GARLAND TECHNOLOGY

See every bit, byte, and packet®

Garland Technology

FAB10G8AC

FAB10G16AC

FAB10G24AC

FAB10G48AC

FAB10G40AC

FAB40G36AC

Graphical User Guide

Firmware Rev Level: 42XX_8.28-20

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.: FAB10GXXXC-GUI_v8.28-20 rev 2.2

Table of Contents

Table of Figures

1. OVERVIEW

The FAB10Gxxx and FAB40G36xx are an intelligent solution to direct the flow of traffic. They have the capabilities to regenerate, load balance, filter, aggregate, or redirect the traffic. The products included in the FAB family are as follows:

- FAB10G8AC (8 ports of 10GbE/1GbE)
- FAB10G16AC (16 ports of 10GbE/1GbE)
- FAB10G24AC (24 ports of 10GbE/1GbE)
- FAB10G48AC (48 ports of 10GbE/1GbE)
- FAB40G36AC (32 ports of 10GbE/1GbE and 4 ports of 40GbE)

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

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 the default password user “**root**” and password “**gtroot1**”.

3. 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.

```
configure terminal
interface cpu0
ip address { <ip address> <subnet mask> }
```

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

```
configure terminal
ip route 0.0.0.0.0.0.0.0 <gateway ip>
```

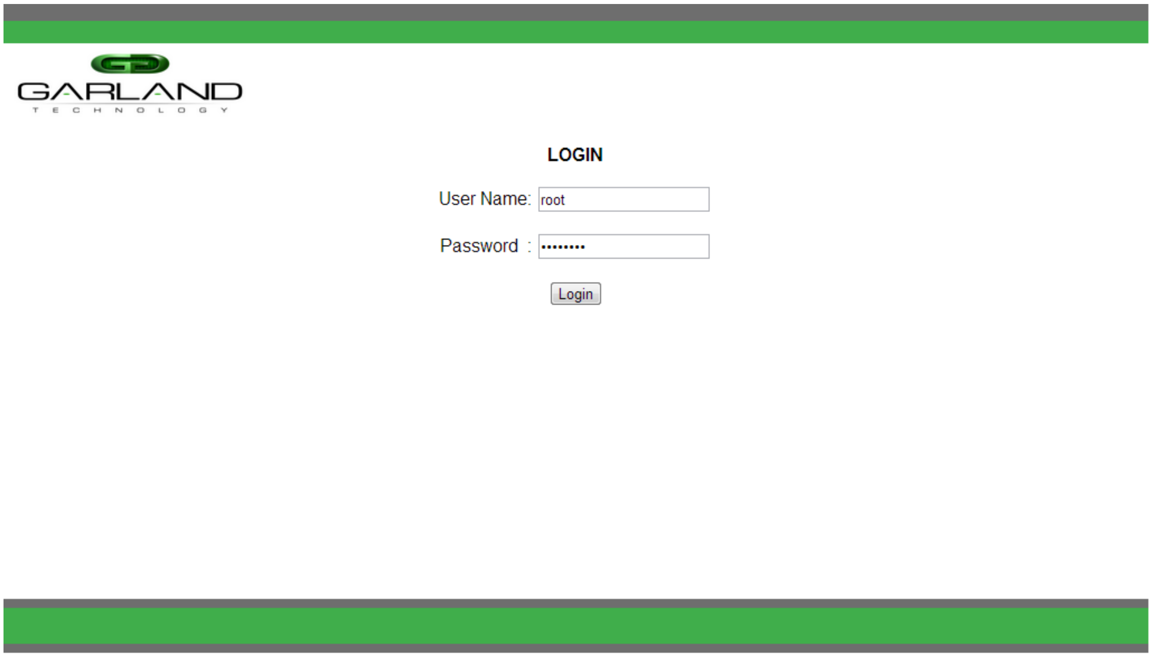
Accessing GUI

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

http://<ip_address>

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

3.1 LOGIN



LOGIN

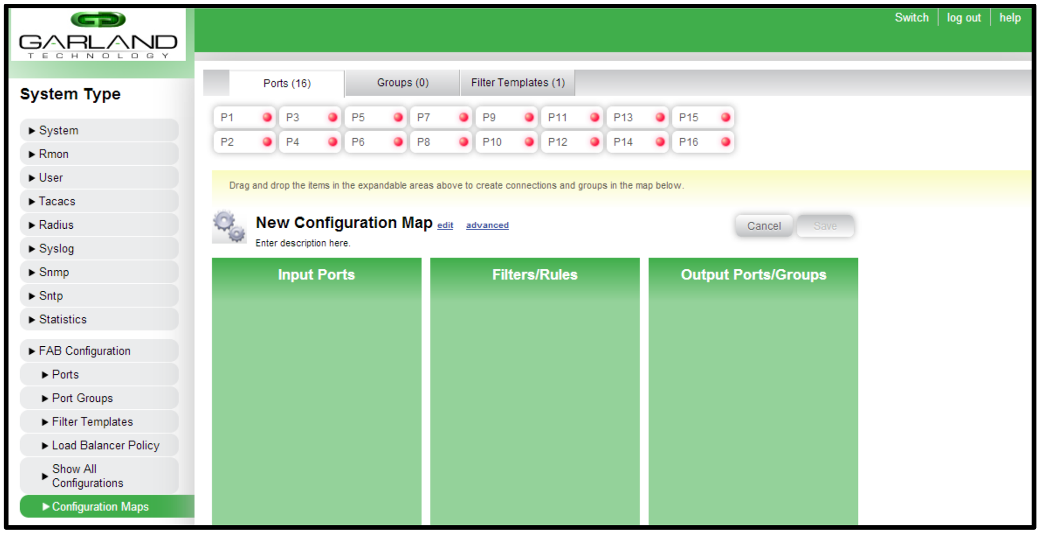
User Name: root

Password : ••••••••

Figure 1: Login Screen

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

3.2 FIRST SCREEN THAT OPENS



Drag and drop the items in the expandable areas above to create connections and groups in the map below.

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.

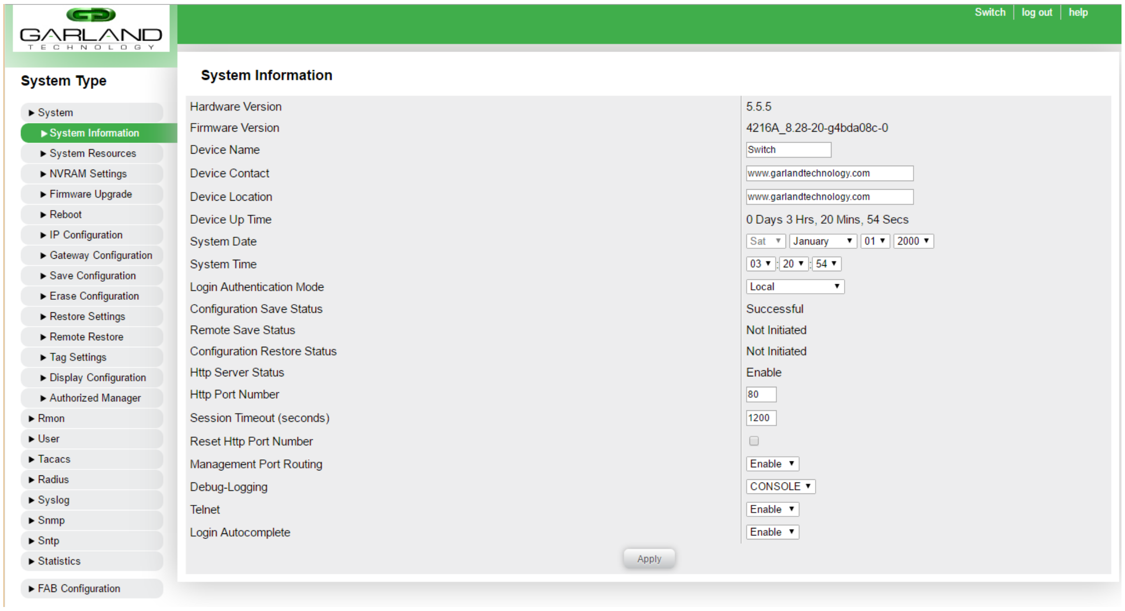
When multiple configuration maps are made, users can set the priority of each to determine which rule should be looked at first.

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. SYSTEM CONFIGURATION SETTINGS



System Information

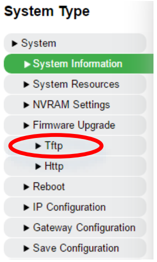
Hardware Version	5.5.5
Firmware Version	4216A_8.28-20-g4bda08c-0
Device Name	Switch
Device Contact	www.garlandtechnology.com
Device Location	www.garlandtechnology.com
Device Up Time	0 Days 3 Hrs, 20 Mins, 54 Secs
System Date	Sat ▾ January ▾ 01 ▾ 2000 ▾
System Time	03 ▾ : 20 ▾ : 54 ▾
Login Authentication Mode	Local ▾
Configuration Save Status	Successful
Remote Save Status	Not Initiated
Configuration Restore Status	Not Initiated
Http Server Status	Enable
Http Port Number	80
Session Timeout (seconds)	1200
Reset Http Port Number	□
Management Port Routing	Enable ▾
Debug-Logging	CONSOLE ▾
Telnet	Enable ▾
Login Autocomplete	Enable ▾

Figure 3: System Information

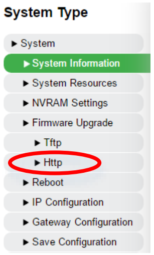
4.1 System Settings

Hardware Version: This field indicates the version of hardware present on the device. This field cannot be modified.

Firmware Version: This field indicates the version of firmware present on the device. Users may upgrade the device's firmware by using TFTP or HTTP.



TFTP firmware upgrade Option



HTTP firmware upgrade Option

Device Name: If there are multiple devices of the same type on a network, users may specify a unique device name to identify specific devices.

Device Contact: Specify an email address for support purposes.

Device Location: If there are multiple devices across different physical locations, users may specify the physical location of specific devices.

Device Up Time: Shows the current time since last boot. This field cannot be modified.

System Date: Users may manually specify the current date of the system.

System Time: Users may manually specify the current time of the system (Note: time is specified in military time).

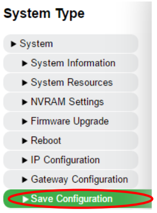
Login Authentication Mode: Users may configure how the device can be accessed remotely.

-Local: Users may login using credentials stored locally on the device.

-Remote: Users may login via a RADIUS server. This feature is currently not supported.

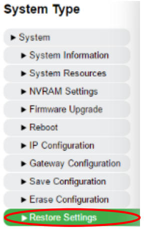
-TACACS: Users may login via a TACACS server.

Configuration Save Status: Shows the status of saving the device's configuration to the flash memory of the device. When the device's configuration has not been saved, this field will show "Not Initiated". Upon successfully saving the device's configuration, this field will show "Successful". Users may perform a save of the device's configuration from the "Save Configuration" page shown below and choosing the "Flash Save" option.
Remote Save Status: Shows the status of remotely saving the device's configuration. When the device's configuration has not been remotely saved, this field will show "Not Initiated". Upon successfully saving the device's configuration, this field will show "Successful". Users may perform a save of the device's configuration from the "Save Configuration" page shown below and choosing the "Remote Save" option.



Save Configuration Page

Configuration Restore Status: This field displays whether the device's configuration will be restored after a hard or soft reboot. In order to restore the device's configuration, users must save the device's configuration, and then enable the restore option from either the "Restore Settings" page or the "Remote Restore" page. When the device's configuration has not been set to restore, this field will show "Not Initiated". Upon enabling the restore option, this field will show "Successful". Users may enable the restore option from the "Restore Settings" page shown below or the "Remote Restore" page and choosing the appropriate restore option.



Restore Settings Page

Http Server Status: Displays the status of the HTTP web server. This field cannot be modified.

Http Port Number: Allows users to specify the port used for the web server. Default is port 80.

Reset Http Port Number: Allows the user to reset the web server's port back to 80 by marking the checkbox and clicking the "Apply" button at the bottom of the page.

Management Port Routing: Modifying this option is not supported for this platform.

Debug-Logging: Options include "Console" and "File". Default option is "Console". This option specifies whether debug messages will be displayed in the console or written to a file. Note: the "File" option is not supported.

Commit Support: This field specifies how the user's configuration will be applied to the device. The "Consolidated" option will apply configuration maps to the traffic based on the configuration map's priority setting. The "Immediate" option will apply configuration maps to the traffic based on the order of their creation. By default, the device is set to "Consolidated". This option should not be modified except for debugging purposes.

Commit Action: This field specifies whether the configuration will be written to the device. If set to "False", configurations will not be written to the device. By default, the device is set to "True". This option should not be modified except for debugging purposes.

Restore Settings Page

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

System Information

System Resources

NVRAM settings

Firmware Upgrade (tftp)

Firmware Upgrade (http)

Reboot

IP Configuration

Gateway Configuration

Save Configuration

Erase Configuration

Restore Configuration

Remote Restore

Tag Settings

Display Configurations

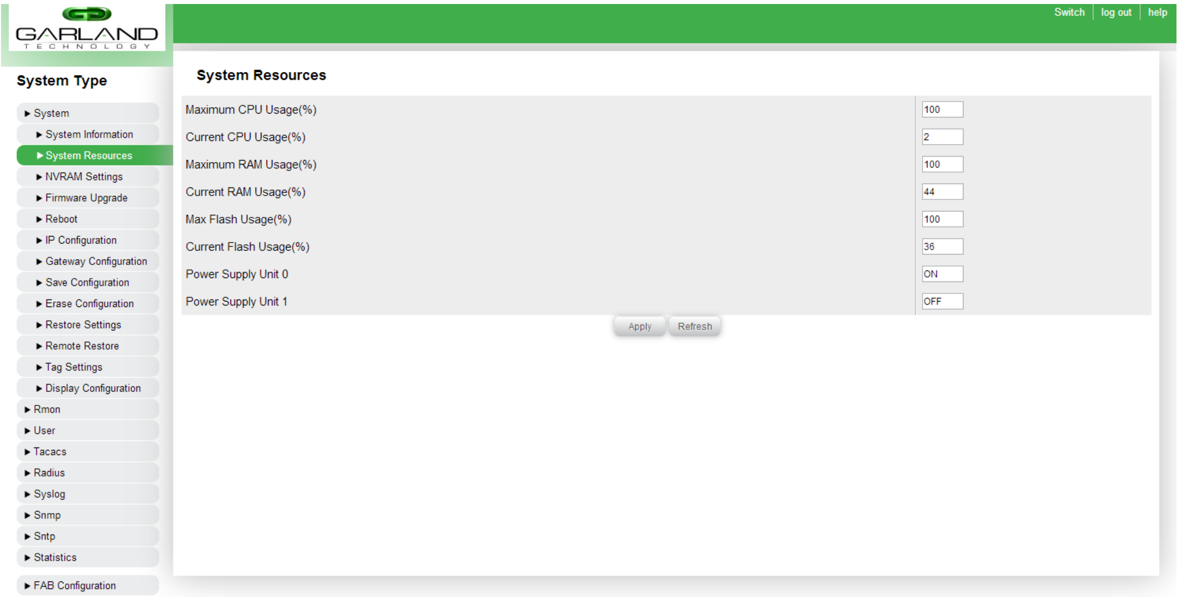
Gateway IP

Tagging setting

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.

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.

4.2 SYSTEM RESOURCES



System Resources

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

Figure 4: System Resources

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.

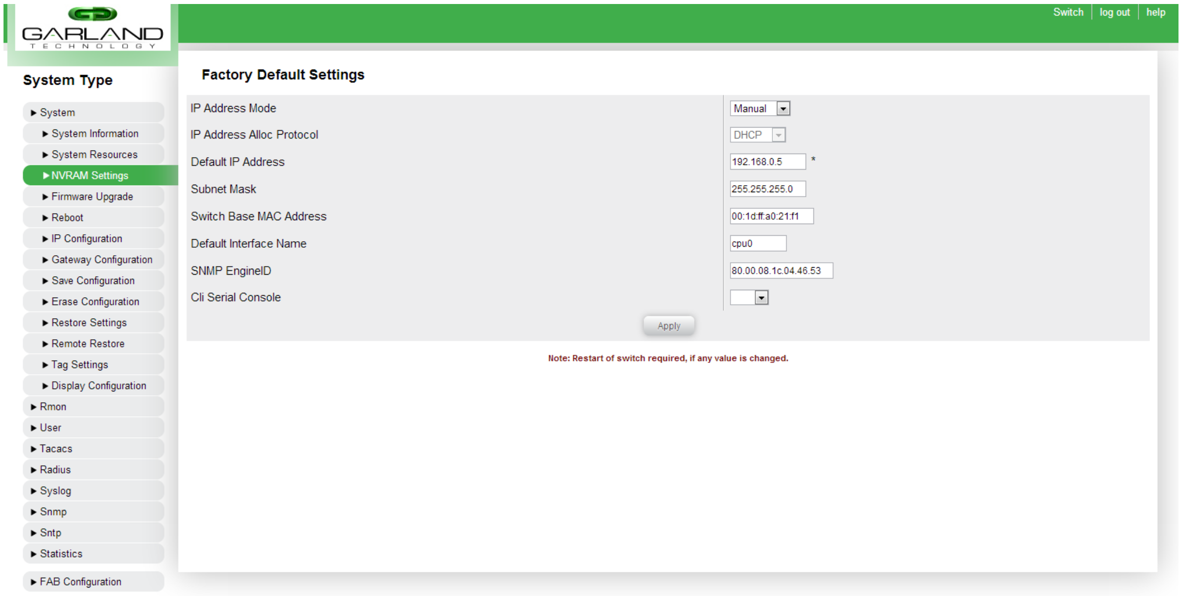
Max Flash Usage(%): This field allows the user to specify the maximum amount of non-volatile memory the device is allowed to use. This option should not be modified except for debugging purposes.

