.
Ex: For severity debug(7) and facility local0(128) the forward priority is 135 (i.e. 128 | 7)

Figure 32: Syslog Forward Table

Forward Priority: This field allows the user to specify which syslog messages will be forwarded to the specified syslog server. The device will send a message to the syslog server if the priority of the message is greater than or equal to the forward priority specified in this field. The priority is calculated by doing an “OR” operation on the “Logging Facility” field and the “Logging Severity” field on the “Syslog Logging” page.

Forward Address Type: The user may select the address type of the syslog server where syslog messages will be sent to. Currently, the available option is IPv4.

Server IP Address: This field allows the user to specify the IP address of the syslog server where the syslog messages will be sent to.

Forward Port: This field allows the user to specify the port on which the syslog server will receive the incoming syslog messages.

Forward Transition Type: This field specifies the protocol in which the device will send messages to the syslog server. Currently, the UDP protocol is supported.

After the user enters values into the required fields on this page, the user may click the “Add” button to add the entered data into the Syslog forward table at the bottom of this page.

The user may also select a Syslog server entry from the table at the bottom of the page and click the “Delete” button to delete the specified entry from the table.

The user may also modify portions of existing syslog server entries in the syslog forward table at the bottom of the page. After desired changes have been made to the table, the user may click the “Apply” button at the bottom of the table to apply changes made.

9.3 **SYSLOG DISPLAY LOG**

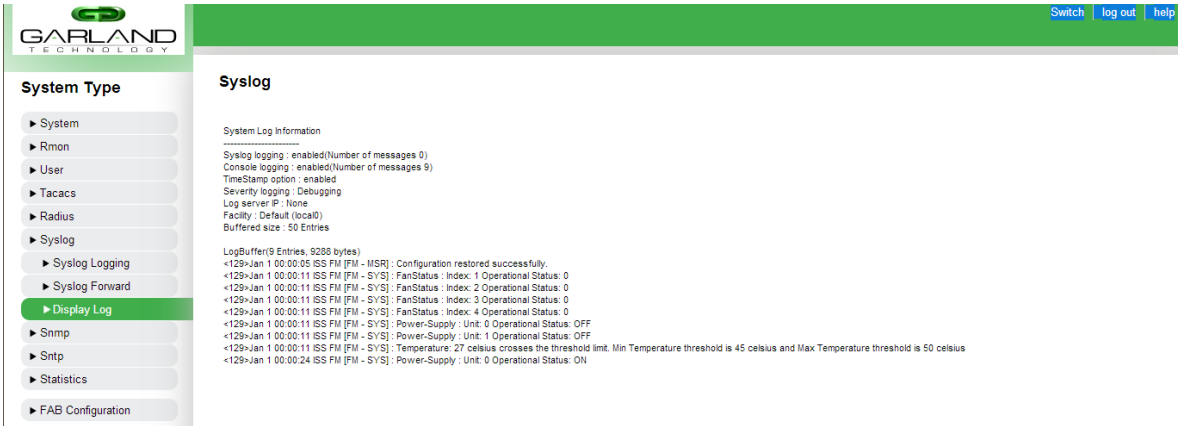


Figure 33: Syslog Display Log

10. SNMP

SNMP allows administrators to configure and extract information from the unit. The following will detail how to configure SNMP from the GUI.SNMP Community

10.1 SNMP COMMUNITY

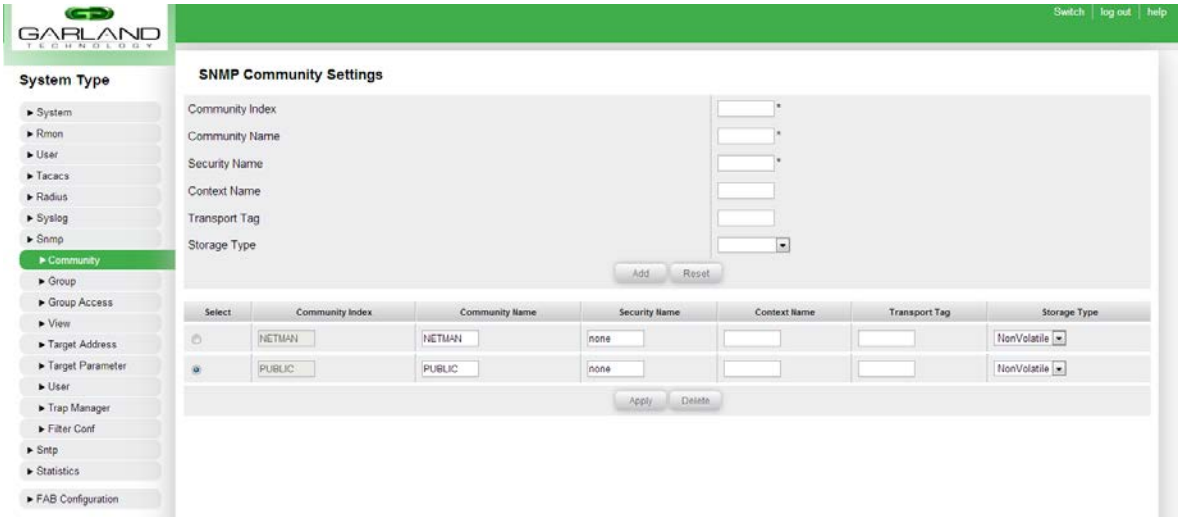


Figure 34: SNMP Community

The system has two default communities in place which should not be deleted. If users wish to add their own community, they may do so on this page.

Community Index: This field allows the user to set a name for the SNMP community to be added. This field accepts alphanumeric characters only, and must be unique for every community name entry.

Community Name: This field allows the user to set the name of the SNMP community to be used.

Security Name: This field allows the user to store the security model of the corresponding SNMP community name.

Context Name: This field is not applicable on this device.

Transport Tag: This field allows the user to specify the addresses of SNMP managers that are allowed use use this community name.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP community table at the bottom of this page.

The user may also select a SNMP community entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP community entries in the SNMP community table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.2 SNMP GROUP

The screenshot shows the 'SNMP GROUP Settings' page. On the left is a navigation menu with 'System Type' expanded, showing options like System, Rmon, User, Tacacs, Radius, Syslog, Snmp, Community, Group (selected), Group Access, View, Target Address, Target Parameter, User, Trap Manager, Filter Conf, Sntp, Statistics, and FAB Configuration. The main content area has fields for 'Security Model' (v1), 'Security Name' (empty), 'Group Name' (empty), and 'Storage Type' (NonVolatile). Below these are 'Add' and 'Reset' buttons. A table lists existing groups with columns: Select, Security Model, Security Name, Group Name, and Storage Type. The table contains five entries. At the bottom are 'Apply' and 'Delete' buttons.

Select	Security Model	Security Name	Group Name	Storage Type
<input type="radio"/>	v1	none	iso	NonVolatile
<input type="radio"/>	v2c	none	iso	NonVolatile
<input type="radio"/>	v3	initial	initial	NonVolatile
<input type="radio"/>	v3	templateIDr	initial	NonVolatile
<input checked="" type="radio"/>	v3	templateSHr	initial	NonVolatile

Figure 35: SNMP Group

Users can store multiple Groups using SNMPv1, SNMPv2c or SNMPv3.

Security Model: This drop-down list allows the user to specify the SNMP version to use. Available options are:

1. -v1
2. -v2c
3. -v3

Security Name: This field allows the user to specify the security name of the specified group entry to be added to the SNMP group table. For SNMPv1 and SNMPv2c, the security name is the "Community" name. For SNMPv3, the security name is the username.

Group Name: This field allows the user to specify the name of the SNMP group.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP group table at the bottom of this page.

The user may also select a SNMP group entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP group entries in the SNMP group table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.3 SNMP GROUP ACCESS

Figure 36: SNMP Group Access

Once the above has been defined, the unit can allow certain Groups to gain Access to the unit via SNMP.

Group Name: This field allows the user to specify the name of the group to be added to the SNMP group access table.

Security Model: This drop-down list allows the user to specify the SNMP version to use. Available options are:

1. -v1
2. -v2c
3. -v3

Security Level: This drop-down list allows the user to specify the security level for SNMPv3 managers. Available options are as follows:

Garland Technology EdgeLens

1. **-NoAuthentication:** This setting uses no authentication or encryption. It is the only available option for SNMPv1 and SNMPv2c, as both do not support any encryption or authentication protocols.
2. **-Authentication:** This setting allows the use of either SHA or MD5 based authentication for SNMPv3. This setting does not offer encryption of data.
3. **-Private:** This setting allows the use of either SHA or MD5 based authentication for SNMPv3. This setting uses encryption.

Read View: This setting allows the user to set the read view identifier for the SNMP group according to the "View Name" entry specified in the SNMP view page.

Write View: This setting allows the user to set the write view identifier for the SNMP group according to the "View Name" entry specified in the SNMP view page.

Notify View: This setting allows the user to set the notify view identifier for the SNMP group according to the "View Name" entry specified in the SNMP view page.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

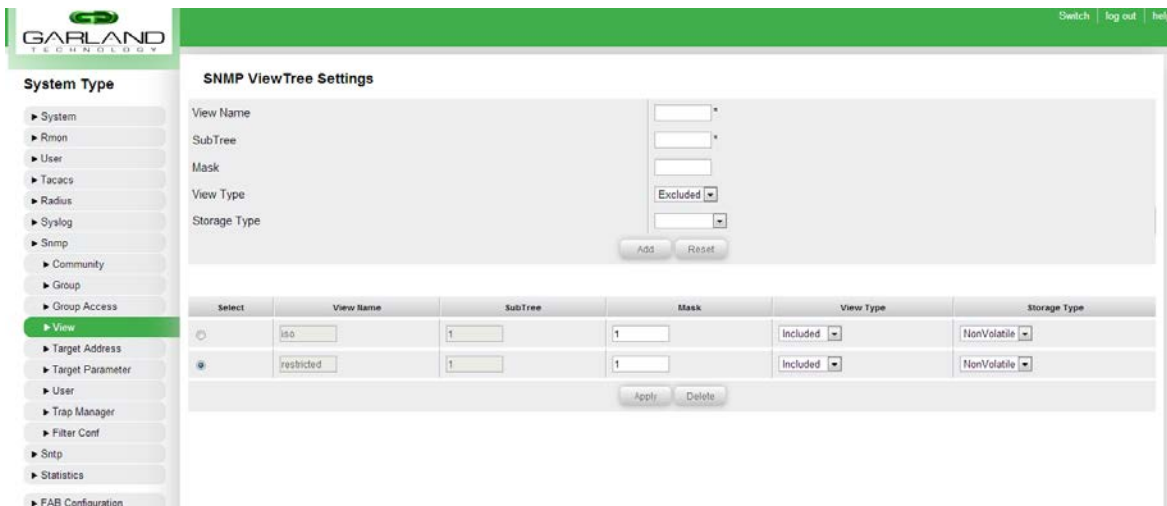
1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP group access table at the bottom of this page.

The user may also select a SNMP group access entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP group access entries in the SNMP group access table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.4 SNMP VIEW



SNMP ViewTree Settings

View Name:

SubTree:

Mask:

View Type:

Storage Type:

Select	View Name	SubTree	Mask	View Type	Storage Type
<input type="radio"/>	iso	1	1	Included	NonVolatile
<input checked="" type="radio"/>	restricted	1	1	Included	NonVolatile

Figure 37: SNMP View

Administrators are able to configure what information is viewable or restricted from various users.

Note: SNMP Group and SNMP Group Access settings must be configured prior to the SNMP View configuration.

View Name: This field allows the user to specify the name for which the view details are to be configured.

SubTree: This field allows the user to specify the Sub Tree value for the specified view.

Mask: This field allows the user to specify the mask value for the specified view. Using a mask allows only certain parts of an OID to be accessible to the user based on their access permissions.

View Type: This drop-down list allows the user to specify the view permissions of the specified Sub Tree. Available options are as follows:

1. **-Included:** This setting allows access to the specified Sub Tree.
2. **-Excluded:** This setting denies access to the specified Sub Tree.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP view table at the bottom of this page.

The user may also select a SNMP view entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP view entries in the SNMP view table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.5 SNMP TARGET ADDRESS

Figure 38: SNMP Target Address

SNMP Target Addresses can be stored here.

Note: A target parameter must be configured in the "SNMP Target Parameter" page before an SNMP target address entry can be created.

Target Name: This field allows the user to specify a unique identifier of the target.

Garland Technology EdgeLens

Target IP Address: This field allows the user to specify a target address to be used in the generation of SNMP operations.

Port: This field allows the user to specify the port of the SNMP manager located at the "Target IP Address" specified above.

Transport Tag: This field allows the user to specify the target address for a particular operation.

Param: This field allows the user to specify an SNMP parameter that has been previously specified in the "SNMP Target Parameter" page.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

-Volatile: This storage type is temporary. The configuration setting will be erased upon restarting the device.

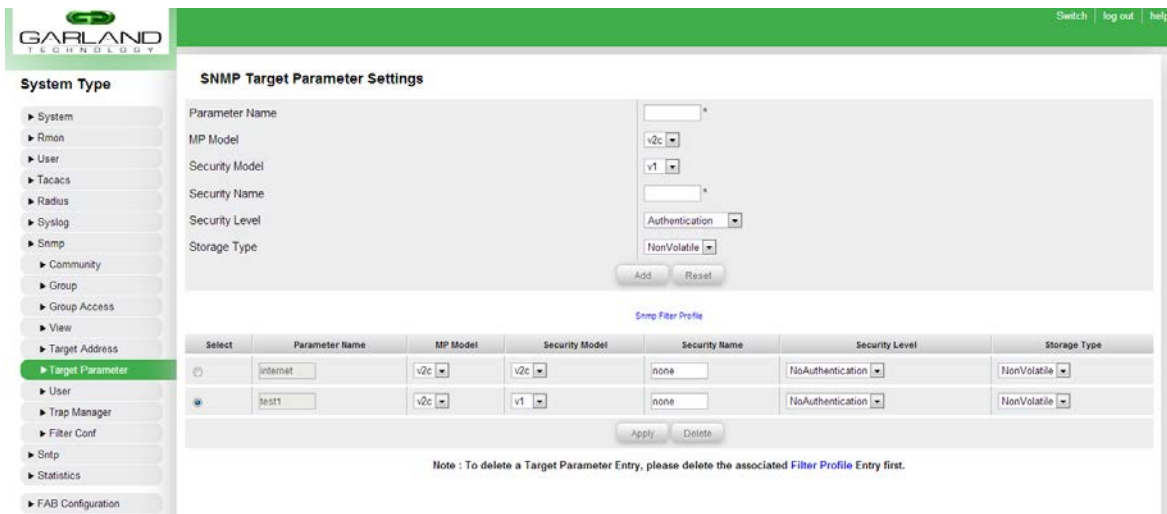
-NonVolatile: This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP target address table at the bottom of this page.

The user may also select a SNMP target address entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP target address entries in the SNMP target address table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.6 SNMP TARGET PARAMETER



SNMP Target Parameter Settings

Parameter Name:

MP Model:

Security Model:

Security Name:

Security Level:

Storage Type:

[Snmp Filter Profile](#)

Select	Parameter Name	MP Model	Security Model	Security Name	Security Level	Storage Type
<input type="radio"/>	internet	v2c	v2c	none	NoAuthentication	NonVolatile
<input checked="" type="radio"/>	test1	v2c	v1	none	NoAuthentication	NonVolatile

Note : To delete a Target Parameter Entry, please delete the associated Filter Profile Entry first.

Figure 39: SNMP Target Parameter

SNMP Target Parameters can be stored here.

Parameter Name: This field allows the user to specify a unique identifier of the parameter.

MP Model: This drop-down list allows the user to set the Message Processing model of the SNMP. Available options are as follows:

1. -v1
2. -v2c
3. -v3

Security Model: This drop-down list allows the user to set the version of the SNMP. Available options are as follows:

1. -v1
2. -v2c
3. -v3

Security Name: This field allows the user to specify the current parameter name, on whose behalf SNMP messages will be generated.

Security Level: This drop-down list allows the user to specify the security level for SNMPv3 managers. Available options are as follows:

1. **-NoAuthentication:** This setting uses no authentication or encryption. It is the only available option for SNMPv1 and SNMPv2c, as both do not support any encryption or authentication protocols.
2. **-Authentication:** This setting allows the use of either SHA or MD5 based authentication for SNMPv3. This setting does not offer encryption of data.
3. **-Private:** This setting allows the use of either SHA or MD5 based authentication for SNMPv3. This setting uses encryption.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP target parameter table at the bottom of this page.

The user may also select a SNMP target parameter entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP target parameter entries in the SNMP target parameter table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.7 SNMP USER

SNMP Security Settings

User Name:

Authentication Protocol:

Authentication Key:

Privacy Protocol:

Privacy Key:

Storage Type:

Select	Engine Id	User Name	Authentication Protocol	Private Protocol	Storage Type
<input checked="" type="radio"/>	80:00:08:1c:04:48:53	initial	No Authentication	No Privacy	NonVolatile
<input type="radio"/>	80:00:08:1c:04:48:53	templateMD5	HMAC-MD5	No Privacy	NonVolatile
<input type="radio"/>	80:00:08:1c:04:48:53	templateSHA	HMAC-SHA	DES	NonVolatile

Figure 40: SNMP User

Garland Technology EdgeLens

Note: Adding users is only supported in SNMPv3. SNMPv1 and SNMPv2c do not support user authentication.

SNMP Users can be created here along with the authentication protocol designated to each user.

User Name: This field allows the user to specify the user-based security model dependent security ID.

Authentication Protocol: This drop-down list allows the user to select the authentication protocol to be used. Available options are as follows:

1. **-No Authentication:** No authentication is used.
2. **-HMAC-MD5:** Message Digest 5 based authentication.
3. **-HMAC-SHA:** Security Hash Algorithm based authentication.

Authentication Key: This field allows the user to specify the secret authentication key to be used for messages sent on behalf of this user to/from the SNMP.

Privacy Protocol: This drop-down list allows the user to choose an encryption method. Available options are as follows:

1. **-No Privacy:** No encryption is used.
2. **-DES:** Data Encryption Standard protocol will be used for encryption.

Privacy Key: This field allows the user to indicate whether messages sent on behalf of a user to/from SNMP can be protected from disclosure.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP user table at the bottom of this page.

The user may also select a SNMP user entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP user entries in the SNMP user table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.8 SNMP TRAP MANAGER

Figure 41: SNMP Trap Manager

The unit can log and send SNMP traps for notification.

Notify Name: This field allows the user to specify a unique identifier associated with this entry.

Notify Tag: This field allows the user to specify the notification tag, which is used to select entries in the "Target Address" table.

Notify Type: This drop-down list allows the user to set the type of notification sent by the SNMP. Available options are:

1. **-Trap:** Traps do not provide confirmation of delivery to the SNMP manager and are only sent once. Traps take up less memory than informs.
2. **-Inform:** Informs provide confirmation upon receipt by the SNMP manager, and are retransmitted if the SNMP manager does not confirm receipt. Informs use more memory than traps.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

1. **-Volatile:** This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile:** This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP trap manager table at the bottom of this page.

The user may also select a SNMP trap manager entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP trap manager entries in the SNMP trap manager table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

10.9 SNMP FILTER CONFIGURATION

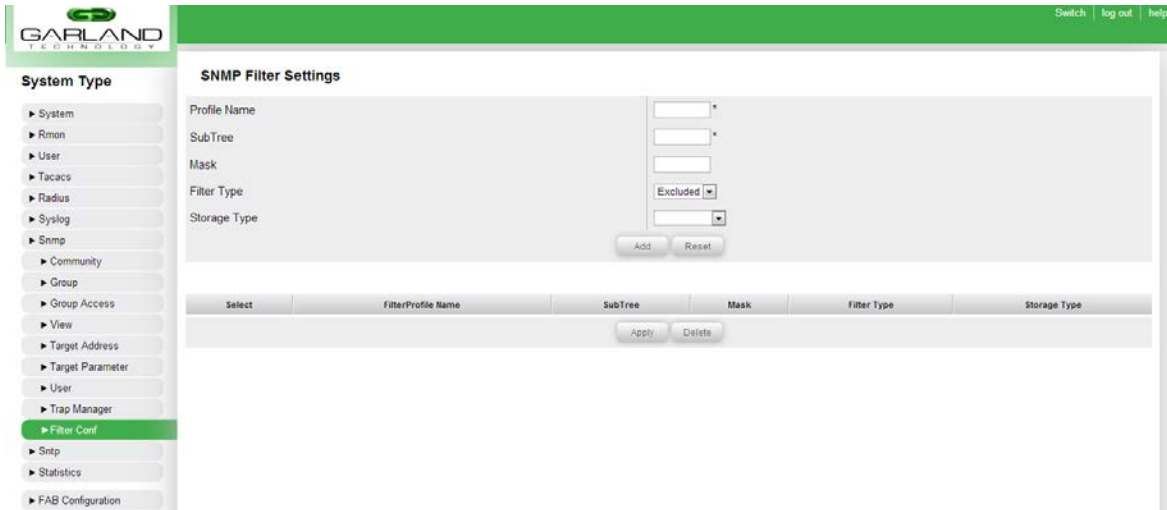


Figure 42: Filter Configuration

Users can set which traps to include or exclude in this page.

This page allows the user to configure filters for traps sent to the SNMP manager.

Profile Name: This field allows the user to specify the name for which the profile details are to be configured.

SubTree: This field allows the user to specify the Sub Tree value for the specified filter.

Mask: This field allows the user to specify the mask value for the specified filter.

Filter Type: This drop-down list allows the user to specify the filter permissions of the specified Sub Tree. Available options are as follows:

-Included: This setting allows access to the specified Sub Tree.

-Excluded: This setting denies access to the specified Sub Tree.

Storage Type: This drop-down list allows the user to select the storage type to use for the User-Group combination. Available options are as follows:

-Volatile: This storage type is temporary. The configuration setting will be erased upon restarting the device.

-NonVolatile: This storage type is permanent. The configuration setting will be saved upon restarting the device.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP filter table at the bottom of this page.

The user may also select a SNMP filter entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNMP filter entries in the SNMP filter table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

11. SNTP

11.1 SNTP UNICAST

Figure 43: SNTP Unicast Table

Forward Address Type: This field specifies the address type of the unicast forwarding address. The user can choose between IPv4 and IPv6 options.