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

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

Power Supply Unit 2: This field displays the status of the second power supply of the device. This field cannot be modified.

4.3 NVRAM SETTINGS



Factory Default Settings

IP Address Mode	Manual
IP Address Alloc Protocol	DHCP
Default IP Address	192.168.0.5 *
Subnet Mask	255.255.255.0
Switch Base MAC Address	00:1d:ff:a0:21:f1
Default Interface Name	cpu0
SNMP EngineID	80.00.08.1c.04.46.53
Cli Serial Console	

Note: Restart of switch required, if any value is changed.

Figure 5: NVRAM Settings

The NVRAM settings page allows user to continue 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 Protoco**l", 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.

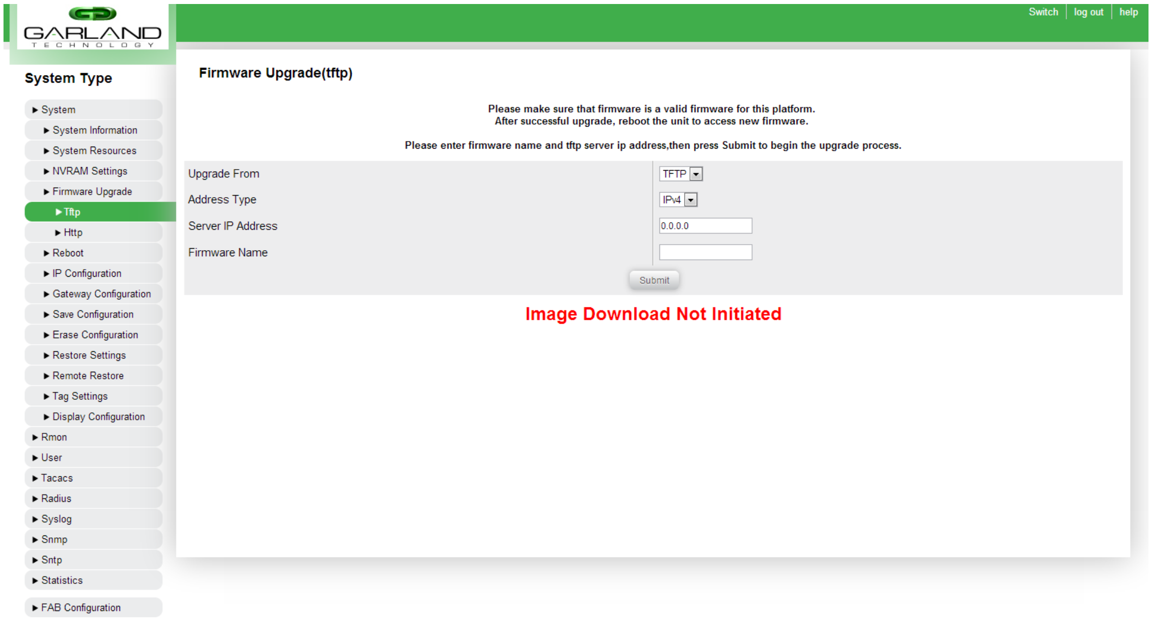
Switch Base MAC Address: This field displays the base MAC address of the device used for the management port as well as the data ports. This field cannot be modified.

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.

4.4 FIRMWARE UPGRADE (TFTP)



Firmware Upgrade(tftp)

Please make sure that firmware is a valid firmware for this platform.
After successful upgrade, reboot the unit to access new firmware.

Please enter firmware name and tftp server ip address,then press Submit to begin the upgrade process.

Upgrade From	TFTP
Address Type	IPv4
Server IP Address	0.0.0.0
Firmware Name	

Image Download Not Initiated

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".

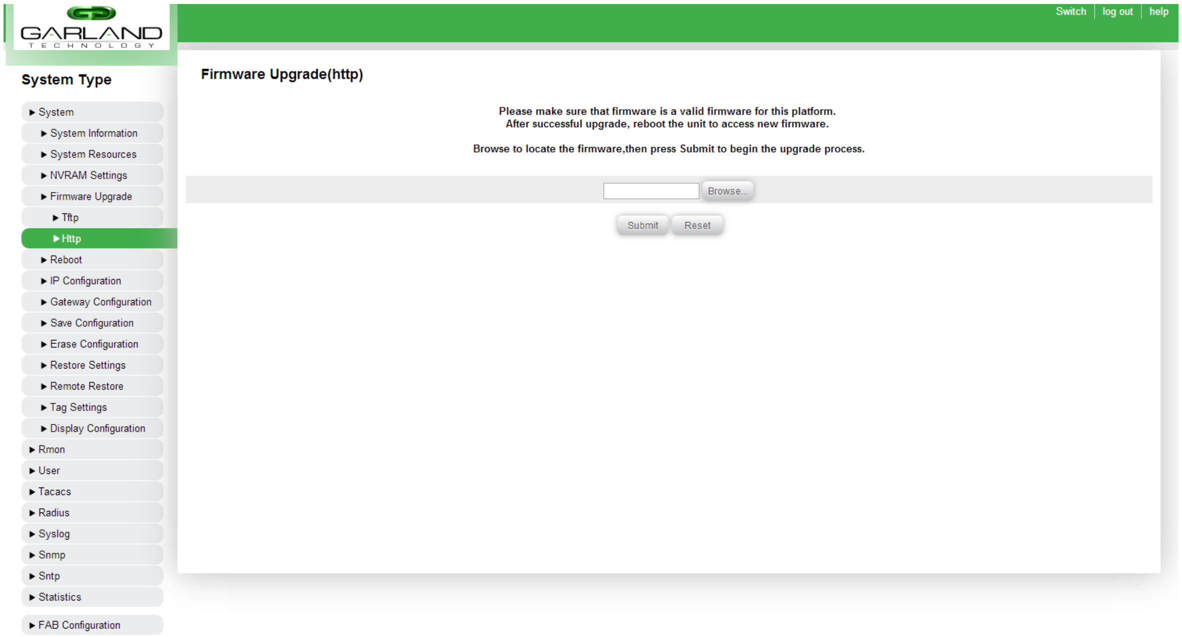
Address Type: This drop-down list allows the user to select the address type of the TFTP server. Currently, the only option present is "IPv4".

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.

4.5 FIRMWARE UPGRADE (HTTP)



Firmware Upgrade(http)

Please make sure that firmware is a valid firmware for this platform.
After successful upgrade, reboot the unit to access new firmware.

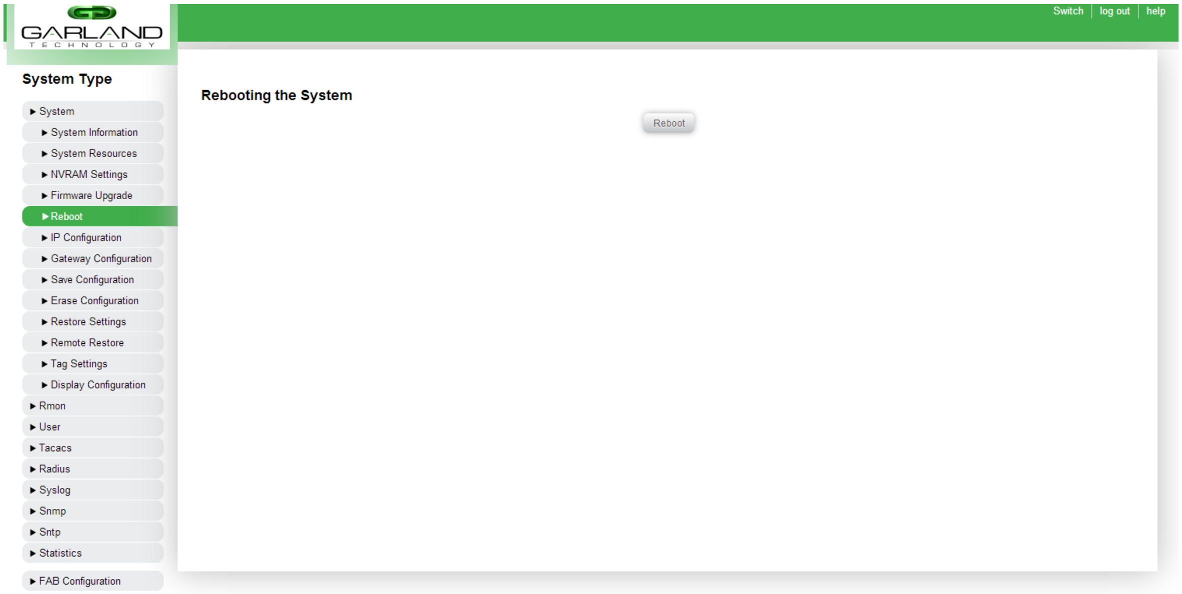
Browse to locate the firmware,then press Submit to begin the upgrade process.

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.

4.6 Reboot



Rebooting the System

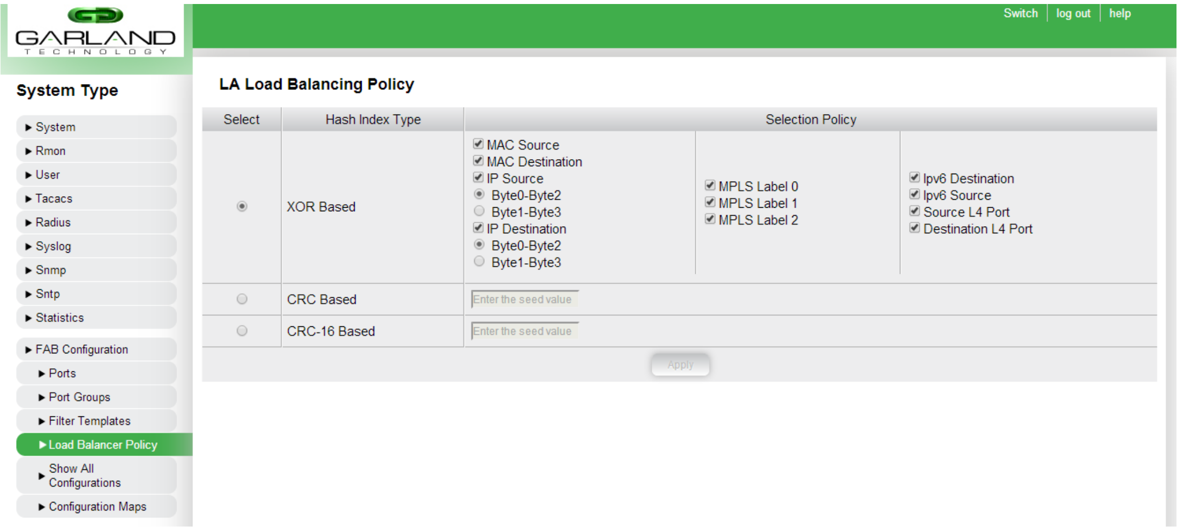
Reboot

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.

4.7 Load Balancer Policy



LA Load Balancing Policy

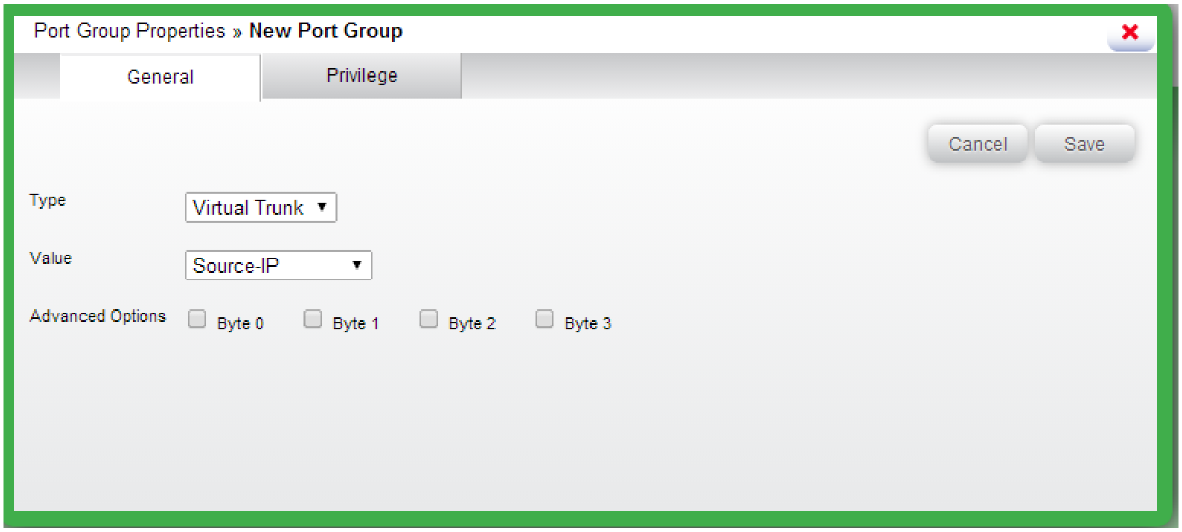
Select	Hash Index Type	Selection Policy		
●	XOR Based	☑ MAC Source ☑ MAC Destination ☑ IP Source ● Byte0-Byte2 ○ Byte1-Byte3 ☑ IP Destination ● Byte0-Byte2 ○ Byte1-Byte3	☑ MPLS Label 0 ☑ MPLS Label 1 ☑ MPLS Label 2	☑ Ipv6 Destination ☑ Ipv6 Source ☑ Source L4 Port ☑ Destination L4 Port
○	CRC Based	Enter the seed value		
○	CRC-16 Based	Enter the seed value		

Apply

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.

4.7.1 Virtual Trunk Balancing Policy



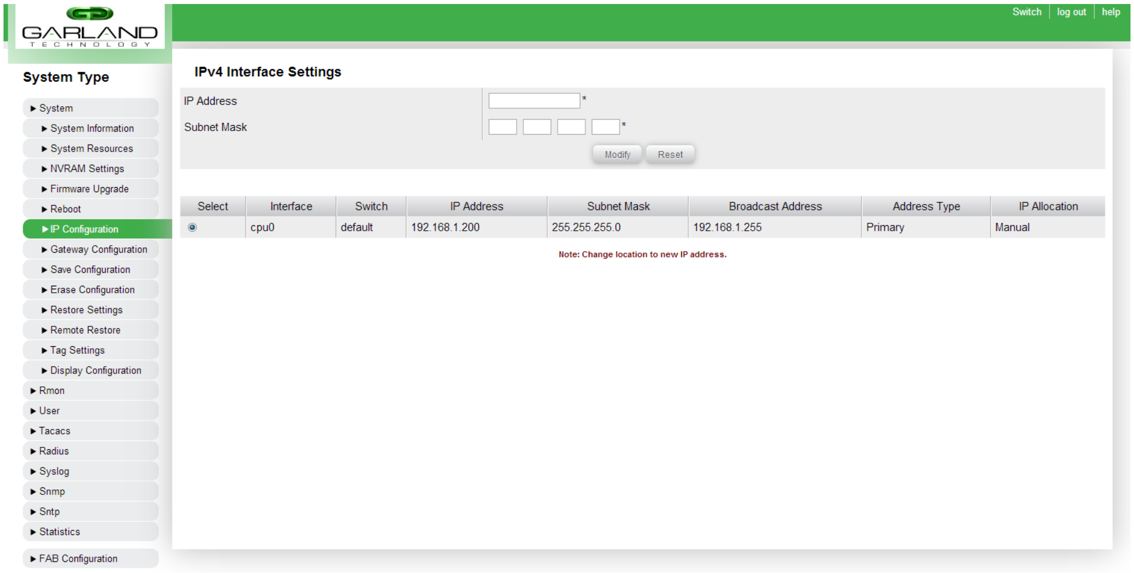
Port Group Properties » New Port Group

Type	Virtual Trunk ▼
Value	Source-IP ▼
Advanced Options	□ Byte 0 □ Byte 1 □ Byte 2 □ Byte 3

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.

4.8 IP Configuration



IPv4 Interface Settings

IP Address	*
Subnet Mask	*

Select	Interface	Switch	IP Address	Subnet Mask	Broadcast Address	Address Type	IP Allocation
●	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

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 load balancing policy is global for the whole device.

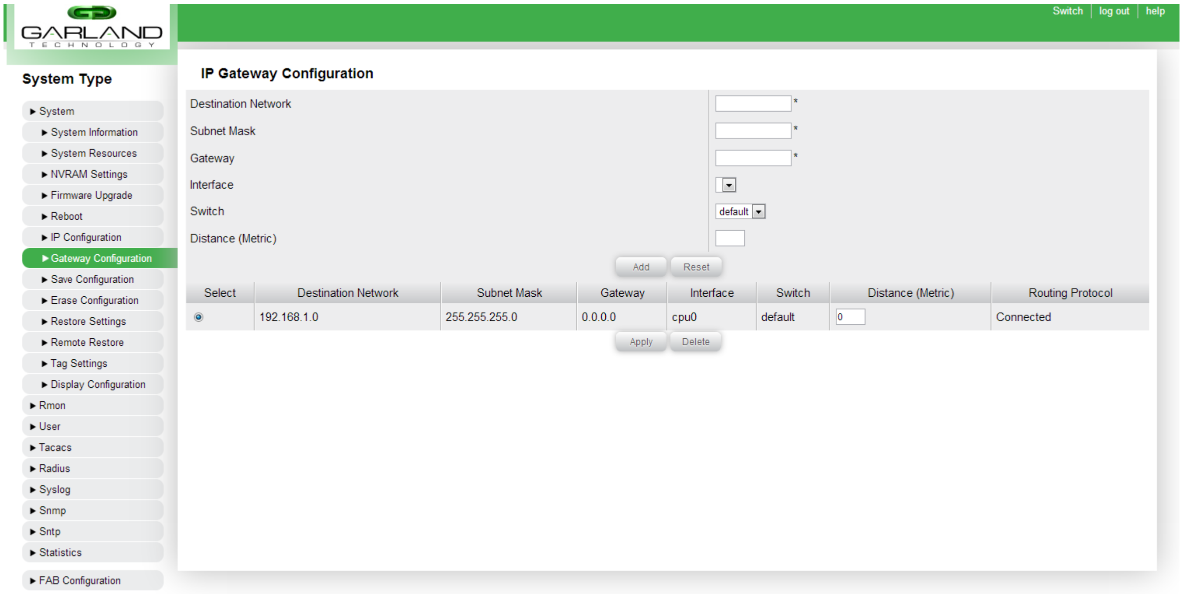
Note: Settings from the "**IP Configuration**" page will take precedence over settings configured in "**NVRAM Settings**".