Unicast ServerIP Addr: This field allows the user to specify the unicast IP address of the SNTP server.

Server Port: This field specifies the port on which the SNTP server is running. Valid range is 1025-65535.

SNTP Version: This field allows the user to specify the SNTP version that is supported by the SNTP server. Available options are as follows:

- Version 3
- Version 4

Unicast Server Type: This drop-down list allows the user to specify whether the SNTP server to be added will be used as a primary SNTP server or a secondary SNTP server.

After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNTP unicast table at the bottom of this page.

The user may also select a SNTP unicast entry from the table at the bottom of the page and click the "Delete" button to delete the specified entry from the table.

The user may also modify portions of existing SNTP unicast entries in the SNTP unicast table at the bottom of the page. After desired changes have been made to the table, the user may click the "Apply" button at the bottom of the table to apply changes made.

11.2 SNTP BROADCAST

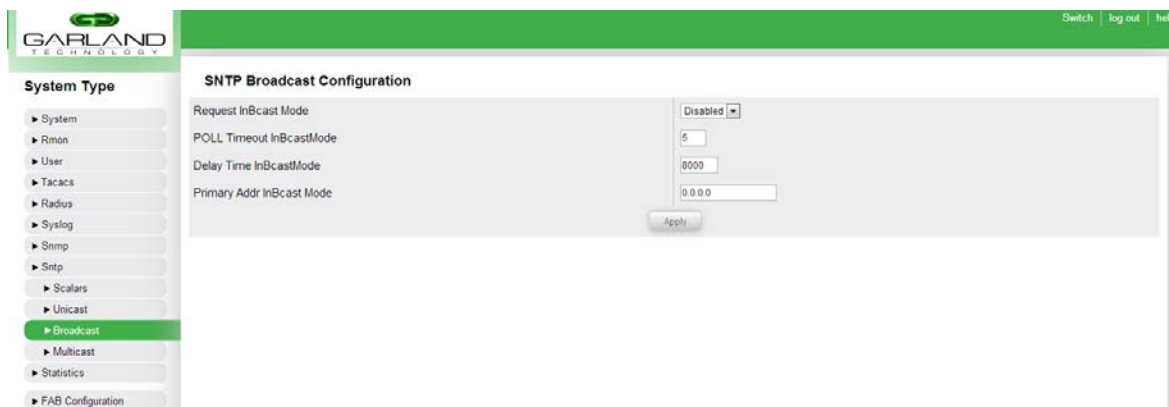


Figure 44: SNTP Broadcast Configuration

Request InBcast Mode: This field allows the user to specify the SNTP send request status in broadcast mode. Available options are as follows:

- **Enabled:** The SNTP request is sent to the broadcast server to calculate the delay time.
- **Disabled:** The SNTP request is not sent.

POLL Timeout InBcast Mode: Specifies the number of seconds to wait for a response from an SNTP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds.

Delay Time InBcast Mode: Specifies the delay time when there is no response from the broadcast server. This value ranges between 1000 and 15000 microseconds.

Primary Addr InBcast Mode: Specifies the primary server IP address learnt in Broadcast addressing mode. This is a read-only field.

11.3 SNTP MULTICAST

The screenshot shows the 'SNTP Multicast Configuration' page. On the left is a 'System Type' sidebar with options like System, Rmon, User, Tacacs, Radius, Syslog, Snmp, Sntp, Scalars, Unicast, Broadcast, Multicast (selected), Statistics, and FAB Configuration. The main area contains configuration fields for SNTP Multicast. The 'Send Request' field is a dropdown menu set to 'Disabled'. The 'Poll timeout' field is a text input with the value '5'. The 'Delay Time' field is a text input with the value '8000'. The 'Group Address Type' field is a dropdown menu. The 'Group Address' field is a text input with the value '0.0.0.0/multicast:3'. The 'Primary Server Addressing Mode' field is a dropdown menu. The 'Primary Server Address' field is a text input with the value '0.0.0.0/multicast:3'. An 'Apply' button is located at the bottom right of the configuration area.

Figure 45: SNTP Multicast Configuration

Send Request In: Specifies the SNTP send request status in Multicast mode. Available options are as follows:

- **Enabled:** The SNTP request is sent to the multicast server to calculate the delay time.
- **Disabled:** The SNTP request is not sent.

Poll Timeout: Specifies the number of seconds to wait for a response from a SNTP server before considering the attempt to have timed out. This value ranges between 1 and 30 seconds.

Delay Time: Specifies the delay time when there is no response from the multicast server. This value ranges between 1000 and 15000 microseconds.

Group Address Type: This field allows the user to specify the multicast group address type.

Group Address: This field allows the user to specify the the multicast group address.

Primary Server Addressing Mode: Specifies the address type of the primary server learnt in Multicast addressing mode.

Primary Server Address: Specifies the primary server IP address learnt in Multicast addressing mode. This is a read-only field.

11.4 SNTP SCALARS

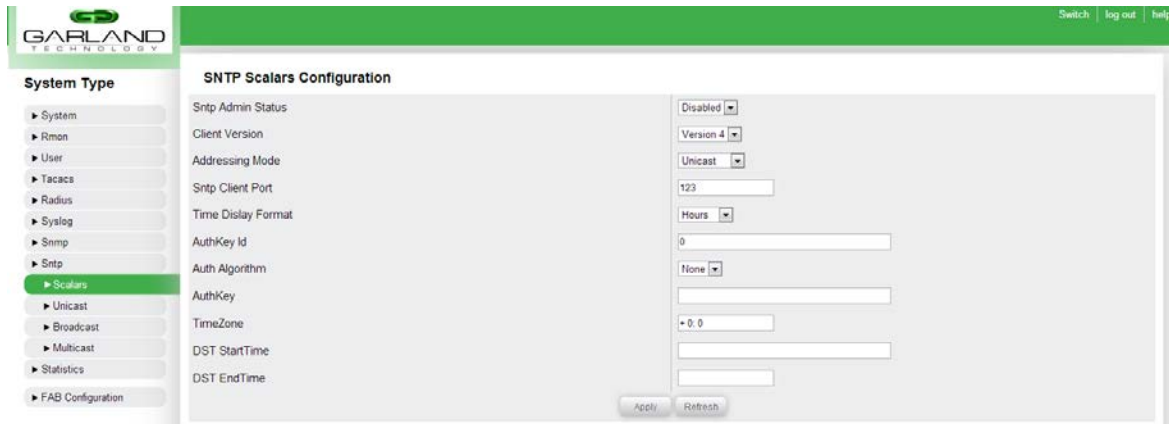


Figure 46: SNTP Scalars Configuration

SNTP Admin Status: Users are able to enable or disable the SNTP client module using this drop-down menu.

Client Version: This field allows users to specify the SNTP client version to use. All SNTP requests will be sent out using the version number specified in this field. Available options are as follows:

1. -Version 1
2. -Version 2
3. -Version 3
4. -Version 4

Addressing Mode: This field allows the user to specify the SNTP client addressing mode. Available options are as follows:

- **Unicast:** SNTP client operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
- **Broadcast:** SNTP client operates in a point-to-multipoint fashion. The SNTP server uses an IP local broadcast address instead of a multicast address. The broadcast address is scoped to a single subnet, while a multicast address has Internet wide scope.
- **Multicast:** SNTP client operates in point-to-multipoint fashion. The SNTP server uses a multicast group address to send unsolicited SNTP messages to clients. The client listens on this address and sends no requests for updates.
- **Anycast:** This feature is currently not supported.

SNTP Client Port: This field allows the user to specify the port that the SNTP client will use. Valid range is 1025-65535.

Time Display Format: This field allows the user to pick the display format for the time. This field is a drop-down menu and has the following options:

- **Hours:** 24 hour time format
- **Am/Pm:** 12 hour AM/PM format

AuthKey ID: This field allows the user to specify the key identifier that will be used to identify the cryptographic key used to generate the message-authentication code.

Auth Algorithm: This drop-down list allows the user to specify the authentication algorithm to be used for SNTP. Available options are as follows:

- **None:** No authentication is used.
- **MD5:** Message Digest-5 will be used.
- **DES:** Data Encryption Standard will be used.

Auth Key: Specifies the authentication key that is used to implement NTP authentication.

TimeZone: Specifies the system time zone with respect to UTC. That is, plus indicates forward time zone and minus indicates backward time zone. The valid format is (+/-)HH:MM.

DST StartTime: Specifies the DST (Daylight Saving Time) start time. The valid format is [weekofmonth-weekofday-month, HH:MM].

DST EndTime: Specifies the DST end time. The valid format is [weekofmonth-weekofday-month, HH:MM].

12. STATISTICS

The system keeps track of the counters passed through the unit since boot time. There are counters, traffic rate, and RMON statistics for every port. Users can clear the statistics of each port as well.

12.1 PORT STATISTICS

Index	MTU	Received Octets	Received Unicast Packets	Received Multicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted Multicast Packets	Transmitted Discards	Transmitted Errors
Ex0/1	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/2	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/3	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/4	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/5	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/6	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/7	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/8	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/9	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/10	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/11	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/12	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/13	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/14	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/15	9216	00	00	00	0	0	0	00	00	00	0	0
Ex0/16	9216	00	00	00	0	0	0	00	00	00	0	0
cpu0	1500	00	00	00	0	0	0	00	00	00	0	0

Figure 47: Port statistics

Users can view the statistics of receive and transmit counters of every port on this page.

This page displays various counters for the ports on the device. The following list describes the various columns of the port statistics table:

- **Index:** This field displays the name of the individual port.
- **MTU:** This field displays the Maximum Transmission Unit of each individual port. The MTU can be configured in the CLI.
- **Received Octets:** This field displays the number of octets (bytes) received for the individual port.
- **Received Unicast Packets:** This field displays the number of unicast packets received for the individual port.
- **Received Multicast Packets:** This field displays the number of non-unicast packets received for the individual port.
- **Received Discards:** This field displays the number of received packets that were discarded for the individual port.
- **Received Errors:** This field displays the number of errors received in incoming packets for the individual port.
- **Received Unknown Protocols:** This field displays the number of packets received where the protocol of the packet could not be identified for the individual port.

Garland Technology EdgeLens

- **Transmitted Octets:** This field displays the number of octets (bytes) transmitted for the individual port.
- **Transmitted Unicast Packets:** This field displays the number of unicast packets transmitted for the individual port.
- **Transmitted Multicast Packets:** This field displays the number of non-unicast packets transmitted for the individual port.
- **Transmitted Discards:** This field displays the number of transmitted packets that were discarded for the individual port.
- **Transmitted Errors:** This field displays the number of errors transmitted in outgoing packets for the individual port.

12.2 CLEAR PORT STATISTICS

12.3 RMON STATISTICS

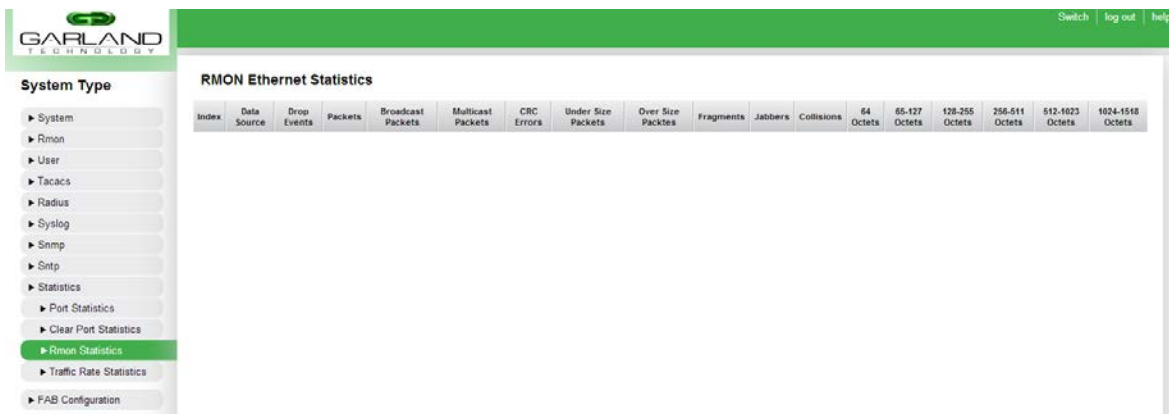


Figure 48: RMON Statistics

Users can view the statistics of each RMON index created.

This page displays various RMON statistics if RMON has been configured on the device. The following list describes the various columns of the RMON statistics table:

- **Index:** This field specifies the index of the entry in the table.
- **Data Source:** This field displays the OID of the port for the RMON statistics entry.
- **Drop Events:** This field displays the number of dropped packets for the RMON statistics entry.
- **Packets:** This field displays the number of packets matching the RMON configuration criteria.
- **Multicast Packets:** This field displays the number of multicast packets matching the RMON config criteria.
- **CRC Errors:** This field displays the number of CRC errors in the traffic matching the RMON config criteria.
- **Under Size Packets:** This field displays the number of under size packets matching the RMON config criteria.
- **Over Size Packets:** This field displays the number of over-size packets matching the RMON config criteria.
- **Fragments:** This field displays the number of fragments in the traffic matching the RMON config criteria.
- **Jabbers:** This field displays the number of jabbers in the traffic matching the RMON config criteria.
- **Collisions:** This field displays the number of collisions in the traffic matching the RMON config criteria.
- **64 Octets:** This field displays the number of 64 byte packets matching the RMON config criteria.

- **65 - 127 Octets:** This field displays the number of packets between 65 and 127 bytes matching the RMON config criteria.
- **128 - 255 Octets:** This field displays the number of packets between 128 and 255 bytes matching the RMON config criteria.
- **256 - 511 Octets:** This field displays the number of packets between 256 and 511 bytes matching the RMON config criteria.
- **512 - 1023 Octets:** This field displays the number of packets between 512 and 1023 bytes matching the RMON config criteria.
- **1024 - 1518 Octets:** This field displays the number of packets between 1024 and 1518 bytes matching the RMON config criteria.

12.4 TRAFFIC RATE STATISTICS



Figure 49: Traffic Rate Statistics

This page shows the current and peak traffic rates of the unit since boot time.

This page displays traffic rate statistics of the ports on the unit. The page displays the current TX and RX rate of each port as well as the peak TX and RX rates.

In the top right of the page there are polling options. Inputting a value in the polling text box will set the polling interval. After the desired interval is entered, it is necessary to click the radio button next to the checkbox for the setting to take effect. Selecting the "No Polling" option will disable the traffic rate polling.

13. EDGELENS CONFIGURATION

Users are able to configure the flow of traffic through the configuration maps. This section will contain the options to create configuration maps, filter templates and port channels (bundles, bond, etc). It will also contain a section for the port options.

13.1 Configuration Maps



Configuration Maps					
		<div> 1 Show All 2 New 3 Edit 4 Delete 5 Set Priorities </div>			
	name	date created	status	priority	packet matched count
	Many to one (aggregation)	2012-10-02T02:24:38.597Z	<div> 8 enabled </div>	<div> 6 2997 7 </div>	0
	One to Many (only HTTP)	2012-10-02T02:23:26.342Z	<div> enabled </div>	<div> 2998 </div>	0

Figure 50: Configuration Maps

1. The “Show All” option in the configuration maps interface will truncate and display all configuration maps on a single page. Users can edit a specific configuration map in this view by clicking on it.
2. Clicking “New” will allow the user to create a new configuration map. It will not be saved until the user clicks “Save” on the configuration map page.
3. Selecting an existing configuration map by clicking on it and then selecting the “Edit” button will open the existing configuration map, allowing the user to edit its current configuration.
4. Selecting an existing configuration map by clicking on it and then selecting the “Delete” button will delete the selected configuration map.
5. After modifying the priority of a configuration map, it is necessary to press the “Set Priorities” button.
6. Clicking this button will raise the priority of the configuration map. This will decrease the numerical priority value.
7. Clicking this button will lower the priority of the configuration map. This will increase the numerical priority value.
8. Clicking this button will enable/disable the configuration map. It can be disabled/enabled by clicking the same button again.

Users are able to create the configuration maps on this page; this will include load balancing, filtering, aggregation and mirroring.

Multiple configuration maps can be made on the system. Users will have the capability to disable or enable each configuration map.

When multiple configuration maps are made, users can set the priority of each to determine which rule should be looked at first.

13.1.1 New Configuration Map

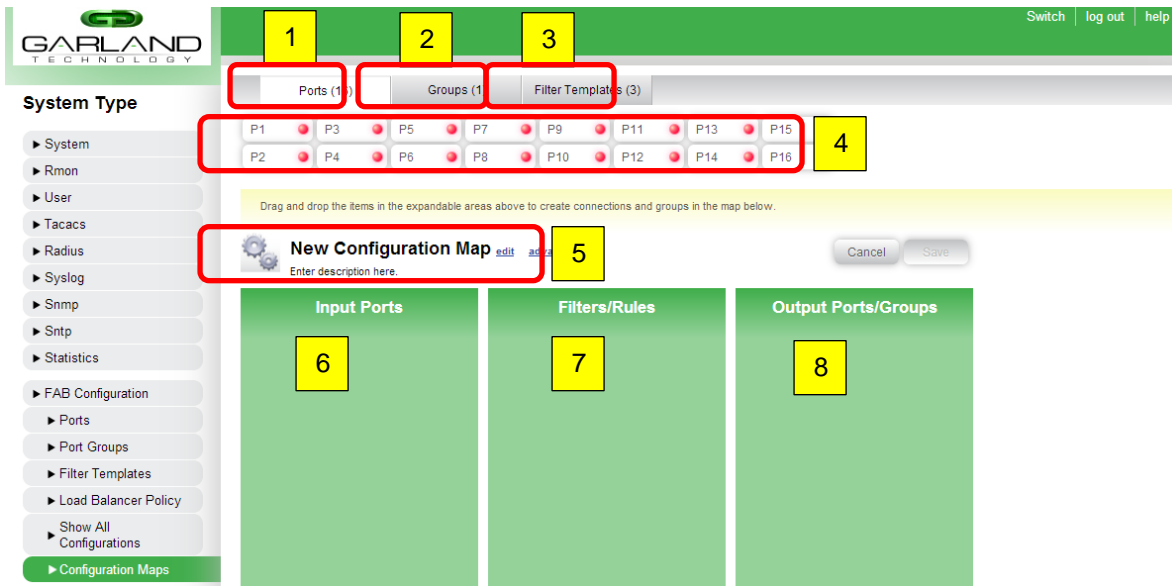


Figure 51: Configuration Maps

1. This is the ports tab which updates what shows in section 4. A green colored bubble signifies that a link has been established, while a red colored bubble signifies that no link has been established.
2. This is the port groups tab which updates what shows in section 4 by default, it will be empty as there is no default port channels created.
3. This is the filter templates tab which updates what shows in section 4. Users can create filter templates and use them in the configuration map.
4. This area refreshes itself when tabs are changed between sections 1-3. Users can drag these icons to sections 6-8.
5. This section allows users to name and write a description for the configuration map without looking into detail.
6. Users can drag ports from section 4 when they are under the ports tab to this section. This will be the input port where traffic comes in.
7. Users can drag rules/filters from section 4 when they are under the filters tab to this section. This is the rule which will determine whether the type of traffic that is allowed to flow through to the output port or deny all traffic.
8. Users can drag ports and port groups from section 4 when they are under the ports or groups tab. This will be the output port(s).*

*If no port groups are created and user wishes to create a port group, users can drag ports on top of each other. A new window will pop up allowing the user to create a port group or virtual trunk for load balancing purposes. Note that the network ports of the Niagara 3216PT system may only function as input ports.

Garland Technology EdgeLens
13.1.2 Multiple Port Selection

13.1.3 Graph



Figure 52: Multiple Port Selection

Users are able to view a graph representing the current traffic rate in packets per second or in bits per second. Users are also able to zoom in on a more specific time period of the graph.