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.

4.9 Gateway Configuration



IP Gateway Configuration

Destination Network	*
Subnet Mask	*
Gateway	*
Interface	
Switch	default
Distance (Metric)	

Select	Destination Network	Subnet Mask	Gateway	Interface	Switch	Distance (Metric)	Routing Protocol
●	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.

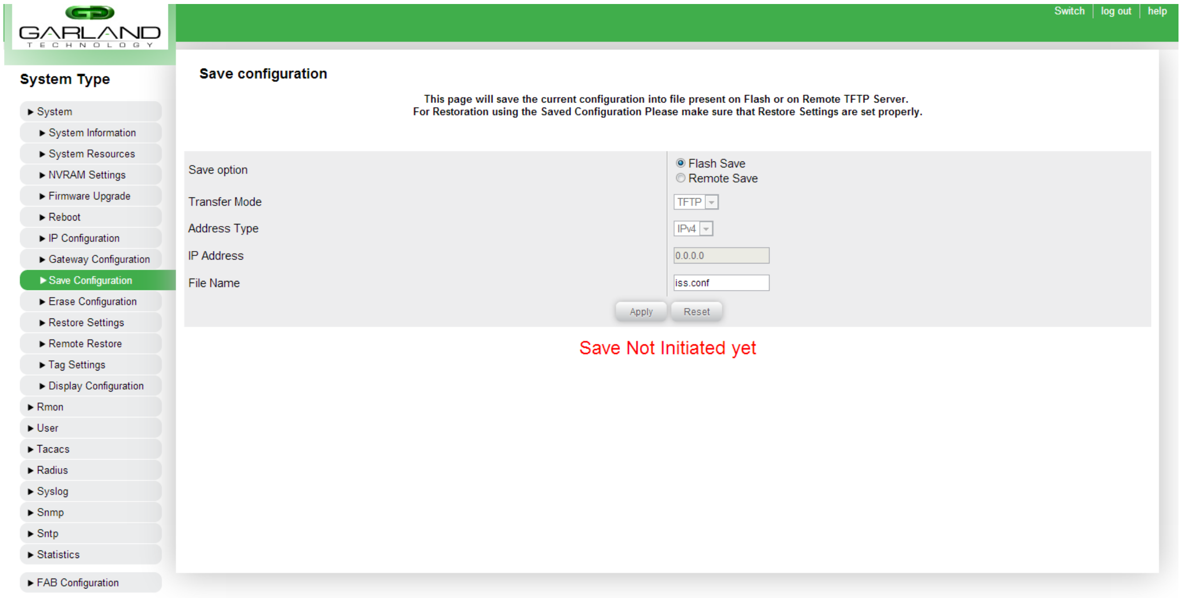
Switch: This field is not applicable on this platform.

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

4.10 Save Configuration



Save configuration

This page will save the current configuration into file present on Flash or on Remote TFTP Server.
For Restoration using the Saved Configuration Please make sure that Restore Settings are set properly.

Save option	● Flash Save ○ Remote Save
Transfer Mode	TFTP
Address Type	IPv4
IP Address	0.0.0.0
File Name	iss.conf

Save Not Initiated yet

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.

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

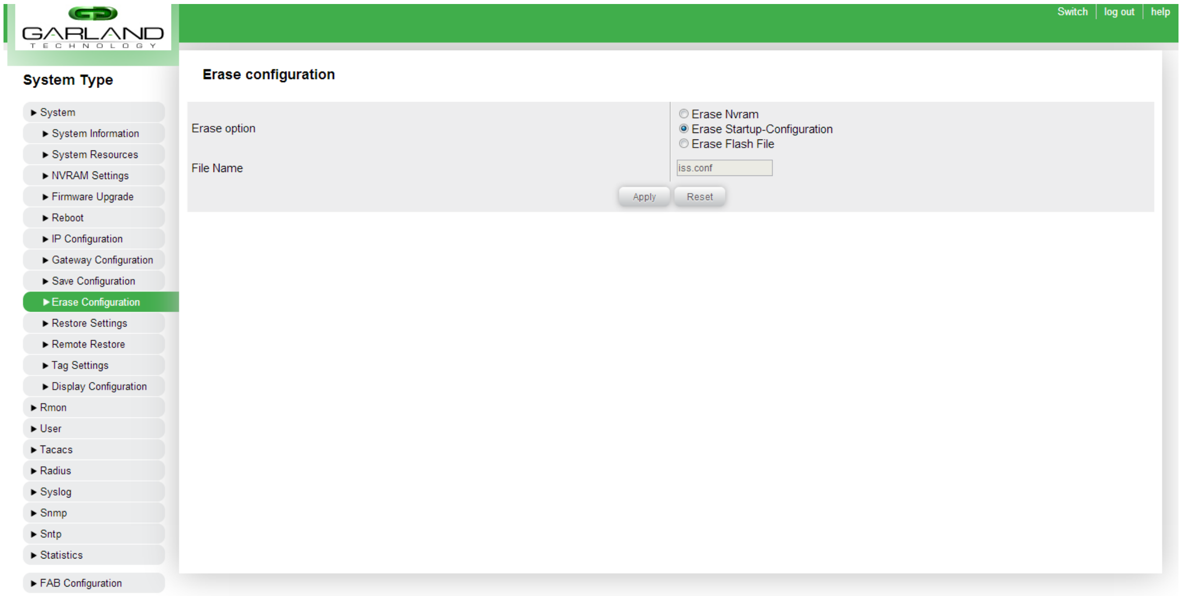
Address Type: Specifies whether the IP address specified in the "IP Address" field below is of type IPv4 or IPv6.

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, the 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 "Save option" specified above.

4.11 Erase Configuration



Erase configuration

Erase option	○ Erase Nvram ● Erase Startup-Configuration ○ Erase Flash File
File Name	iss.conf

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 "iss.conf".

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

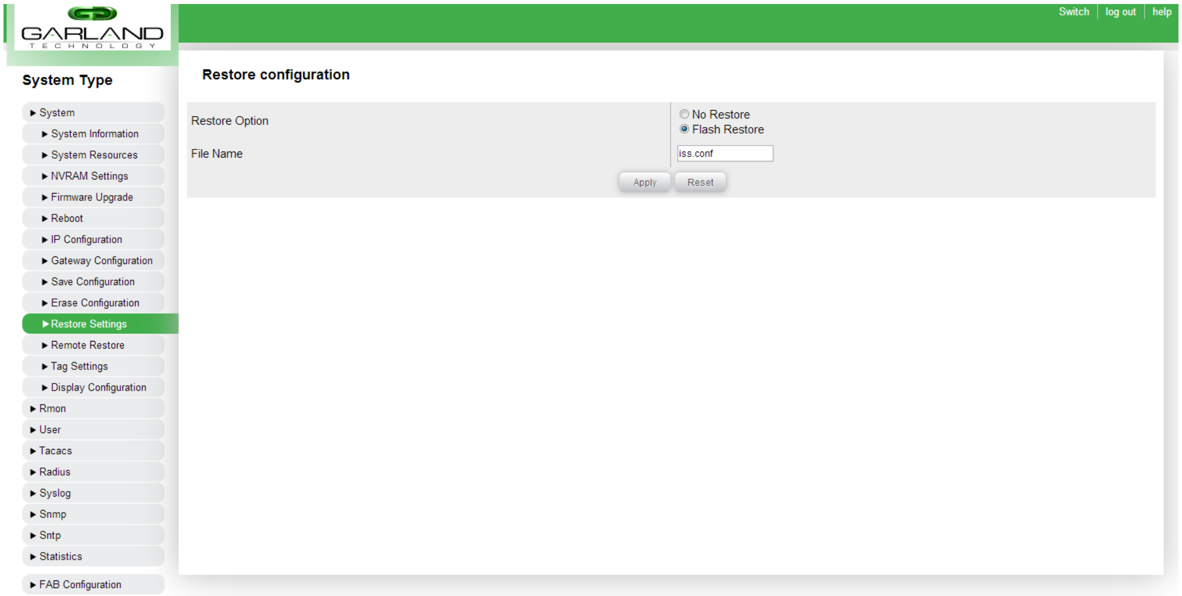
-Erase Startup-Configuration: Selecting this option will erase the existing startup-configuration that is written to the device's flash memory.

-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 "iss.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 "iss.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.

4.12 RESTORE SETTINGS



Restore configuration

Restore Option	○ No Restore ● Flash Restore
File Name	iss.conf

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:

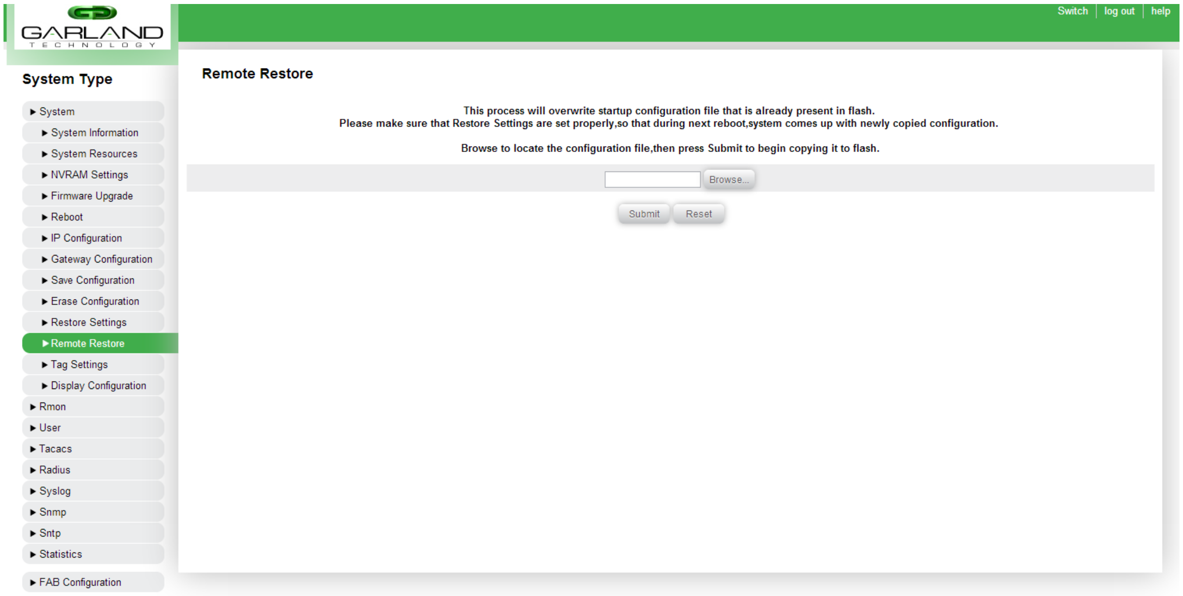
-No Restore: Users may select this option if they do not want the saved configuration to be restored upon boot.

-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 "iss.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 "iss.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.

4.13 REMOTE RESTORE



Remote Restore

This process will overwrite startup configuration file that is already present in flash.
Please make sure that Restore Settings are set properly,so that during next reboot,system comes up with newly copied configuration.

Browse to locate the configuration file,then press Submit to begin copying it to flash.

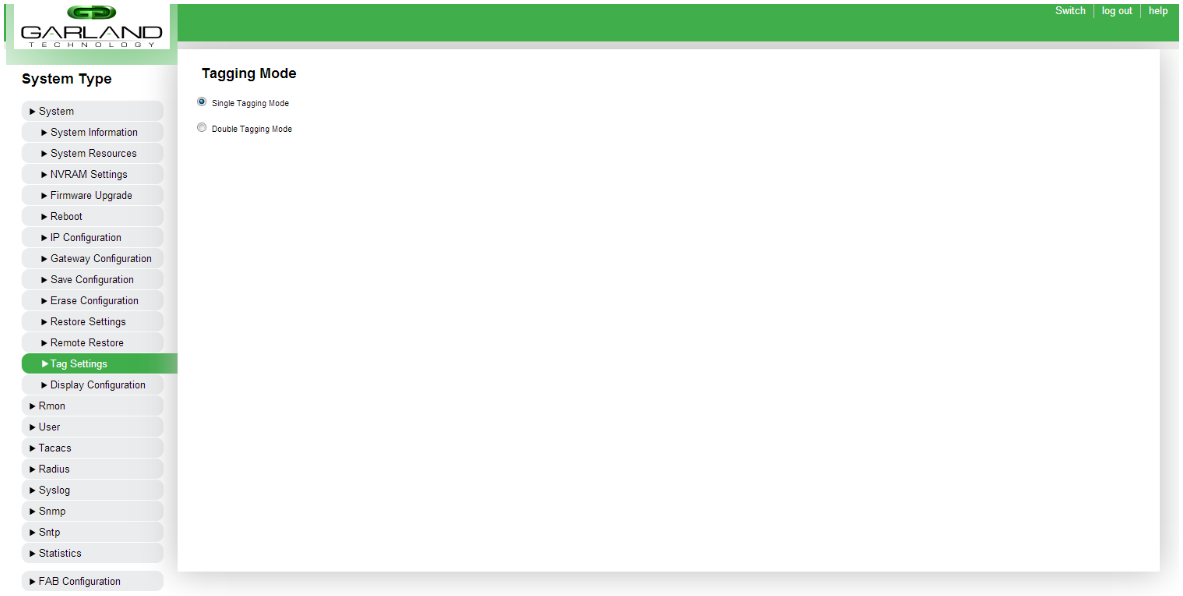
Figure 16: Remote Restore

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).

4.14 TAG SETTINGS



Tagging Mode

● Single Tagging Mode

○ Double Tagging Mode

Figure 17: Tagging Mode

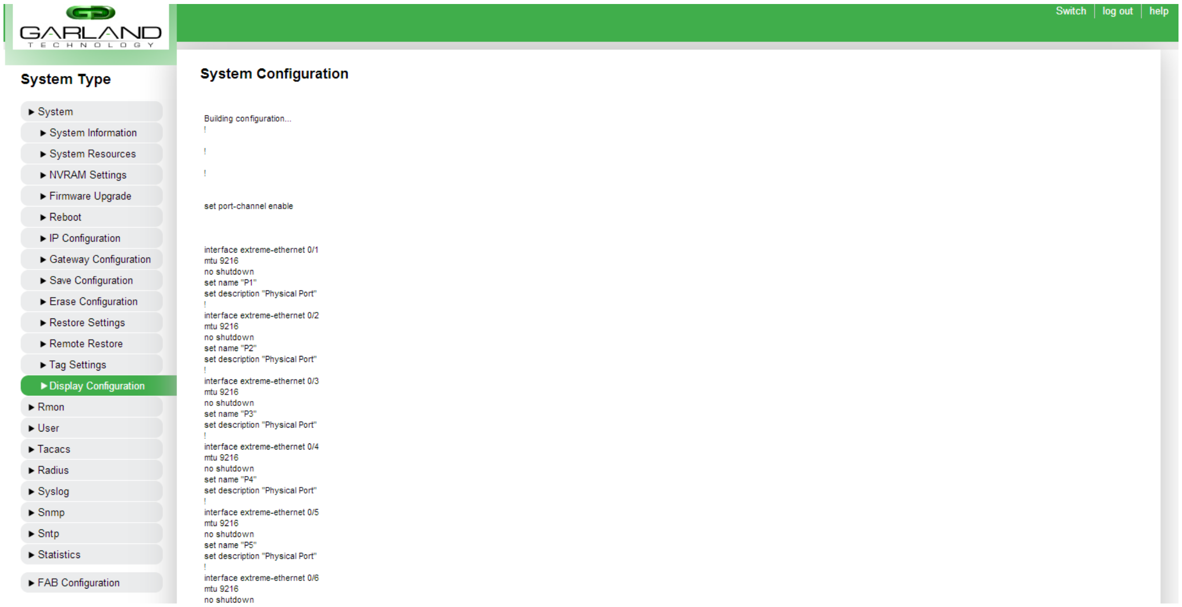
The unit can be configured to remove a single VLAN tag or two VLAN tags.

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

Double Tagging Mode: When this option is selected, any filters that use the "Strip vlan" advanced action (see screenshot below) 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.