13.1.4 Port/Filter Statistics

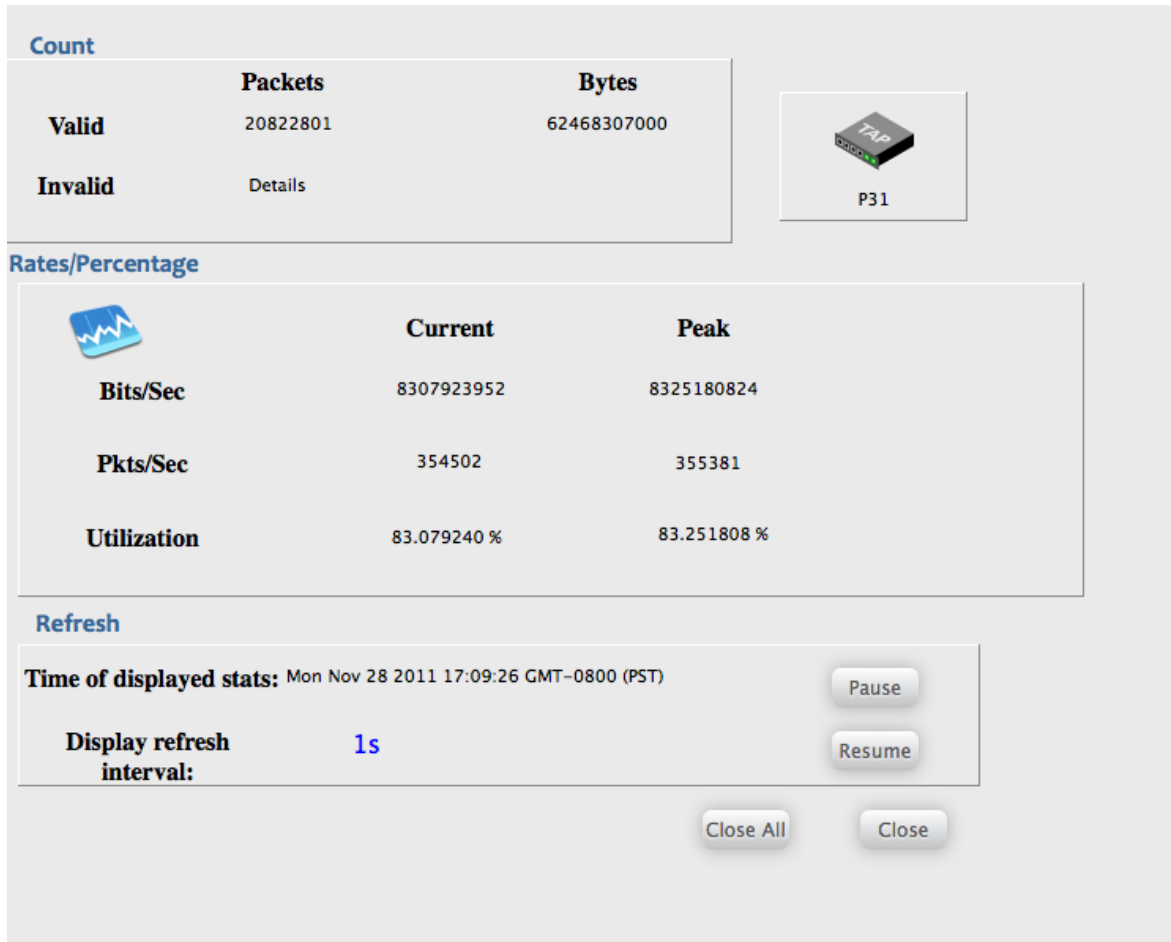
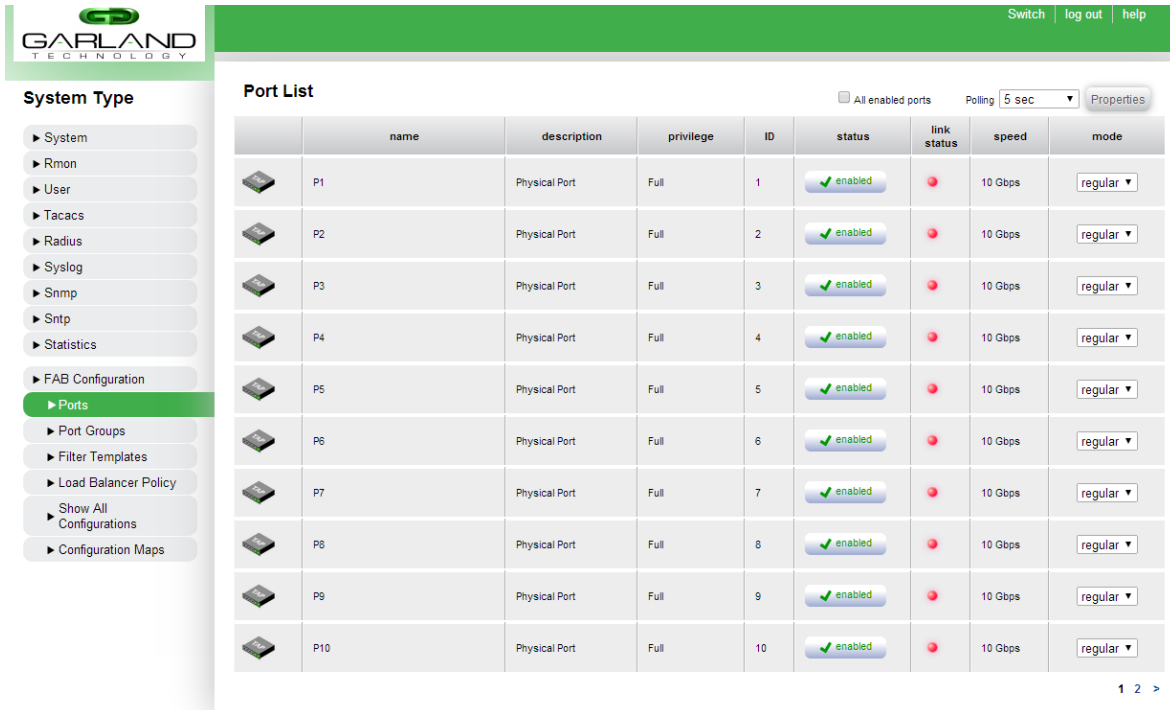


Figure 53: Port/Filter Statistics





















Users are able to view statistics for specific ports and filters. To view statistics of a specific port, users can select the “statistic” button of a specific port from the configuration maps interface. To view statistics of a specific filter, users can select the “statistic” button of a specific filter from the configuration maps, or from the edit port page (to view egress filter statistics).

13.1.5 Ports



Port List

☐ All enabled ports Polling: 5 sec Properties

	name	description	privilege	ID	status	link status	speed	mode
	P1	Physical Port	Full	1	enabled		10 Gbps	regular
	P2	Physical Port	Full	2	enabled		10 Gbps	regular
	P3	Physical Port	Full	3	enabled		10 Gbps	regular
	P4	Physical Port	Full	4	enabled		10 Gbps	regular
	P5	Physical Port	Full	5	enabled		10 Gbps	regular
	P6	Physical Port	Full	6	enabled		10 Gbps	regular
	P7	Physical Port	Full	7	enabled		10 Gbps	regular
	P8	Physical Port	Full	8	enabled		10 Gbps	regular
	P9	Physical Port	Full	9	enabled		10 Gbps	regular
	P10	Physical Port	Full	10	enabled		10 Gbps	regular

1 2 >

Figure 54: Ports

Users can re-label each port's name and description as well as change the icon when they highlight and edit a port. They can administratively bring a port up/down under the status column. They are also able to force the port up. Ports will be forced up under the following conditions.

1. The port is administratively up.
2. There is an SFP present.

Editing a port allows users to apply egress filters to specific port(s),

13.1.6 Egress Filters

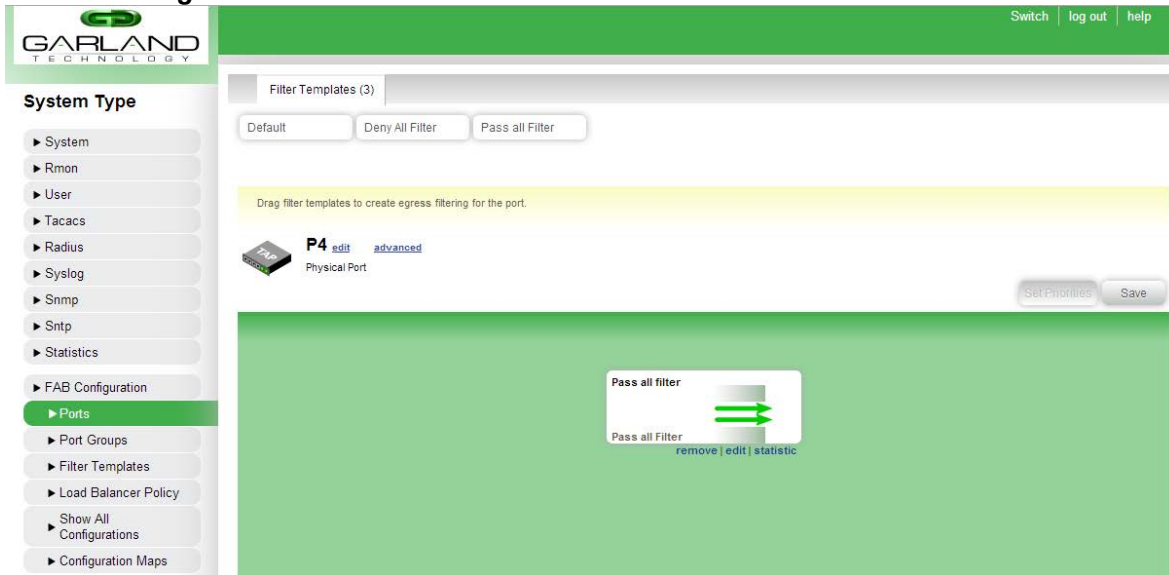


Figure 55: Egress Filters

Egress filters can be applied on a per-port basis. To apply an egress filter to a port, Click on the desired port from the “Ports” list and click the “Edit” button. An interface similar to the configuration maps interface will be shown, where users can add/edit a filter.

13.1.7 Ports – Advanced Options

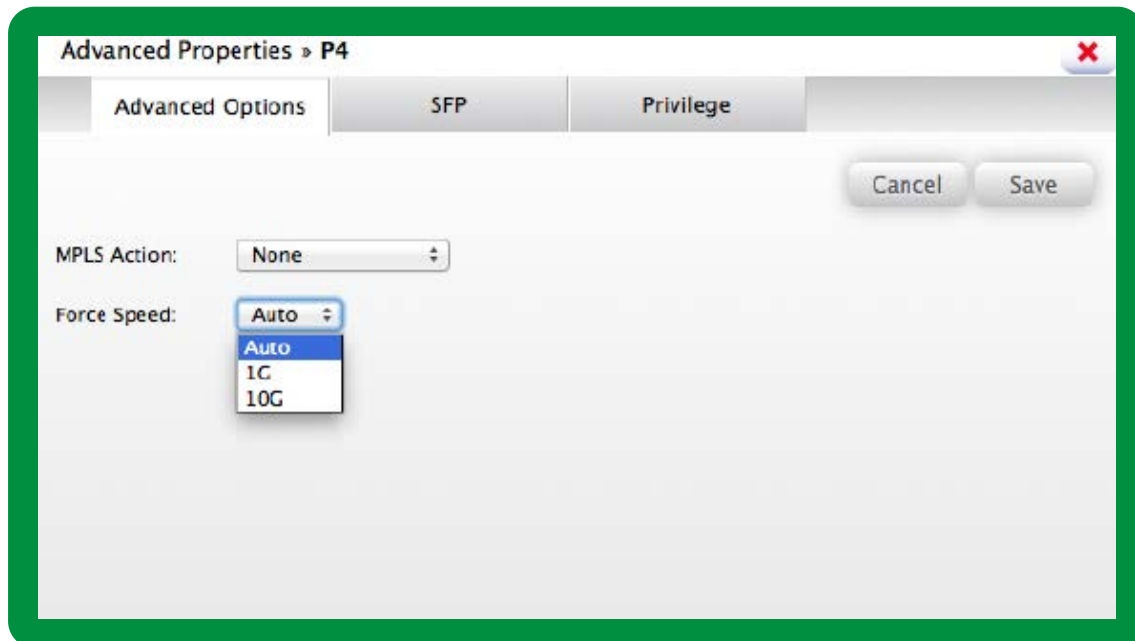


Figure 56: Advanced Options

The advanced options of a specific port allow users to strip MPLS labels for all traffic incoming on that port. Users may also force a port to use a specific speed if a dual-speed SFP+ module is used. Note that the speed can only be forced if a supported dual-speed SFP+ module is plugged in.

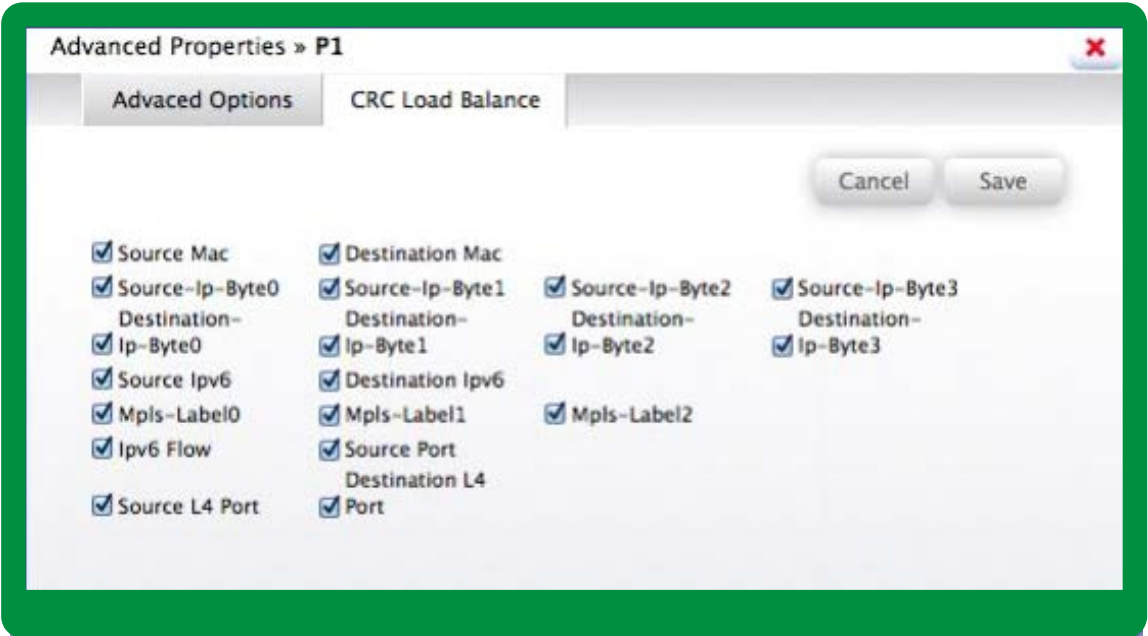


Figure 57: CRC Load Balancing Policy

Users may change the CRC Load Balancing policy on a per-port basis.

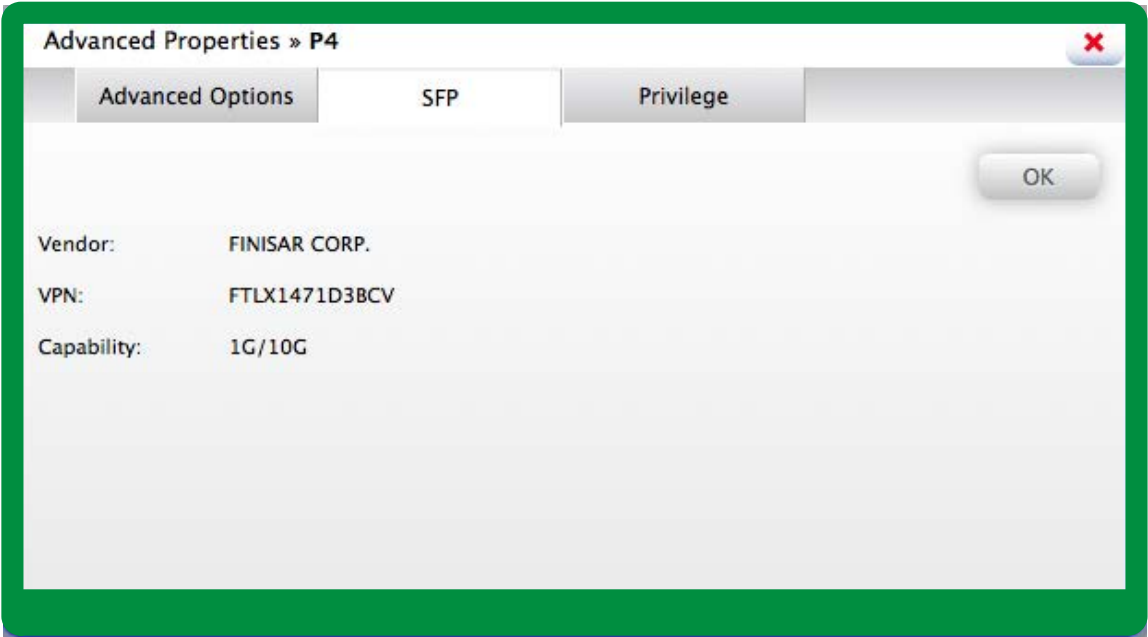


Figure 58: Port SFP Information

Users may view the information about an SFP/SFP+ module plugged in to the port. Available information includes vendor, part number, and speed capabilities.

13.2 PORT GROUPS

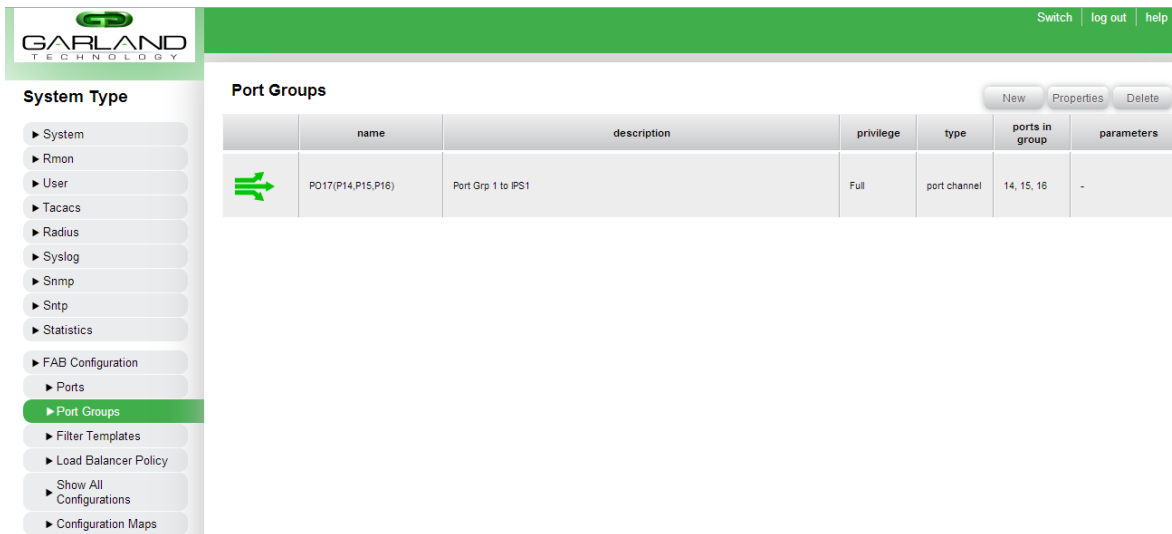


Figure 59: Port Groups

Users can create, edit and delete port groups (bundle/bonds) on this page.

13.2.1 New Port Groups

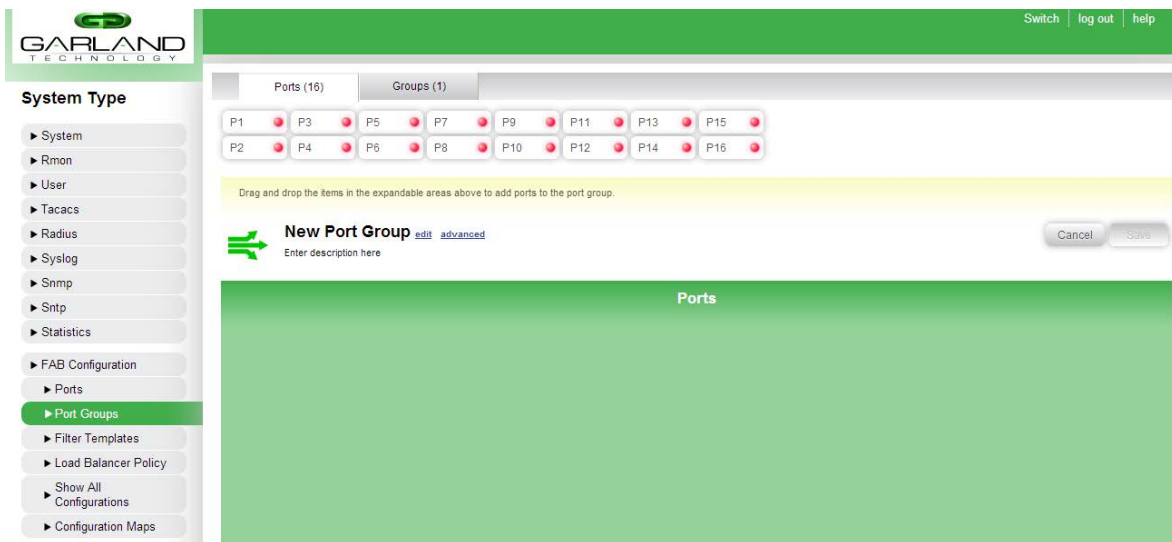


Figure 60: New Ports Group

Users can drag the ports under “Ports(#)” into the green box labeled “Ports”. A maximum of 8 ports can be applied to the port group. A port group can be named and contain a description.

This page allows the user to create, modify, or delete port groups. From this page, the user can only create a port-channel based port group.

Garland Technology EdgeLens

To create a new port group, the user can click the "New" button in the top right of the page. From there, the user can drag the desired physical ports from the "Ports" area at the top of the page to the blue area in the middle of the page.

Note: Physical ports cannot be part of more than one port group.

Users can click the "edit" button to modify the port group's description.

After the desired ports have been added to the port group, it is necessary to click the "Save" button to save the configuration to the device.

To edit a port group that has been previously created, the user can click on the existing port group and click the "Edit" button in the top right of the page. This will allow the user to add or remove ports from the port group. After editing is completed, it is necessary to click the "Save" button on the page to save the configuration to the device.

To delete a port group, click the existing port group and click the "Delete" button in the top right of the page.

13.3 FILTER TEMPLATES

Filters are used to direct the flow of traffic on the FAB Systems. Users can deny traffic, pass all traffic, pass traffic by certain criteria and tag packets with a VLAN. They can create a filter template such that it can be used in the configuration maps.

13.4 FILTER TEMPLATES PAGE

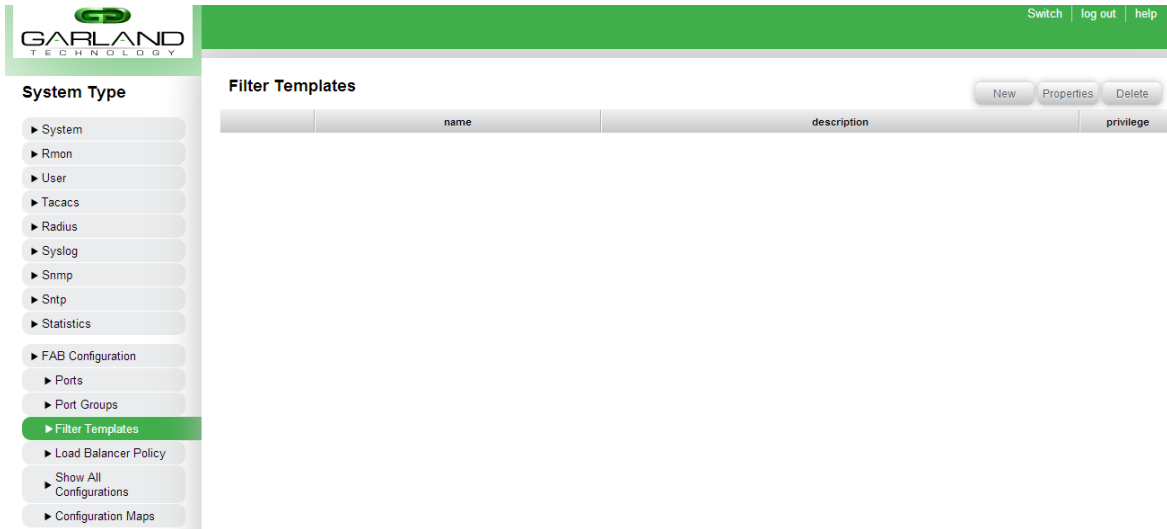


Figure 61: Filter Templates Page

This page allows user to create, edit and delete custom filter templates.