4.15 DISPLAY CONFIGURATION



System Configuration

```
Building configuration...
!

!

!


set port-channel enable



interface extreme-ethernet 0/1
mtu 9216
no shutdown
set name "P1"
set description "Physical Port"
!
interface extreme-ethernet 0/2
mtu 9216
no shutdown
set name "P2"
set description "Physical Port"
!
interface extreme-ethernet 0/3
mtu 9216
no shutdown
set name "P3"
set description "Physical Port"
!
interface extreme-ethernet 0/4
mtu 9216
no shutdown
set name "P4"
set description "Physical Port"
!
interface extreme-ethernet 0/5
mtu 9216
no shutdown
set name "P5"
set description "Physical Port"
!
interface extreme-ethernet 0/6
mtu 9216
no shutdown
```

Figure 18: System Configuration

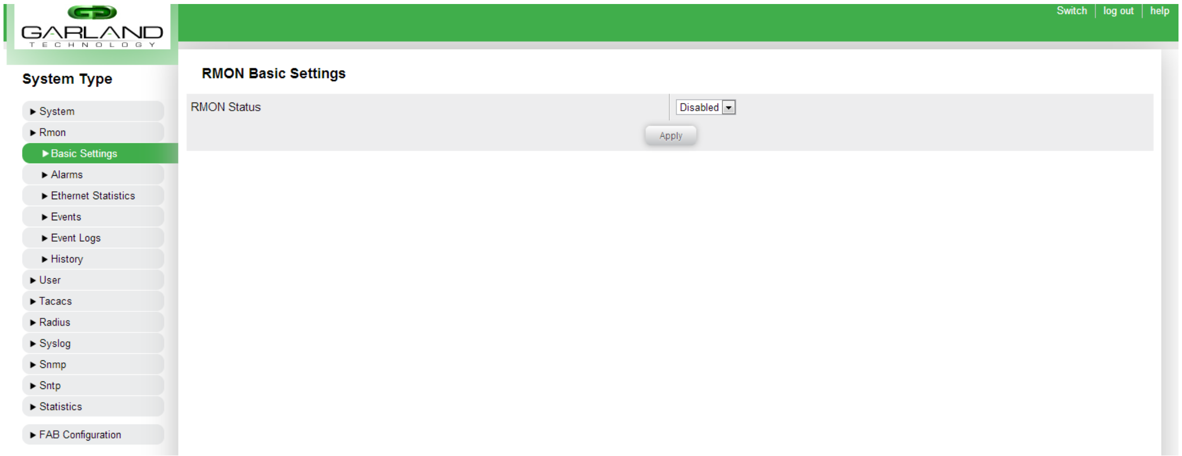
The entire running configuration is now viewable in the web GUI. This is equivalent to “show running-config” in the CLI.

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



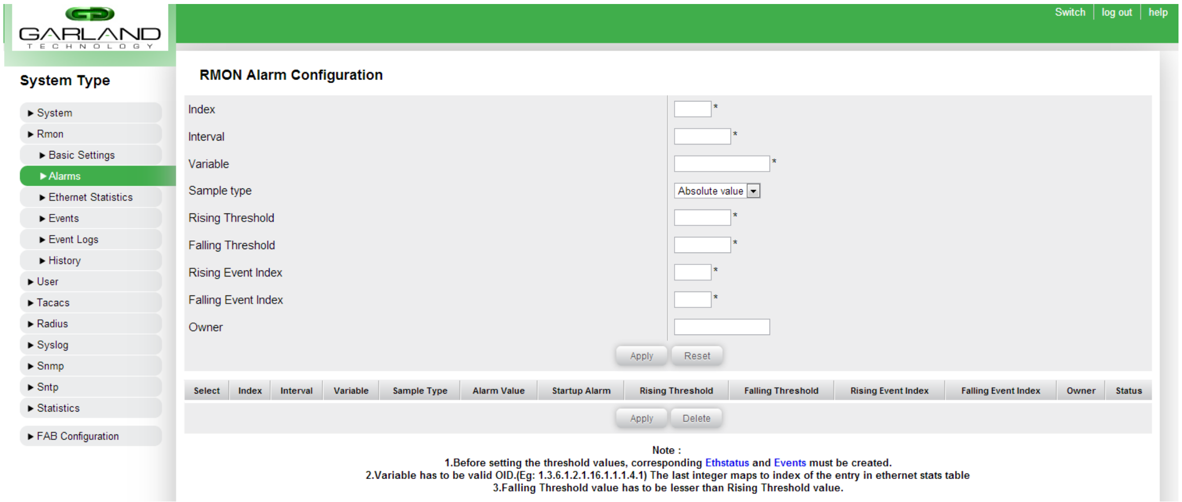
RMON Basic Settings

RMON Status	Disabled

Figure 19: RMON Basics

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

5.2 RMON ALARMS



RMON Alarm Configuration

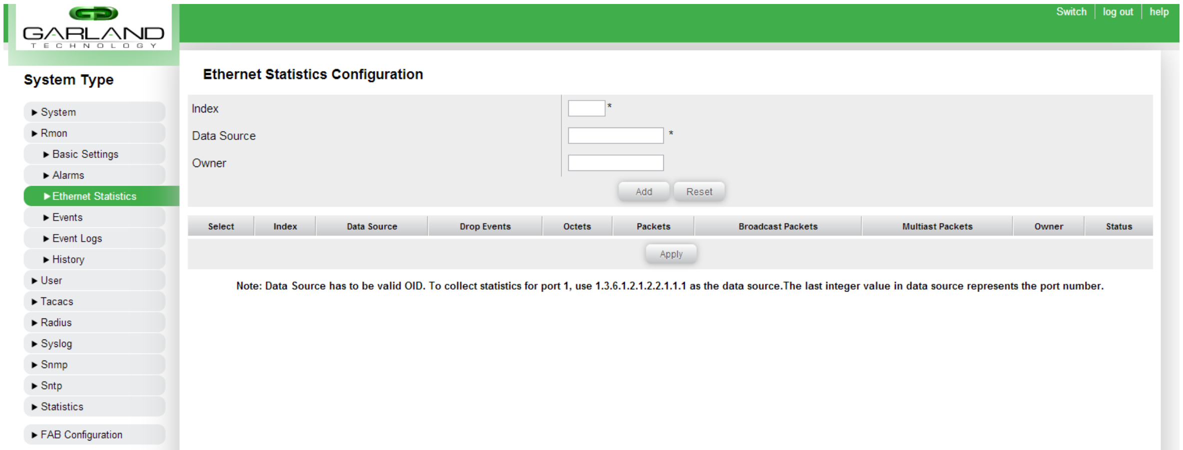
Index	*
Interval	*
Variable	*
Sample type	Absolute value
Rising Threshold	*
Falling Threshold	*
Rising Event Index	*
Falling Event Index	*
Owner	

Select	Index	Interval	Variable	Sample Type	Alarm Value	Startup Alarm	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Status

Note :
1.Before setting the threshold values, corresponding Ethstatus and Events must be created.
2.Variable has to be valid OID.(Eg: 1.3.6.1.2.1.16.1.1.1.4.1) The last integer maps to index of the entry in ethernet stats table
3.Falling Threshold value has to be lesser than Rising Threshold value.

Figure 20: RMON Alarms

5.3 RMON Ethernet Statistics



Ethernet Statistics Configuration

Index	*
Data Source	*
Owner	

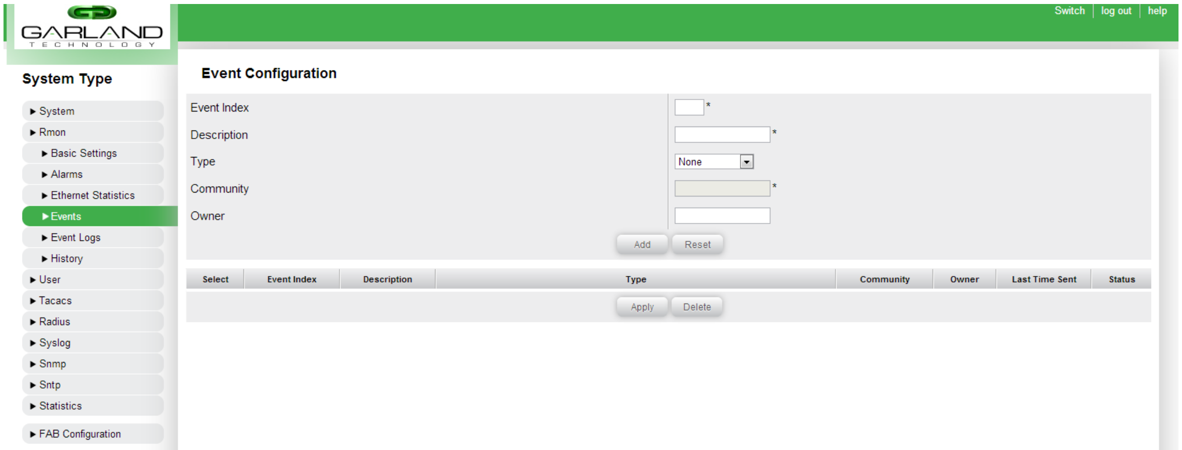
Select	Index	Data Source	Drop Events	Octets	Packets	Broadcast Packets	Multiast Packets	Owner	Status

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



Event Configuration

Event Index	*
Description	*
Type	None
Community	*
Owner	

Select	Event Index	Description	Type	Community	Owner	Last Time Sent	Status

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

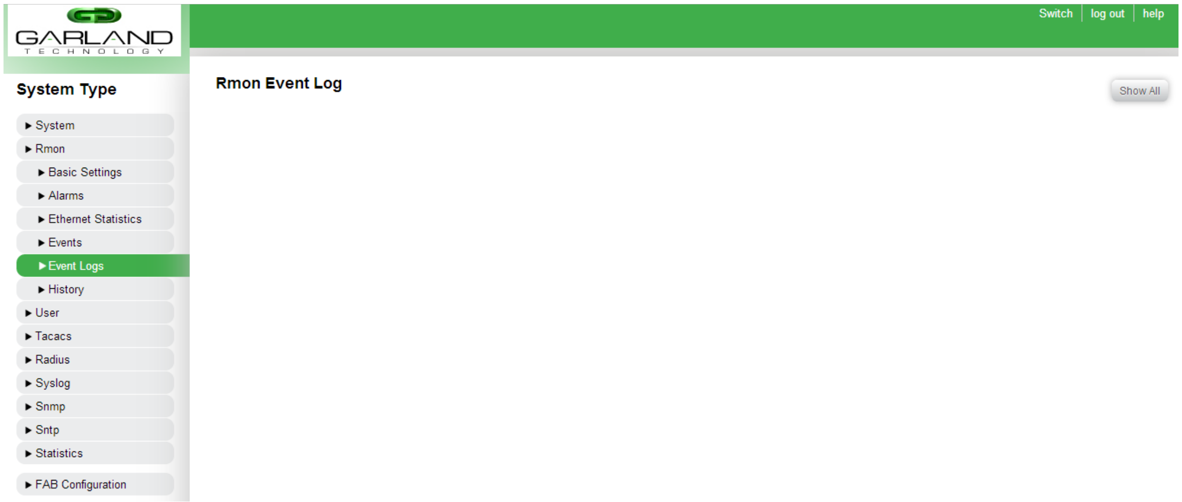
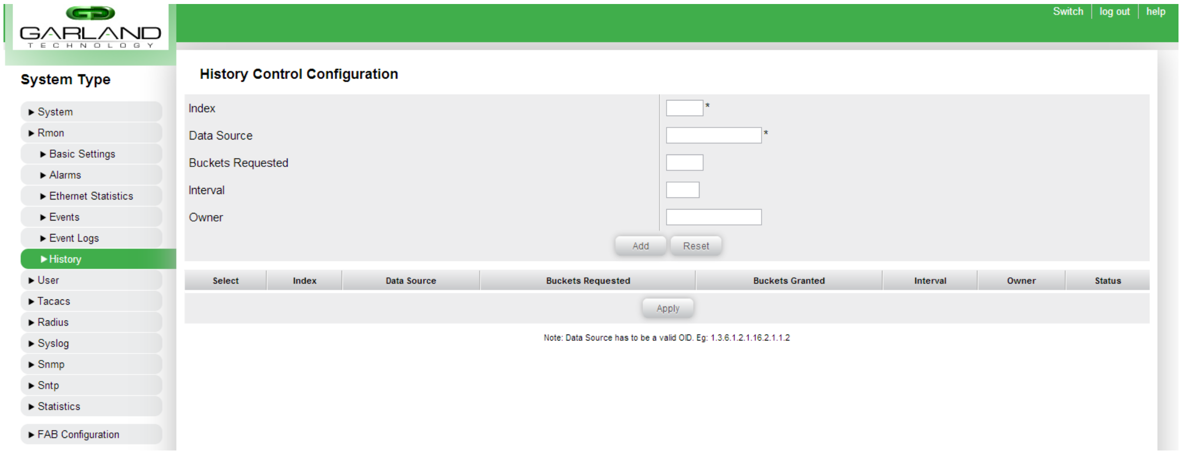


Figure 23: RMON Event Logs

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

5.6 RMON History



Select	Index	Data Source	Buckets Requested	Buckets Granted	Interval	Owner	Status

Note: Data Source has to be a valid OID. Eg: 1.3.6.1.2.1.16.2.1.1.2

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.

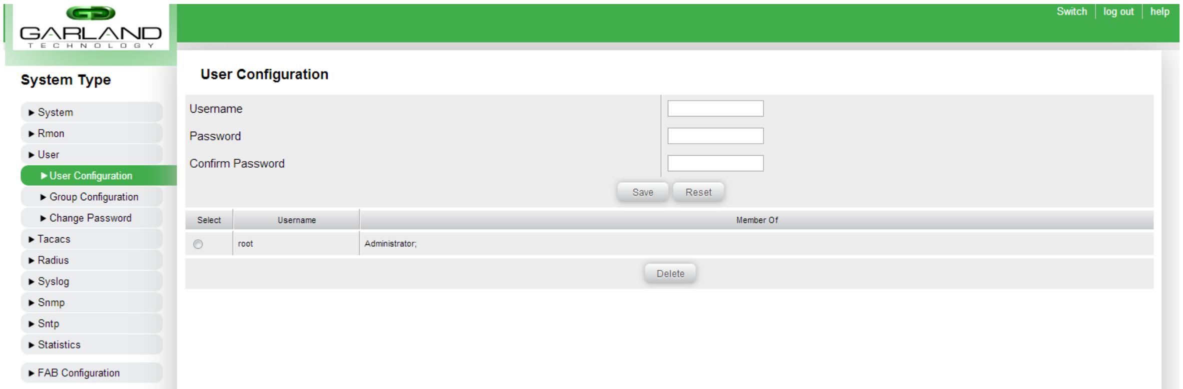
Owner: This field allows the user to specify the creator of the RMON History entry to be created.

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



User Configuration

Username	
Password	
Confirm Password	

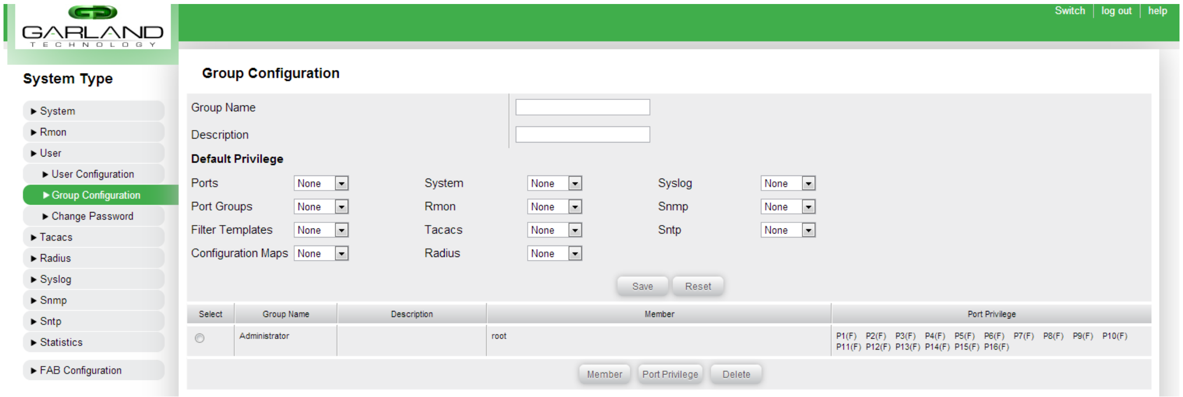
Select	Username	Member Of
○	root	Administrator;

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



Group Configuration

Group Name	
Description	

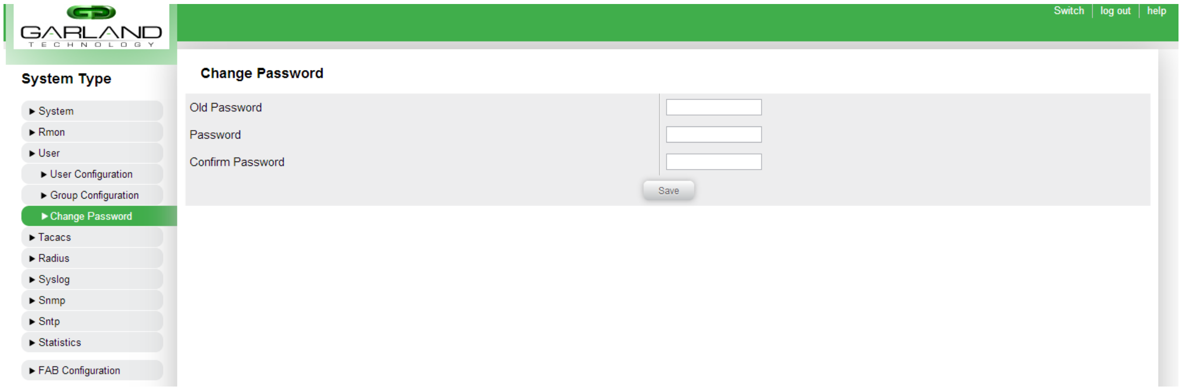
Default Privilege

Ports	None	System	None	Syslog	None
Port Groups	None	Rmon	None	Snmp	None
Filter Templates	None	Tacacs	None	Sntp	None
Configuration Maps	None	Radius	None		

Select	Group Name	Description	Member	Port Privilege
○	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

6.3 User Change Password



Change Password

Old Password	
Password	
Confirm Password	

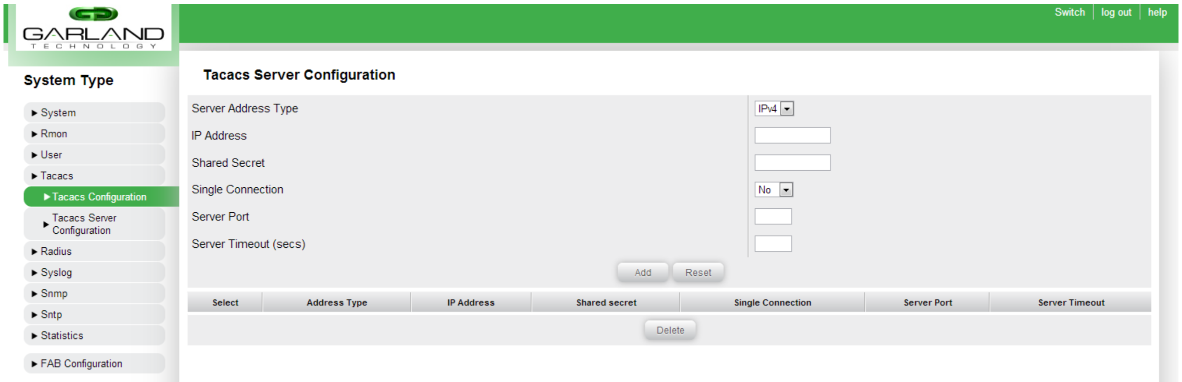
Figure 27: Change Password

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



Tacacs Server Configuration

Server Address Type	IPv4
IP Address	
Shared Secret	
Single Connection	No
Server Port	
Server Timeout (secs)	

Select	Address Type	IP Address	Shared secret	Single Connection	Server Port	Server Timeout

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 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.