Filters are used to direct the flow of traffic on the device. Users can deny traffic, pass all traffic, pass traffic by certain criteria and tag packets with a VLAN. They can create a filter template such that it can be used in the configuration maps.

When users create a new filter template, they can define a filter name and its description under the General Tab.

Users can define the filter to pass all traffic, deny all traffic, pass it by certain criteria, or deny it by certain criteria. The criteria are the following.

1. -Layer 2
2. -Layer 3/4 (IPv4)
3. -IPv6
4. -User defined byte (UDB)

The system can tag packets, remove tags from packets, truncate the packets (sending only the first 128 bytes of the packet), or do nothing with it. Users that wish to strip VLAN tags of the packets will need to go under System -> Tag Settings and decide whether to remove one or two VLAN tags.

13.5 NEW FILTER TEMPLATES

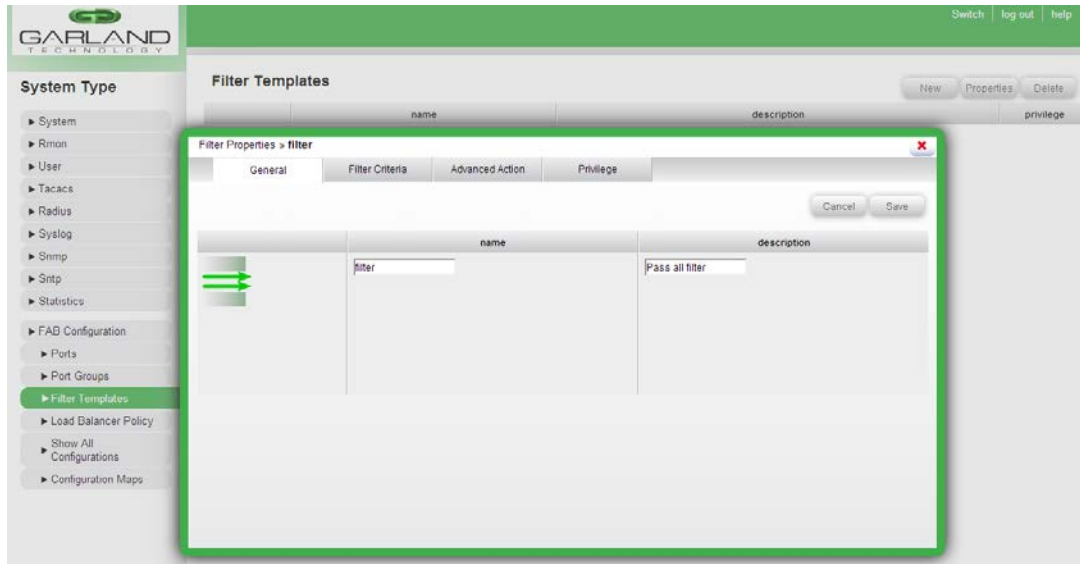


Figure 62: New Filter Template (General Tab)

When users create a new filter template, they can define a filter name and its description under the General tab.

13.6 NEW FILTER TEMPLATE

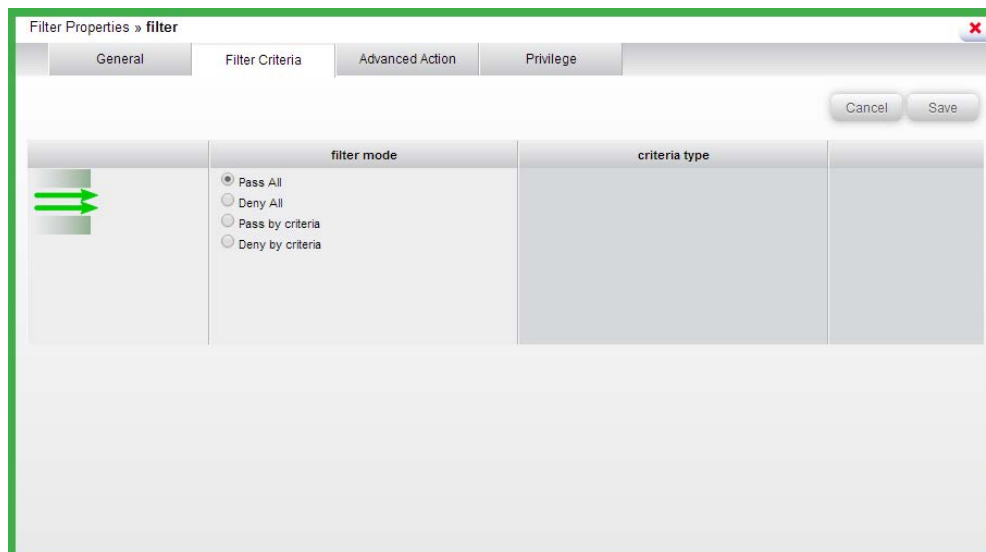


Figure 63: New Filter Criteria (Filter Criteria Tab)

Users can define the filter to pass all traffic, deny all traffic, pass it by certain criteria, or deny it by certain criteria. Multiple filter criteria can be added to a single filter by clicking the “Add” button. The criteria are the following.

1. Layer 2
2. Layer 3/4 (ipv4)
3. IPv6
4. User defined byte (UDB)

13.7 ADVANCED

Filter Properties » filter

General Filter Criteria Advanced Action Privilege

Cancel Save

action type	vlan-id
<input type="radio"/> Strip vlan <input type="radio"/> Tag vlan <input type="radio"/> Pkt Slice <input type="radio"/> L3-VPN-MPLS Strip <input checked="" type="radio"/> None	

Figure 64: Advanced

The system can tag packets, remove tags from packets, truncate the packets (sending only 128 bytes per packet), or do nothing with it. Users that wish to strip VLAN tags will need to go under System -> Tag Settings and decide whether to remove one or two VLAN tags. Users may also strip

L3 VPN (IP over MPLS) labels from this screen. Note that there may only be one output port/port group when L3 MPLS stripping is enabled.

14. Bypass Configuration

Users can configure appliance pairs, segment specific configuration maps, and other features relating specifically for the bypass segments.

14.1 BYPASS SEGMENTS

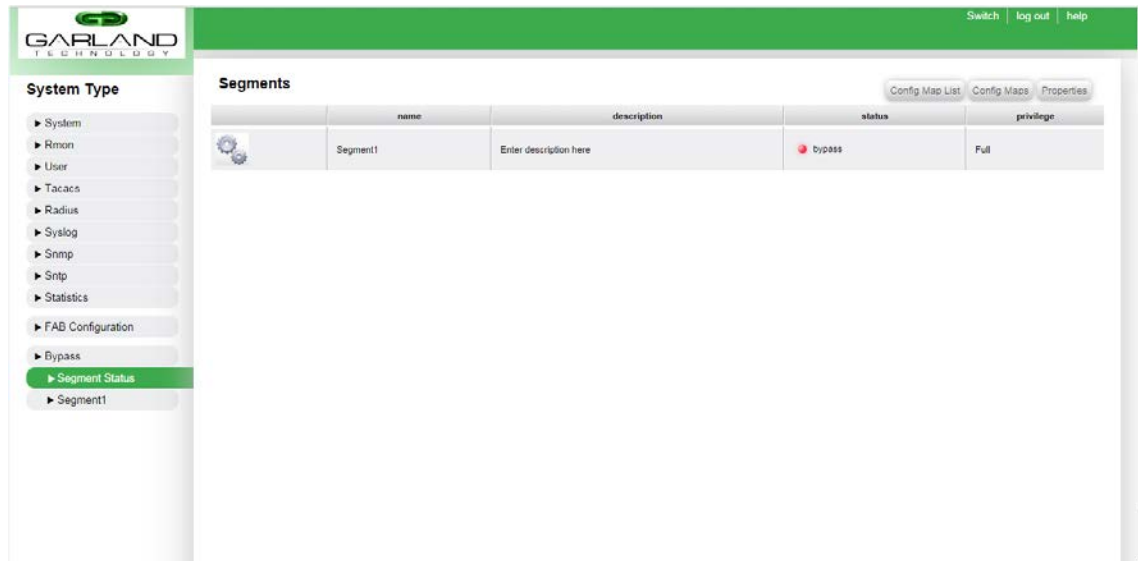


Figure 65: Bypass Segments

The “Segments” page displays a summary of the bypass segments configured on the FAB19GXXXX-BPAC. The page displays the segment name, segment description, and segment status. To modify a segment’s settings, click the segment followed by clicking the “Edit” button.

To view the configuration maps in list form for a specific bypass segment, click the segment followed by clicking the “Config Map List” button.

To view the configuration maps in summary form for a specific bypass segment, click the segment followed by clicking the “Config Maps” button

14.2 CONFIG MAP LIST



Figure 66: Config Map List

This page displays the configuration maps of a specific segment in list form. Users can enable/disable specific configuration maps of a segment from this page, as well as change the priorities of specific configuration maps.

14.3 CONFIG MAPS

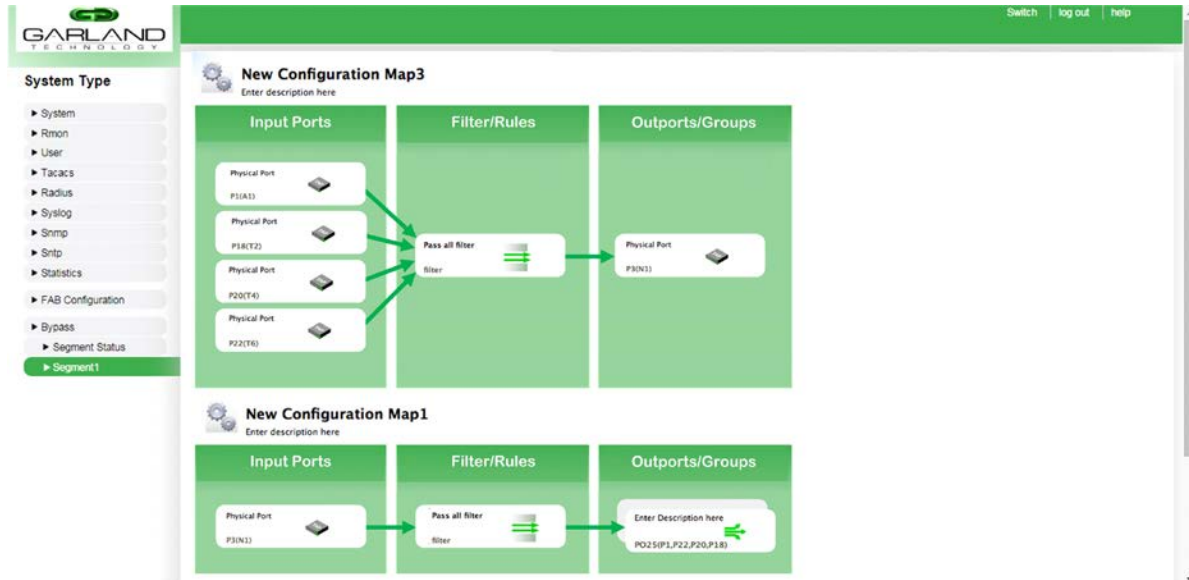


Figure 67: Config Map

This page displays the configuration maps of a specific segment in summary form. Users can view all of the configuration maps of a single segment from this page. Clicking on a specific configuration map from this page will allow the user to edit the specified configuration map.

14.4 Segment Configuration

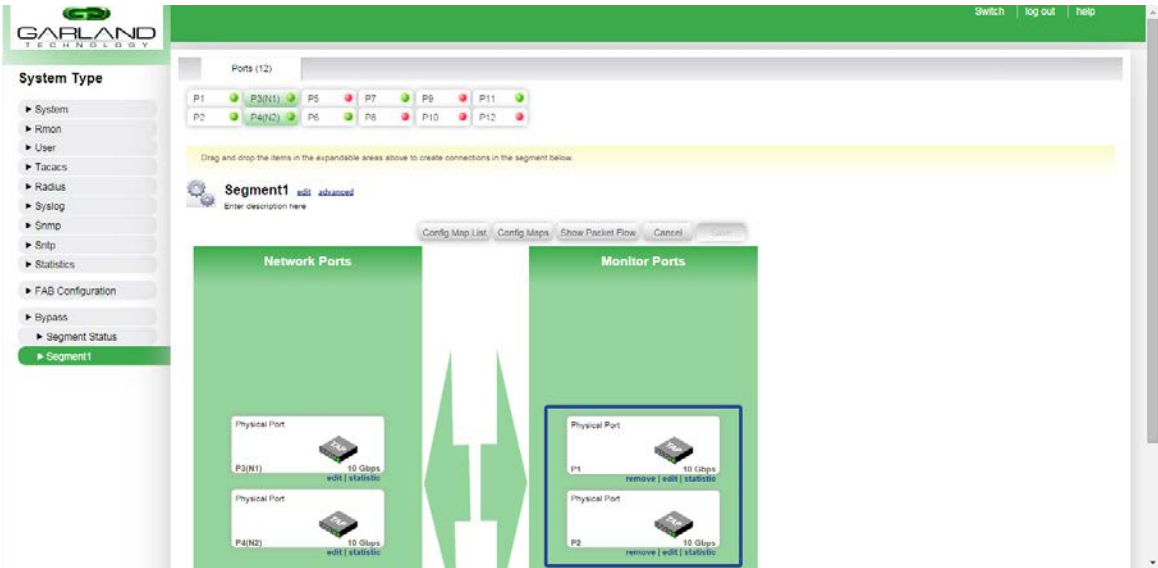


Figure 68: Segment Configuration

This page allows users to add or modify a bypass segment’s configuration. Users are able to add or remove appliance pairs from the segment, edit the name and description, as well as set advanced options for a particular segment.

To add an appliance pair to the bypass segment, users may simply drag an unused port from the port list at the top of the page to the “Appliance Ports” section on the page. Appliance ports must be added in pairs, and single ports cannot be added to a segment.

Each bypass segment contains 4 configuration maps that are automatically generated to define the traffic flow. If users add an additional appliance pair to a bypass segment’s configuration, the traffic flow will be automatically load balanced to the additional appliance pairs.

Note: Users cannot remove the default appliance pairs. It is only possible to add additional appliance pairs to a segment. Also, it is not possible to remove or replace the network ports associated with a bypass segment.

14.5 Segment Packet Flow

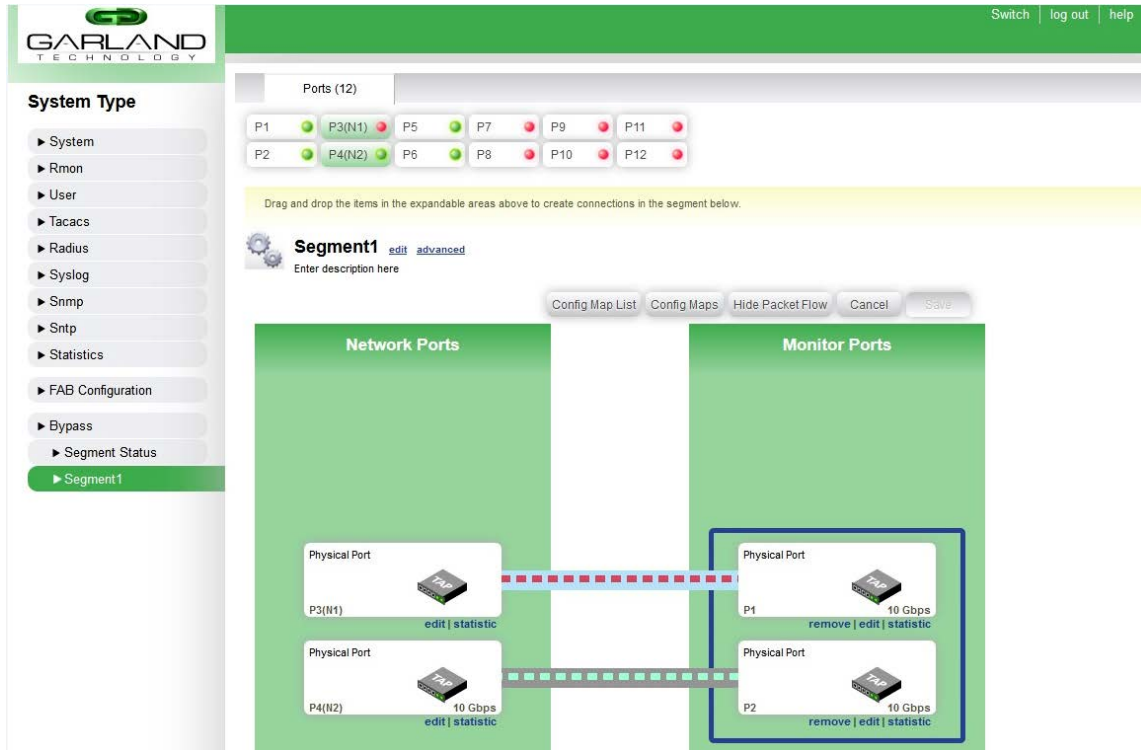


Figure 69: Segment Packet Flow

In a bypass segment's configuration page, users can click the "Show Packet Flow" button to view the current packet flow throughout the segment. The packet flow will dynamically change based on the current state of the segment (bypass/inline modes). The figure above displays the packet flow when the segment is inline.

14.6 Segment General Settings

Segment Properties » Segment1

General

Advanced

Cancel

Save

Bypass Segment

Enable

Fail Appliance Pair Threshold (0-10)

0

HB Lost Threshold (0-10)

2

HB Recv Threshold

3

HB Packet Type

ETH

HB Source Mac Address

00:00:00:00:00:00

HB Destination Mac Address

00:00:00:00:00:00

HB Source IP Address

0.0.0.0

HB Destination IP Address

0.0.0.0

HB Tx Frequency (msec)

30

HB Drop Timeout (msec)

100

Figure 70: Segment General Settings

Users may click the “advanced” button in a segment’s configuration page to view the individual settings of the bypass segment. Users are able to configure the following settings on this page:

- Bypass Segment Mode
- Failed Appliance Pair Threshold
- HB Lost Threshold
- HB Received Threshold
- HB Packet Type
- HB Source/Destination MAC addresses
- HB Source/Destination IP addresses
- HB Transmit Frequency
- HB Drop Timeout

Fail Appliance Pair Threshold defines the number of appliances that must fail before the segment goes into bypass mode. For example, if there are 4 appliance pairs in the segment, and the Fail Appliance Pair Threshold is set to “2”, then **more than 2** appliances must fail before the system goes into bypass mode. 3 appliances must fail in this example before the system goes into bypass mode.

14.7 Segment Advanced Settings

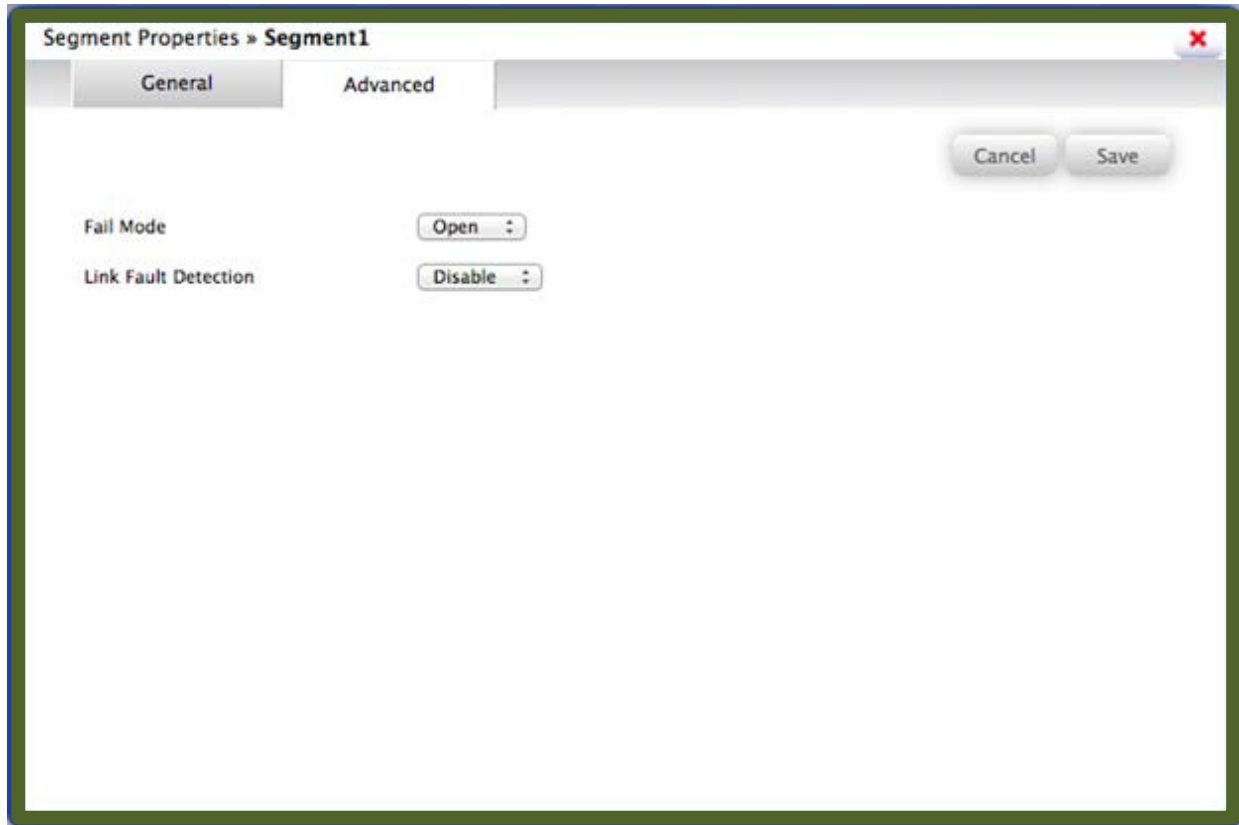


Figure 71: Segment Advanced Settings

Users may change the “Fail Mode” configuration of the bypass segment, as well as enable/disable Link Fault Detection (LFD) from the “Advanced” tab of the “advanced” page of the bypass segment

History

Version	Author	Date Effective	Nature of Change
1.3	George Bouchard	June 24, 2014	Genesis
1.4	George Bouchard	March 21, 2016	Minor corrections
2.0	George Bouchard	April 18, 2016	New Features and minor corrections