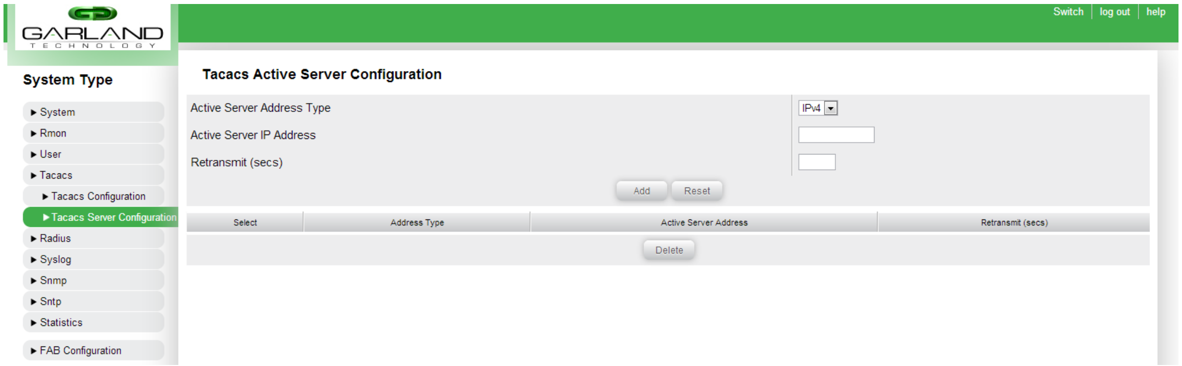
Note: the remote TACACS server must support single connection mode in order for this setting to function.

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



Tacacs Active Server Configuration

Active Server Address Type	IPv4
Active Server IP Address	
Retransmit (secs)	

Select	Address Type	Active Server Address	Retransmit (secs)

Figure 29: TACACS Active 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.

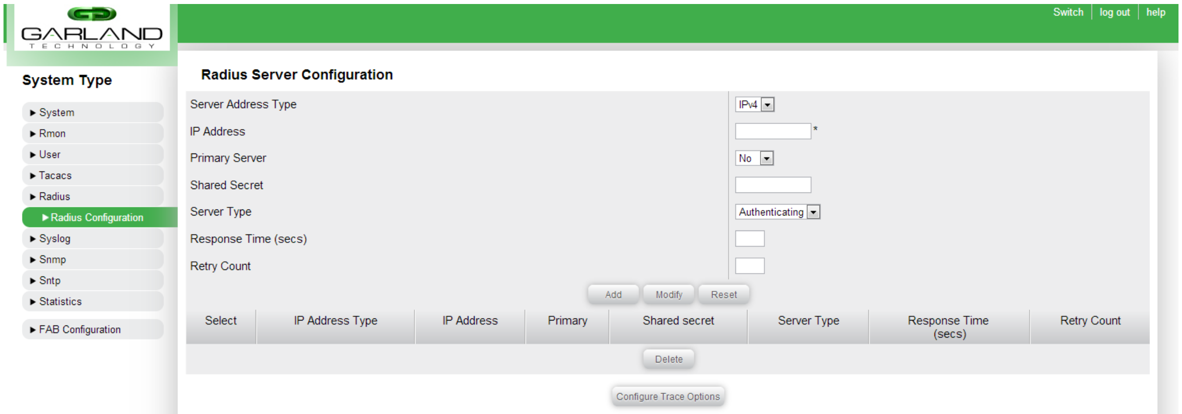
Retransmit: This field allows the user to specify how often the device will send an authentication request to the TACACS server if the server does not respond. Units are in seconds.

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



Radius Server Configuration

Server Address Type	IPv4
IP Address	*
Primary Server	No
Shared Secret	
Server Type	Authenticating
Response Time (secs)	
Retry Count	

Select	IP Address Type	IP Address	Primary	Shared secret	Server Type	Response Time (secs)	Retry Count

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.

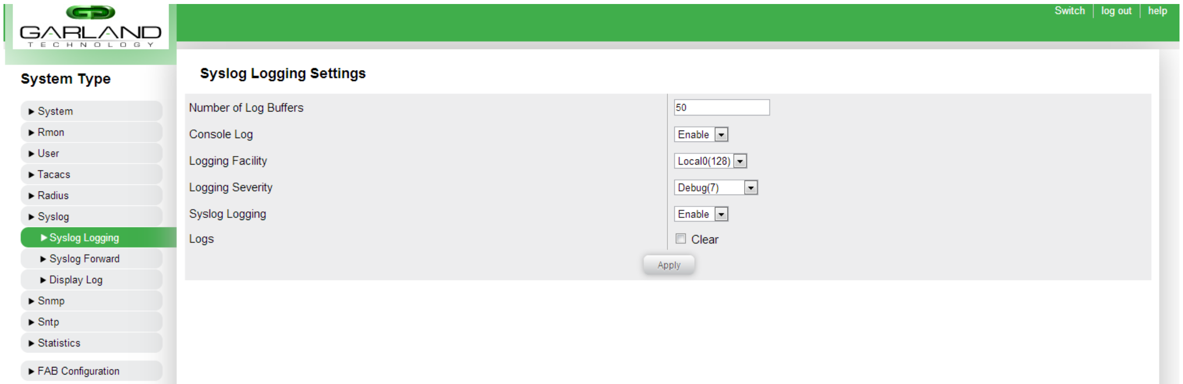
Response Time: Users may specify the maximum response time for the Radius server. Units are in seconds.

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



Syslog Logging Settings

Number of Log Buffers	50
Console Log	Enable
Logging Facility	Local0(128)
Logging Severity	Debug(7)
Syslog Logging	Enable
Logs	□ Clear

Apply

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.

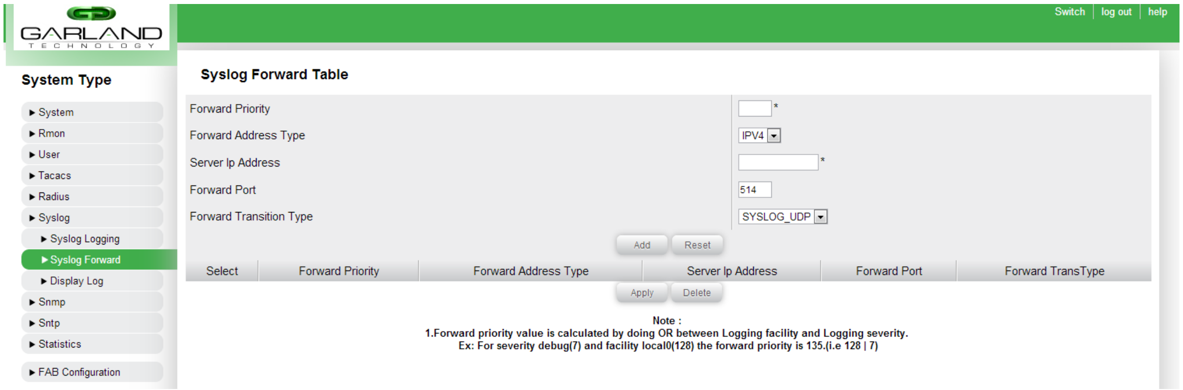
Logging Severity: This field specifies which messages should be logged to the syslog daemon. Available options are as follows:

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	IPV4 ▾
Server Ip Address	*
Forward Port	514
Forward Transition Type	SYSLOG_UDP ▾

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.

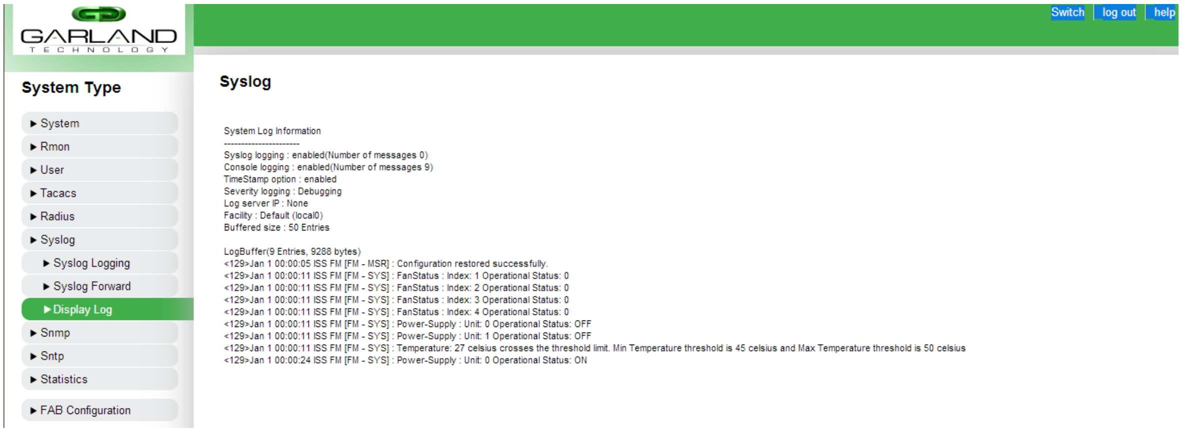
Forward Transition Type: This field specifies the protocol in which the device will send messages to the syslog server. Currently, the UDP protocol is supported.

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



```
System Log Information
-----------------------
Syslog logging : enabled(Number of messages 0)
Console logging : enabled(Number of messages 9)
TimeStamp option : enabled
Severity logging : Debugging
Log server IP : None
Facility : Default (local0)
Buffered size : 50 Entries

LogBuffer(9 Entries, 9288 bytes)
<129>Jan 1 00:00:05 ISS FM [FM - MSR] : Configuration restored successfully.
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : FanStatus : Index: 1 Operational Status: 0
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : FanStatus : Index: 2 Operational Status: 0
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : FanStatus : Index: 3 Operational Status: 0
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : FanStatus : Index: 4 Operational Status: 0
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : Power-Supply : Unit: 0 Operational Status: OFF
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : Power-Supply : Unit: 1 Operational Status: OFF
<129>Jan 1 00:00:11 ISS FM [FM - SYS] : Temperature: 27 celsius crosses the threshold limit. Min Temperature threshold is 45 celsius and Max Temperature threshold is 50 celsius
<129>Jan 1 00:00:24 ISS FM [FM - SYS] : Power-Supply : Unit: 0 Operational Status: ON
```

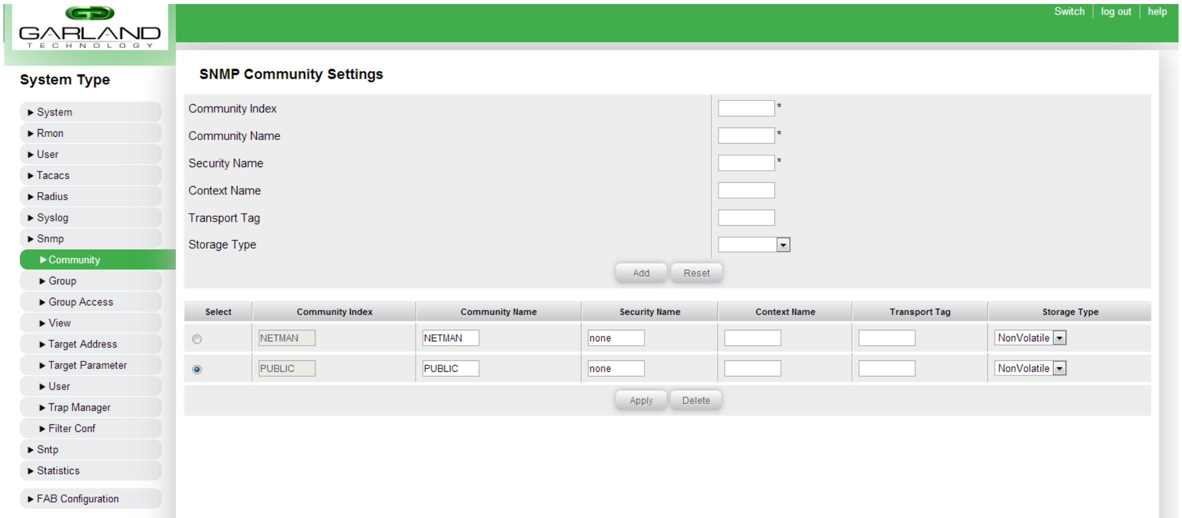
Figure 33: Syslog Display Log

This page shows the system log information.

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



SNMP Community Settings

Community Index	*
Community Name	*
Security Name	*
Context Name	
Transport Tag	
Storage Type	

Select	Community Index	Community Name	Security Name	Context Name	Transport Tag	Storage Type
○	NETMAN	NETMAN	none			NonVolatile
●	PUBLIC	PUBLIC	none			NonVolatile

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.

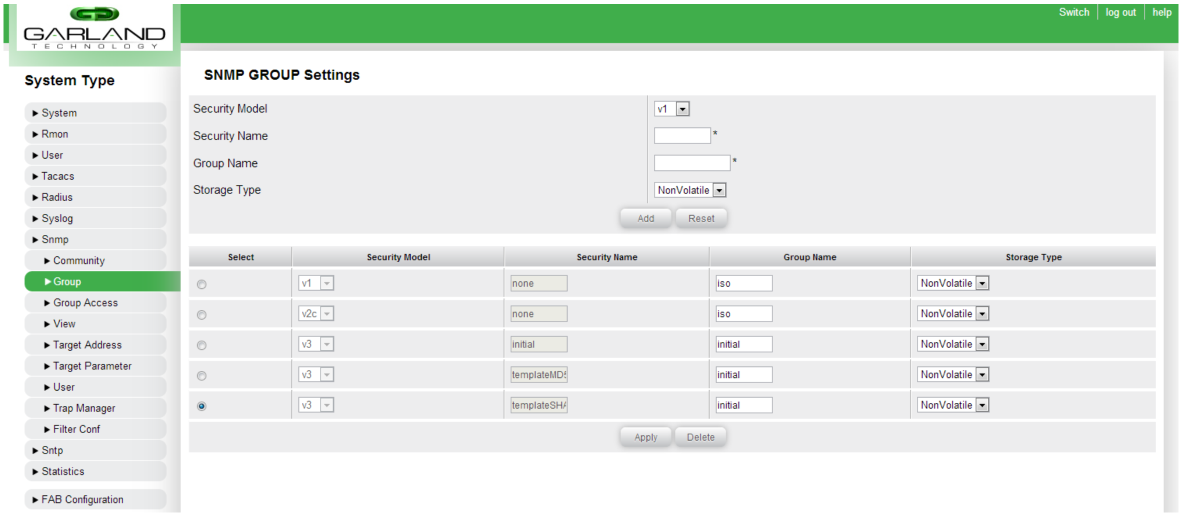
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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



SNMP GROUP Settings

Security Model	v1
Security Name	*
Group Name	*
Storage Type	NonVolatile

Select	Security Model	Security Name	Group Name	Storage Type
○	v1	none	iso	NonVolatile
○	v2c	none	iso	NonVolatile
○	v3	initial	initial	NonVolatile
○	v3	templateMD5	initial	NonVolatile
●	v3	templateSHA	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.

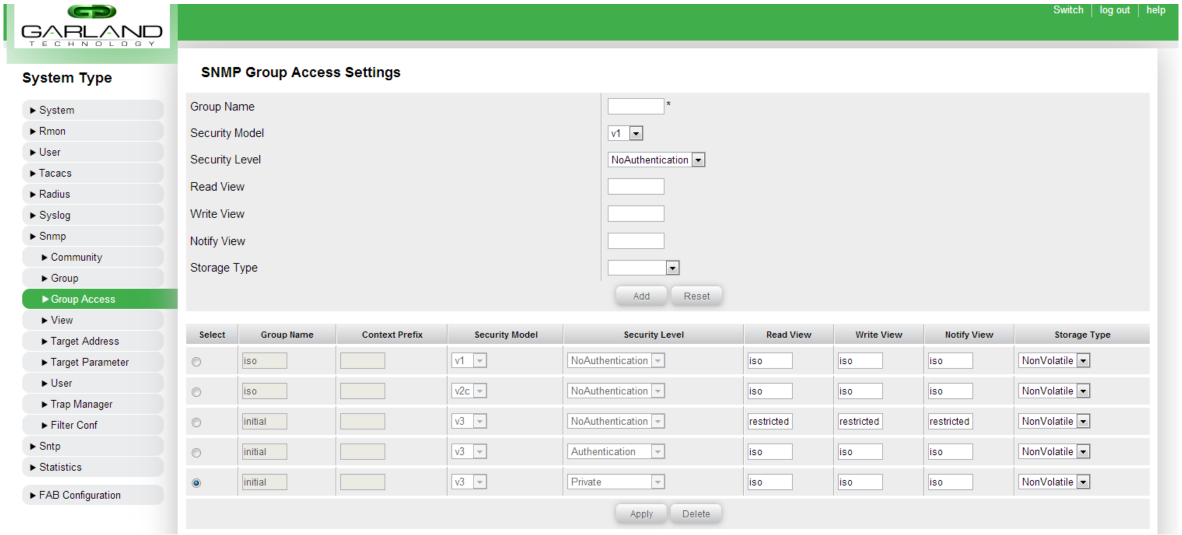
2. **–NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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



SNMP Group Access Settings

Group Name	*
Security Model	v1
Security Level	NoAuthentication
Read View	
Write View	
Notify View	
Storage Type	

Select	Group Name	Context Prefix	Security Model	Security Level	Read View	Write View	Notify View	Storage Type
○	iso		v1	NoAuthentication	iso	iso	iso	NonVolatile
○	iso		v2c	NoAuthentication	iso	iso	iso	NonVolatile
○	initial		v3	NoAuthentication	restricted	restricted	restricted	NonVolatile
○	initial		v3	Authentication	iso	iso	iso	NonVolatile
●	initial		v3	Private	iso	iso	iso	NonVolatile

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:

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.

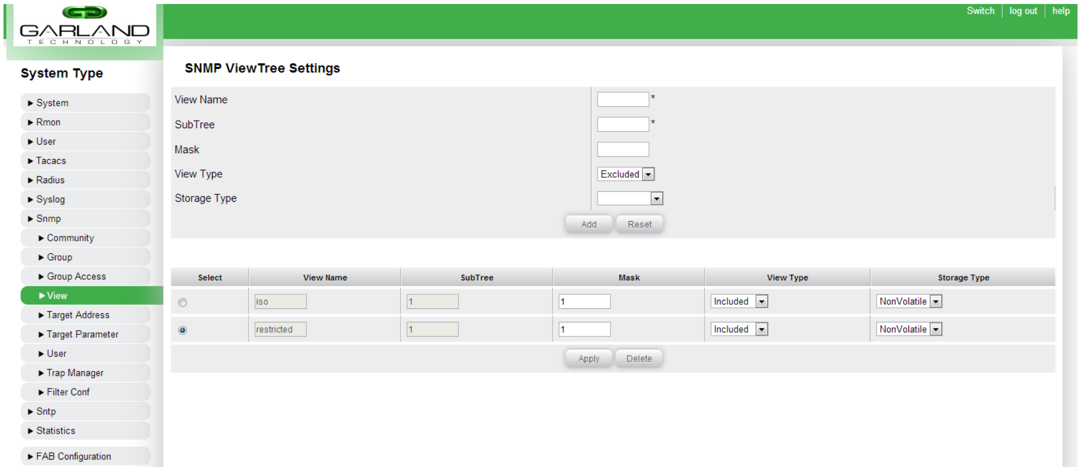
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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	Excluded
Storage Type	

Select	View Name	SubTree	Mask	View Type	Storage Type
○	iso	1	1	Included	NonVolatile
●	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:

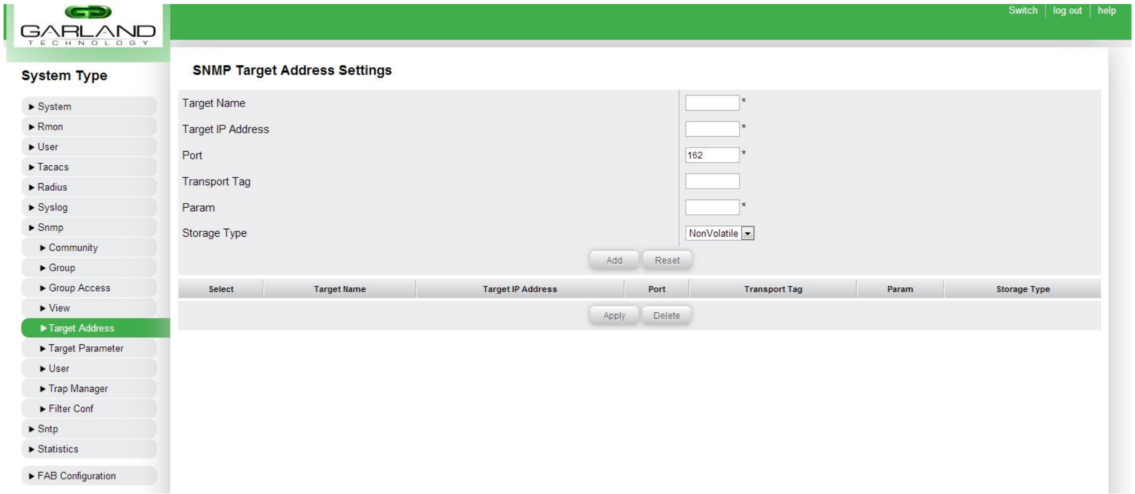
1. **-Volatile**: This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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



SNMP Target Address Settings

Target Name	*
Target IP Address	*
Port	162 *
Transport Tag	
Param	*
Storage Type	NonVolatile ▾

Select	Target Name	Target IP Address	Port	Transport Tag	Param	Storage Type

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.

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.

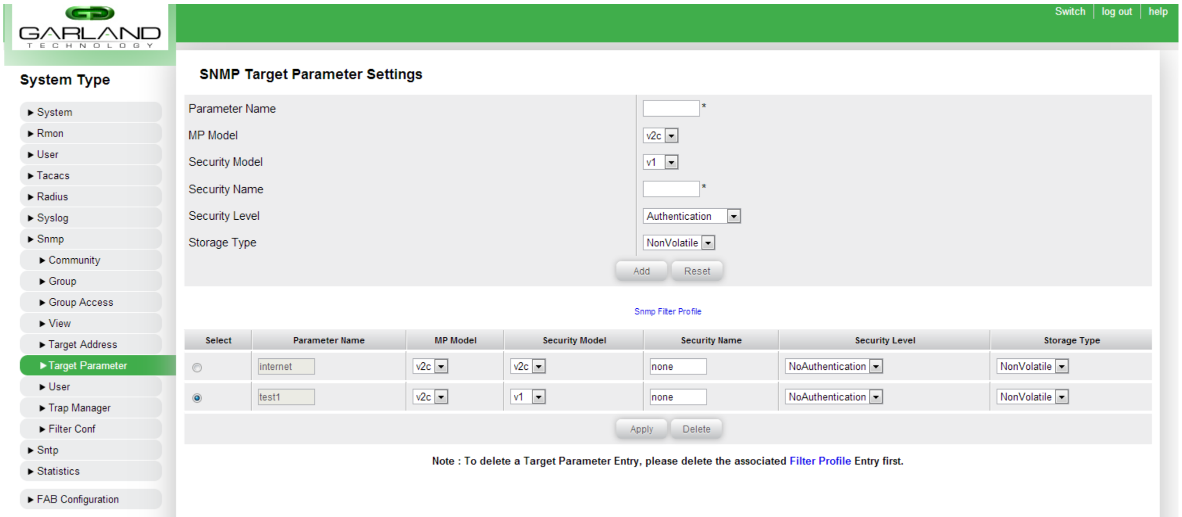
-NonVolatile: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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	v2c
Security Model	v1
Security Name	*
Security Level	Authentication
Storage Type	NonVolatile

Select	Parameter Name	MP Model	Security Model	Security Name	Security Level	Storage Type
○	internet	v2c	v2c	none	NoAuthentication	NonVolatile
●	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.

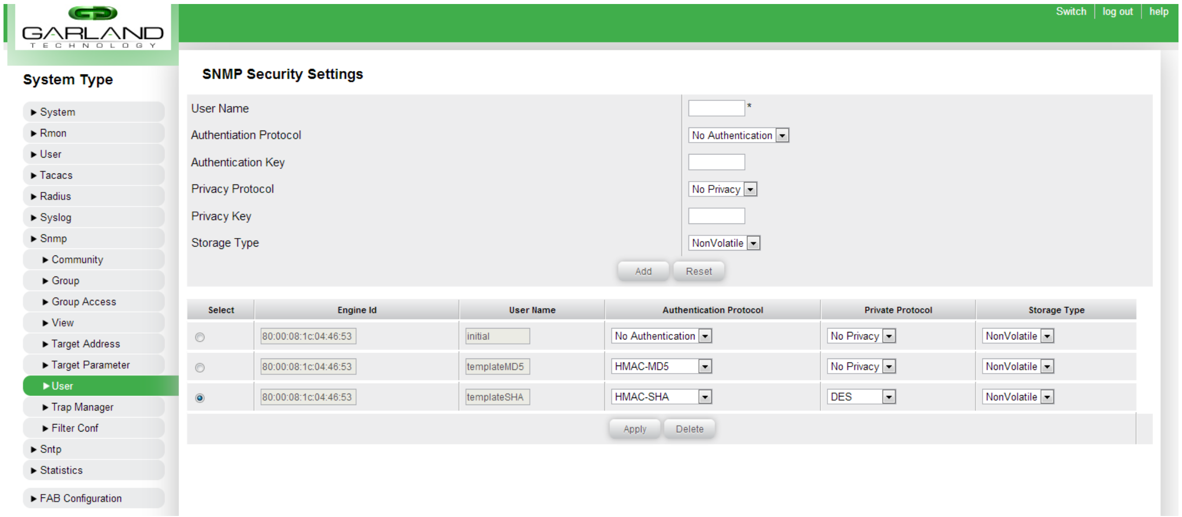
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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	*
Authentiation Protocol	No Authentication
Authentication Key	
Privacy Protocol	No Privacy
Privacy Key	
Storage Type	NonVolatile

Select	Engine Id	User Name	Authentication Protocol	Private Protocol	Storage Type
○	80:00:08:1c:04:46:53	initial	No Authentication	No Privacy	NonVolatile
○	80:00:08:1c:04:46:53	templateMD5	HMAC-MD5	No Privacy	NonVolatile
●	80:00:08:1c:04:46:53	templateSHA	HMAC-SHA	DES	NonVolatile

Figure 40: SNMP User

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:

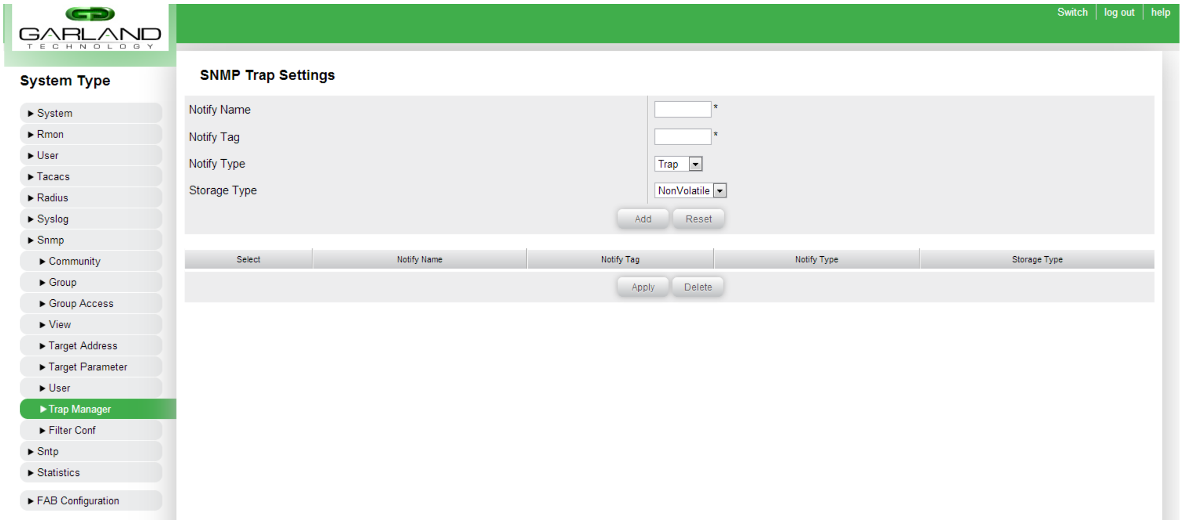
1. **-Volatile**: This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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



SNMP Trap Settings

Notify Name	*
Notify Tag	*
Notify Type	Trap
Storage Type	NonVolatile

Select	Notify Name	Notify Tag	Notify Type	Storage Type

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:

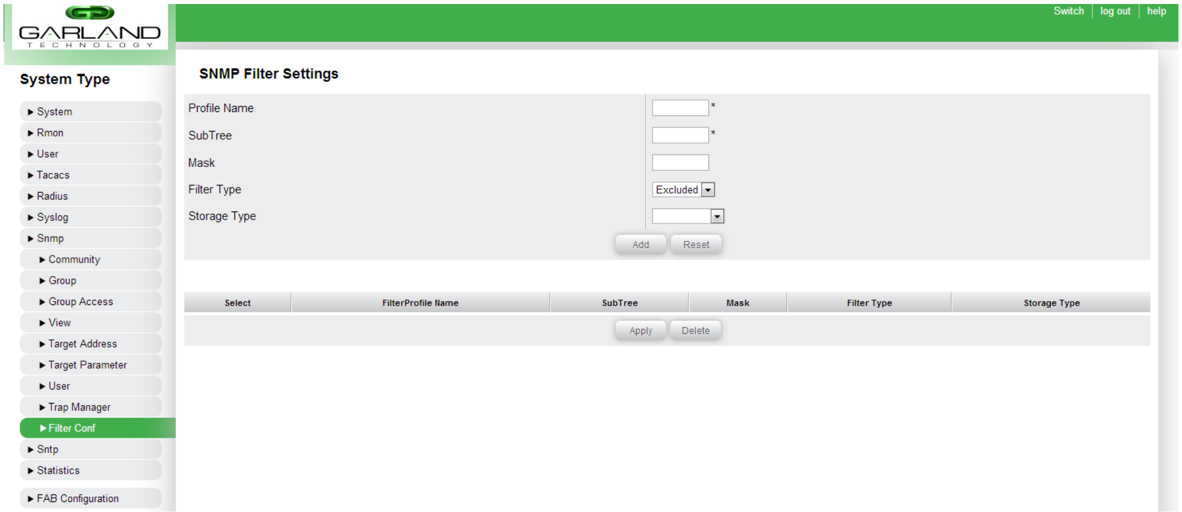
1. **-Volatile**: This storage type is temporary. The configuration setting will be erased upon restarting the device.
2. **-NonVolatile**: This storage type is permanent. The configuration setting will be saved upon restarting the device.

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



SNMP Filter Settings

Profile Name	*
SubTree	*
Mask	
Filter Type	Excluded
Storage Type	

Select	FilterProfile Name	SubTree	Mask	Filter Type	Storage Type

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.

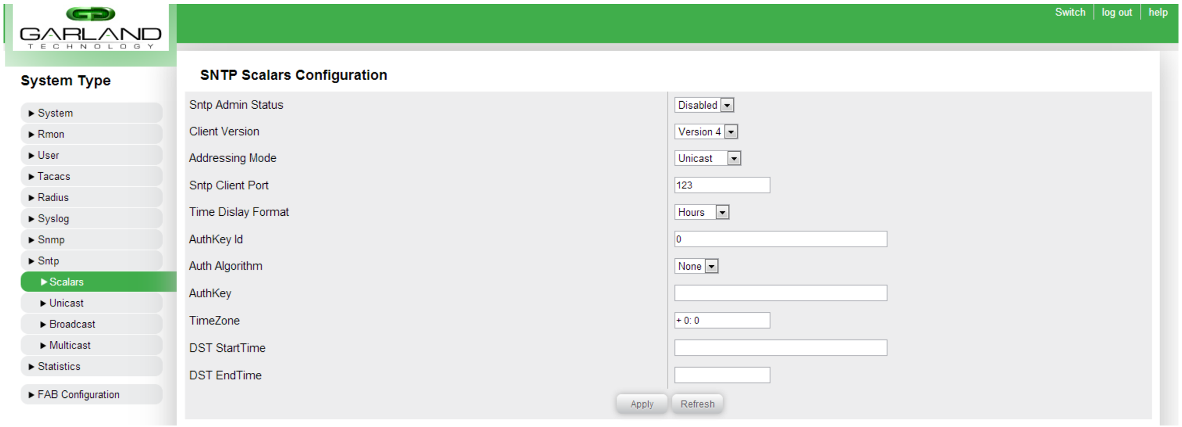
After the user enters values into the required fields on this page, the user may click the "Add" button to add the entered data into the SNMP filter table at the bottom of this page.

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 SCALARS



SNTP Scalars Configuration

Sntp Admin Status	Disabled
Client Version	Version 4
Addressing Mode	Unicast
Sntp Client Port	123
Time Dislay Format	Hours
AuthKey Id	0
Auth Algorithm	None
AuthKey	
TimeZone	+ 0: 0
DST StartTime	
DST EndTime	

Figure 43: 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.

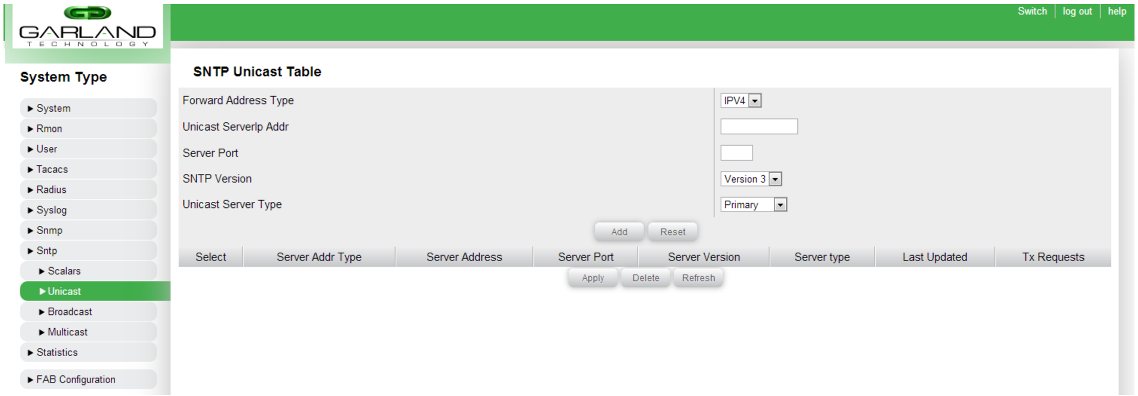
Auth Key: Specifies the authentication key that is used to implement NTP authentication.

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].

11.2 SNTP Unicast



SNTP Unicast Table

Forward Address Type	IPV4
Unicast ServerIp Addr	
Server Port	
SNTP Version	Version 3
Unicast Server Type	Primary

Select	Server Addr Type	Server Address	Server Port	Server Version	Server type	Last Updated	Tx Requests

Figure 44: Filter Configuration

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

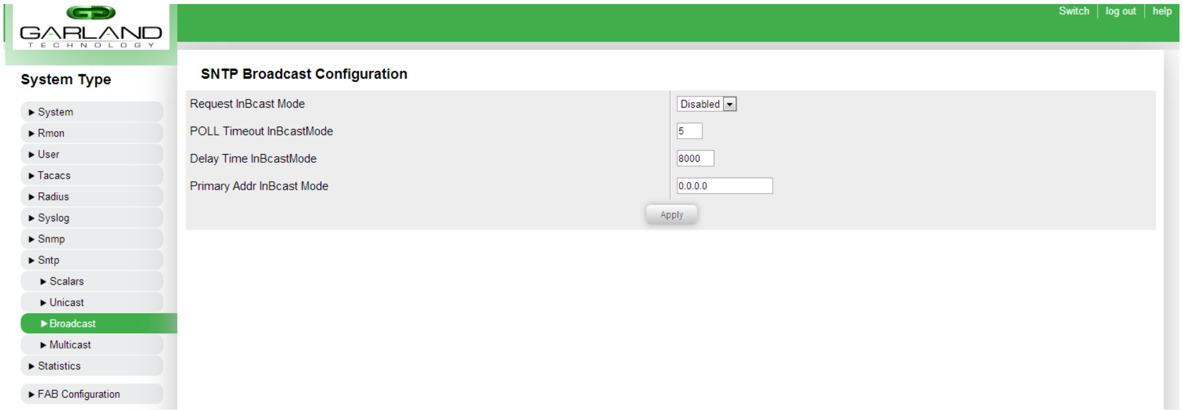
Unicast Server Type: This drop-down list allows the user to specify whether the SNTP server to be added will be used as a primary SNTP server or a secondary SNTP server.

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.

11.3 SNTP BROADCAST



SNTP Broadcast Configuration

Request InBcast Mode	Disabled
POLL Timeout InBcastMode	5
Delay Time InBcastMode	8000
Primary Addr InBcast Mode	0.0.0.0

Figure 45: 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:

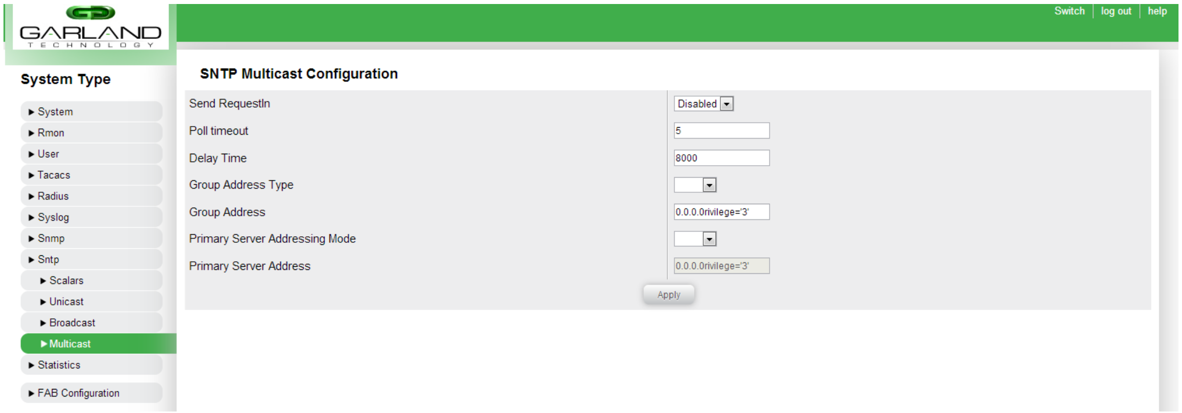
- **Enabled**: The SNTP request is sent to the broadcast server to calculate the delay time.
- **Disabled**: The SNTP request is not sent.

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.

11.4 SNTP MULTICAST



SNTP Multicast Configuration

Send RequestIn: Disabled

Poll timeout: 5

Delay Time: 8000

Group Address Type:

Group Address: 0.0.0.0rivilege='3'

Primary Server Addressing Mode:

Primary Server Address: 0.0.0.0rivilege='3'

Figure 46: 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.

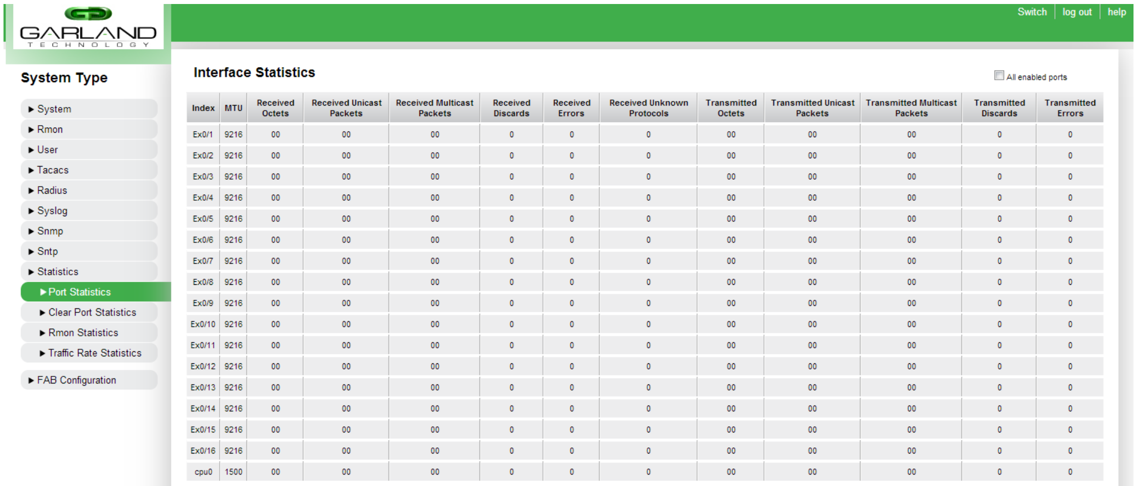
Primary Server Addressing Mode: Specifies the address type of the primary server learnt in Multicast addressing mode.

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

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



Interface Statistics

□ All enabled ports

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

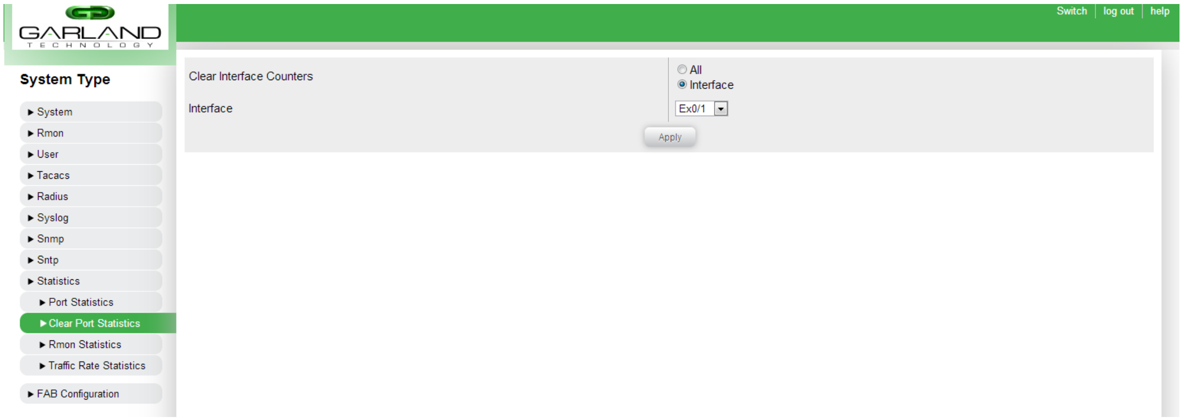
Figure 47: Port statistics

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 Nunicast 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.
- **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 Nunicast 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



Clear Interface Counters ○ All ● Interface

Interface Ex0/1

Figure 48: Clear Port Statistics

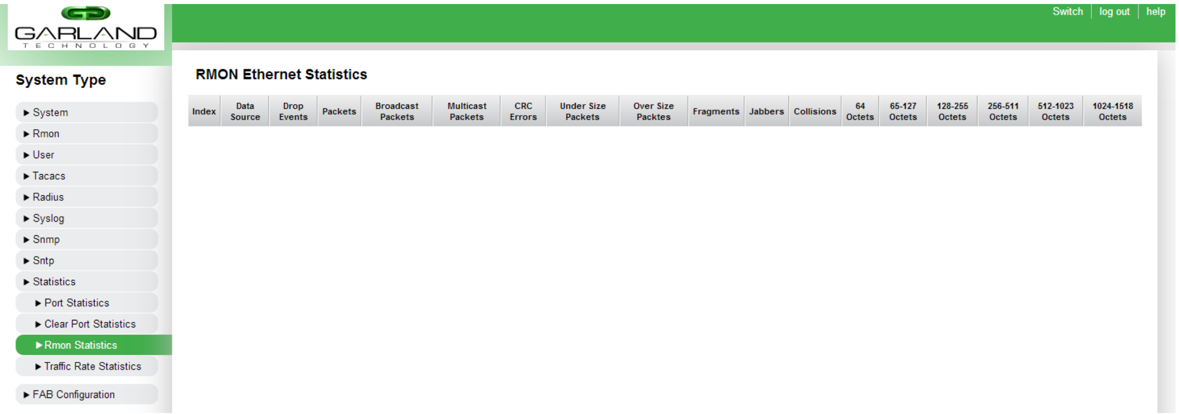
Users can clear all the port data or individually through this page.

Clear Interface Counters: This option allows the user to select whether all of the port counters should be cleared or just a specific port.

Interface: This drop-down list allows the user to select a specific port if the "Interface" option was chosen above.

After selecting the desired options, the user can click on the "Apply" button to clear the specified counters.

12.3 RMON STATISTICS



RMON Ethernet Statistics

Index	Data Source	Drop Events	Packets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packtes	Fragments	Jabbers	Collisions	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets

Figure 49: RMON Statistics

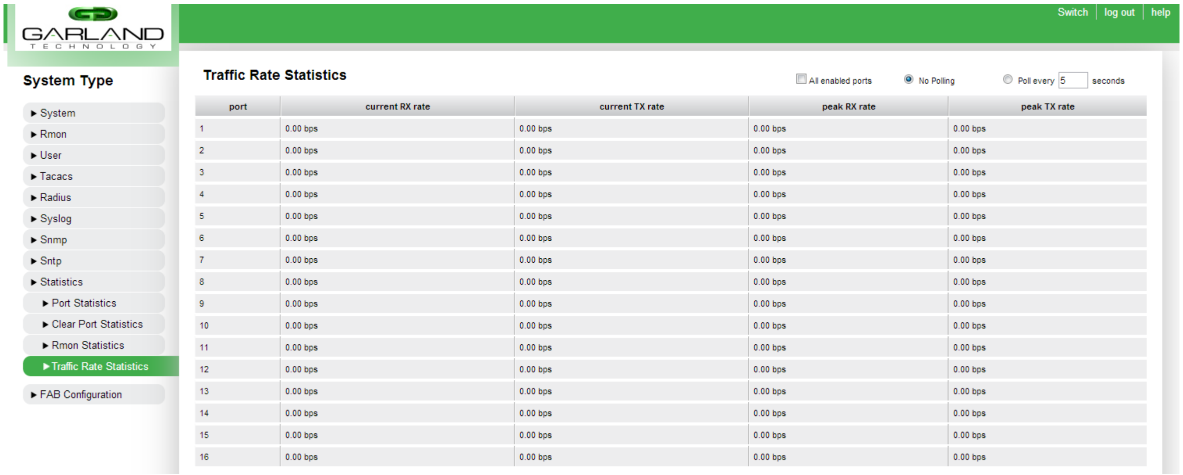
Users can view the statistics of each RMON index created.

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 config 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



Traffic Rate Statistics

□ All enabled ports ● No Polling ○ Poll every 5 seconds

port	current RX rate	current TX rate	peak RX rate	peak TX rate
1	0.00 bps	0.00 bps	0.00 bps	0.00 bps
2	0.00 bps	0.00 bps	0.00 bps	0.00 bps
3	0.00 bps	0.00 bps	0.00 bps	0.00 bps
4	0.00 bps	0.00 bps	0.00 bps	0.00 bps
5	0.00 bps	0.00 bps	0.00 bps	0.00 bps
6	0.00 bps	0.00 bps	0.00 bps	0.00 bps
7	0.00 bps	0.00 bps	0.00 bps	0.00 bps
8	0.00 bps	0.00 bps	0.00 bps	0.00 bps
9	0.00 bps	0.00 bps	0.00 bps	0.00 bps
10	0.00 bps	0.00 bps	0.00 bps	0.00 bps
11	0.00 bps	0.00 bps	0.00 bps	0.00 bps
12	0.00 bps	0.00 bps	0.00 bps	0.00 bps
13	0.00 bps	0.00 bps	0.00 bps	0.00 bps
14	0.00 bps	0.00 bps	0.00 bps	0.00 bps
15	0.00 bps	0.00 bps	0.00 bps	0.00 bps
16	0.00 bps	0.00 bps	0.00 bps	0.00 bps

Figure 50: Traffic Rate Statistics

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

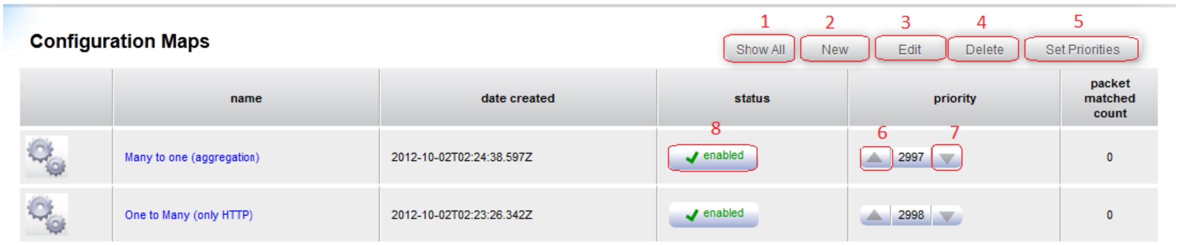
This page displays traffic rate statistics of the ports on the unit. The page displays the current TX and RX rate of each port as well as the peak TX and RX rates.

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. FAB 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



	name	date created	status	priority	packet matched count
	Many to one (aggregation)	2012-10-02T02:24:38.597Z	✓ enabled	▲ 2997 ▼	0
	One to Many (only HTTP)	2012-10-02T02:23:26.342Z	✓ enabled	▲ 2998 ▼	0

Figure 51: Configuration Maps

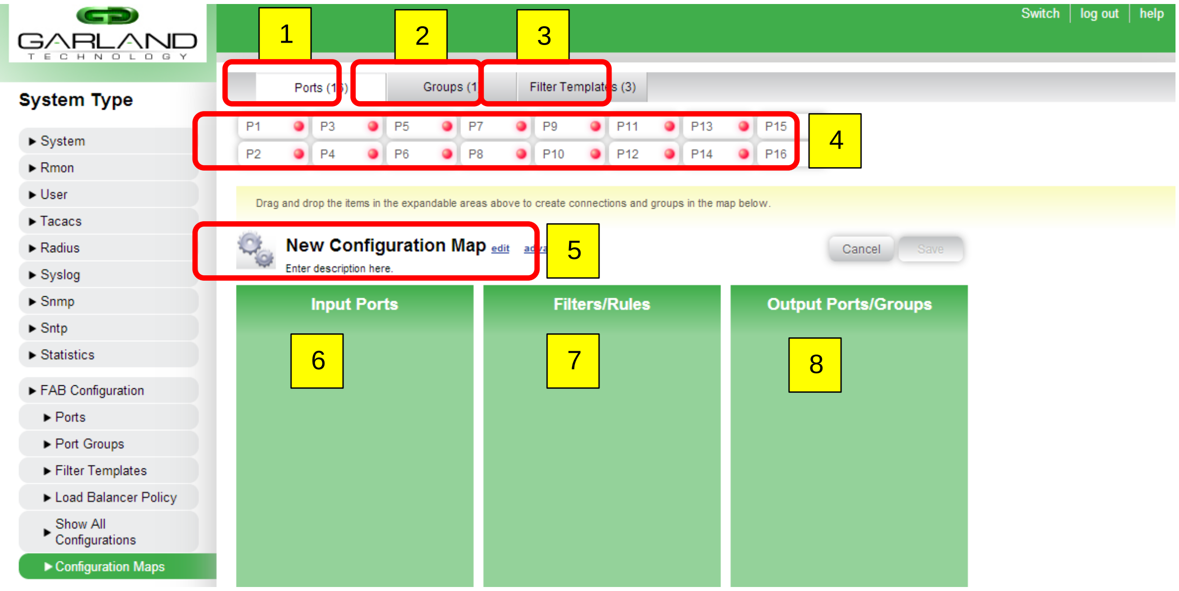
1. The "Show All" option in the configuration maps interface will truncate and display all configuration maps on a single page. Users can edit a specific configuration map in this view by clicking on it.
2. Clicking "New" will allow the user to create a new configuration map. It will not be saved until 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



Drag and drop the items in the expandable areas above to create connections and groups in the map below.

New Configuration Map edit

Enter description here.

Figure 52: Configuration Maps

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.

13.1.2 Multiple Port Selection

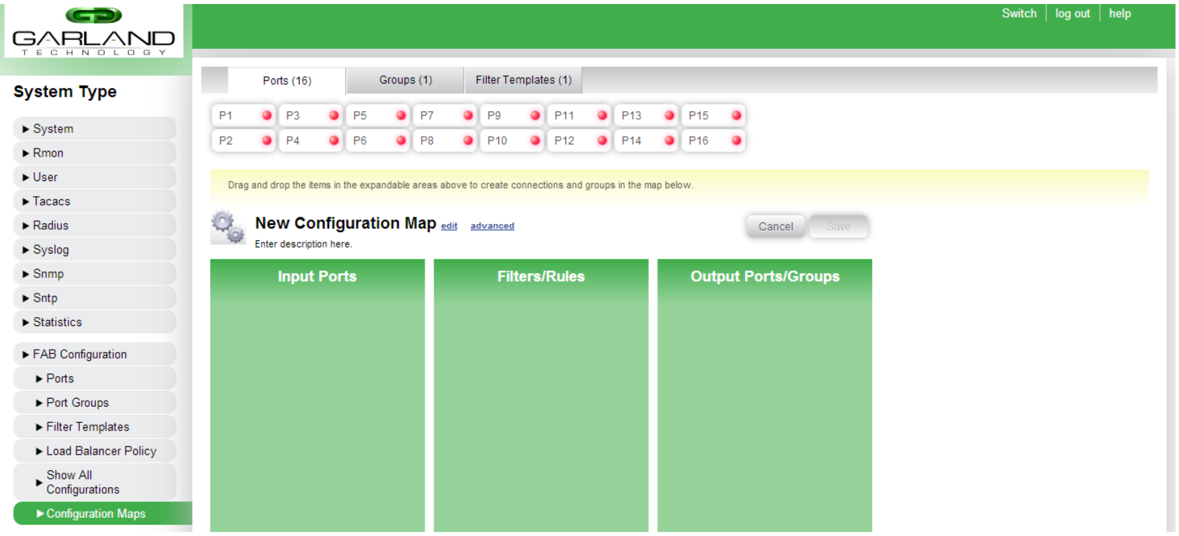
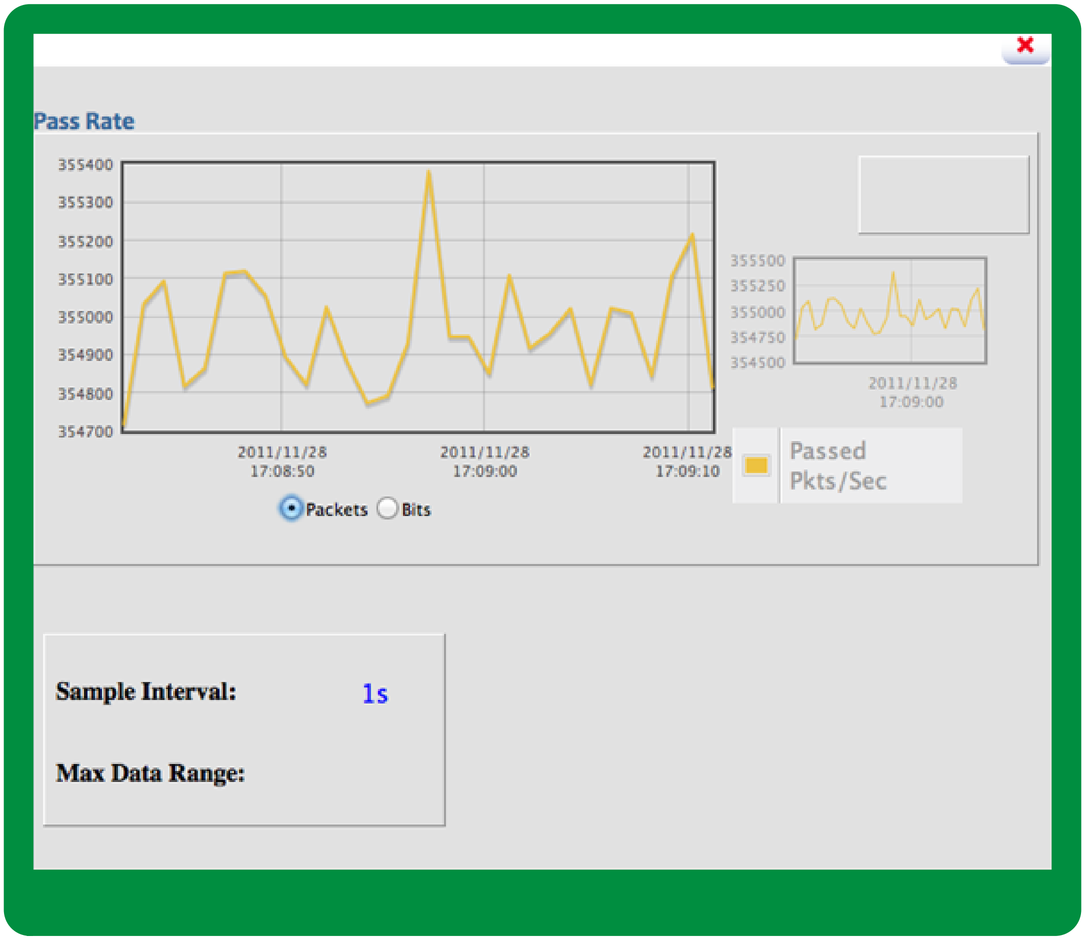


Figure 53: Multiple Port Selection

Users may select multiple ports at a time for use in a configuration map by holding down the CONTROL key on the keyboard and selecting the desired ports using the mouse. Once all desired ports have been selected, users may drag the ports into a section of the configuration map as though all of the ports are a single port.

To un-select a group of ports, users may click on any other port in the port list.

13.1.3 Graph



● Packets ○ Bits

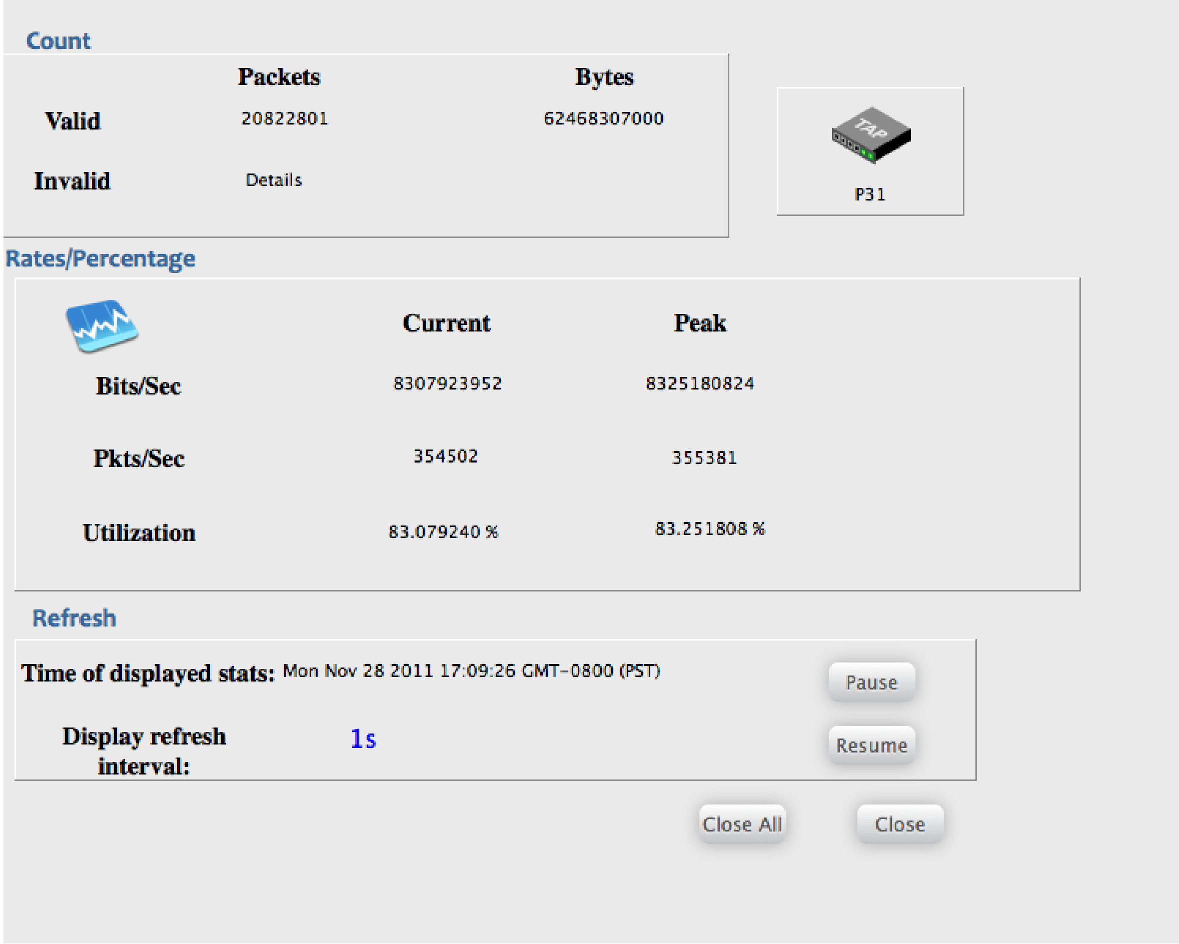
Sample Interval: 1s

Max Data Range:

Figure 54: 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



Count

	Packets	Bytes
Valid	20822801	62468307000
Invalid	Details	

Rates/Percentage

	Current	Peak
Bits/Sec	8307923952	8325180824
Pkts/Sec	354502	355381
Utilization	83.079240 %	83.251808 %

Refresh

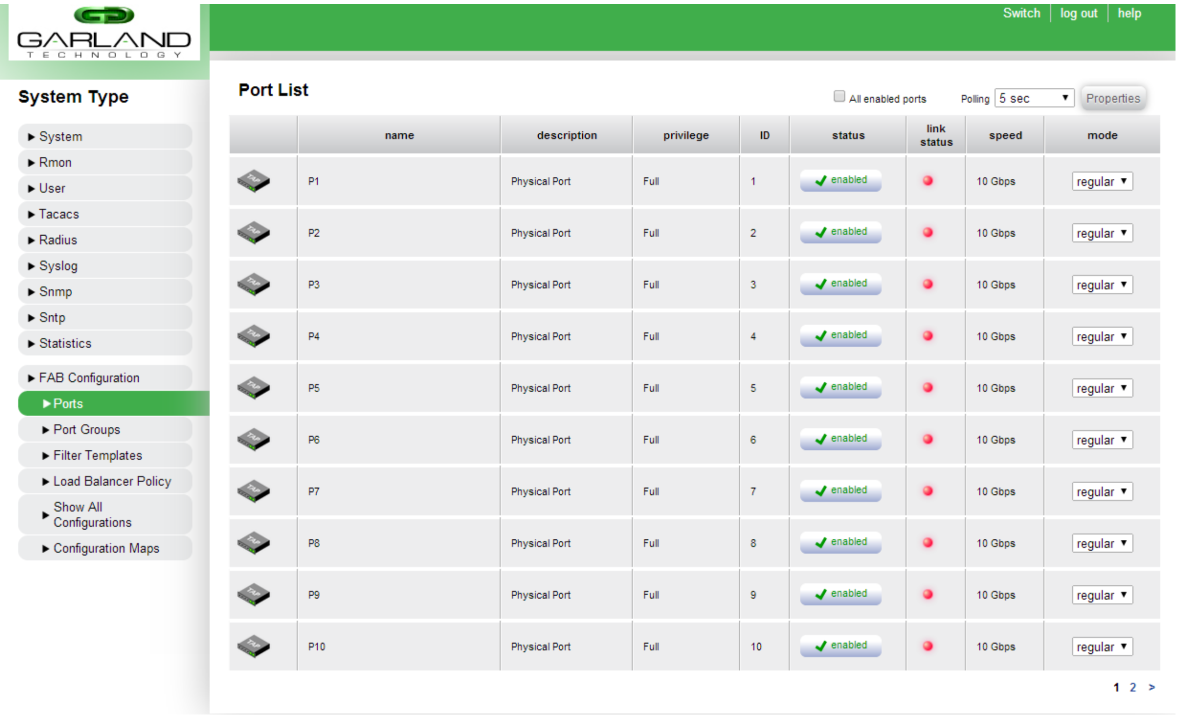
Time of displayed stats: Mon Nov 28 2011 17:09:26 GMT-0800 (PST)

Display refresh interval: 1s

Figure 55: 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 56: Ports

This page lists all of the physical ports available on the device. Users can view information about each individual port. Such information includes:

-Link up/down status: link status will be green if link is up, red if link is down.

-Port speed: Shows the link speed of the port. All ports are set to auto-negotiate and cannot be set manually.

-Port name: Users can modify and view custom name for all ports.

Users are also able to modify certain port properties. Modifiable properties include:

-Force mode: Users may forcibly link up a port when a link cannot be automatically established. This is generally used when connecting TAPs that don't have a transmit laser (such as passive TAPs).

-Link status: Users may administratively bring a port up or down by clicking the button in the "status" column associated with the specific port. Users may also set the port to loopback mode as well by clicking this button.

-Clicking on a specific port, then clicking the "Edit" button in the top right of the page will open the "Edit Port" interface. From this page, the user can edit the port's name, description, and picture. The user is also able to apply egress filters by dragging a filter from the "Filter Templates" tab at the top of the page to the blue area in the middle of the page. Clicking on the "advanced" link allows the user to enable/disable MPLS stripping for the port.

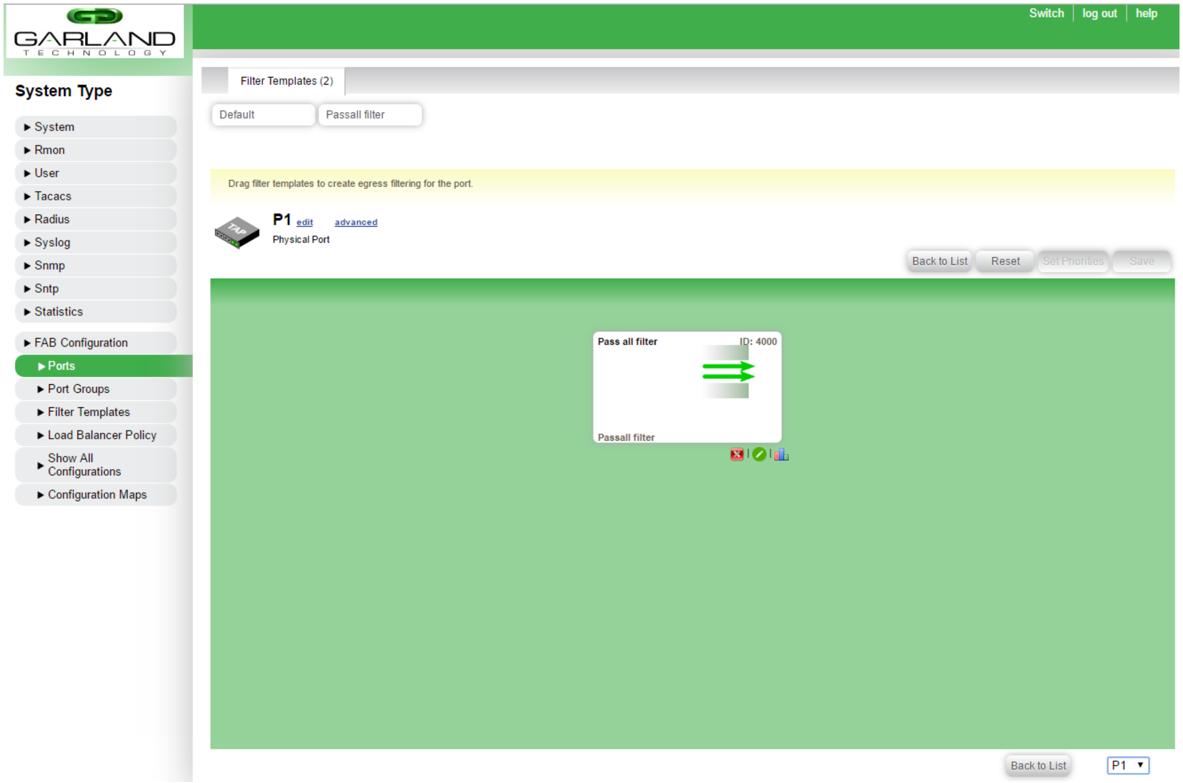
After the desired changes have been made, it is necessary to click on the "Save" button to apply the changes to the device.

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

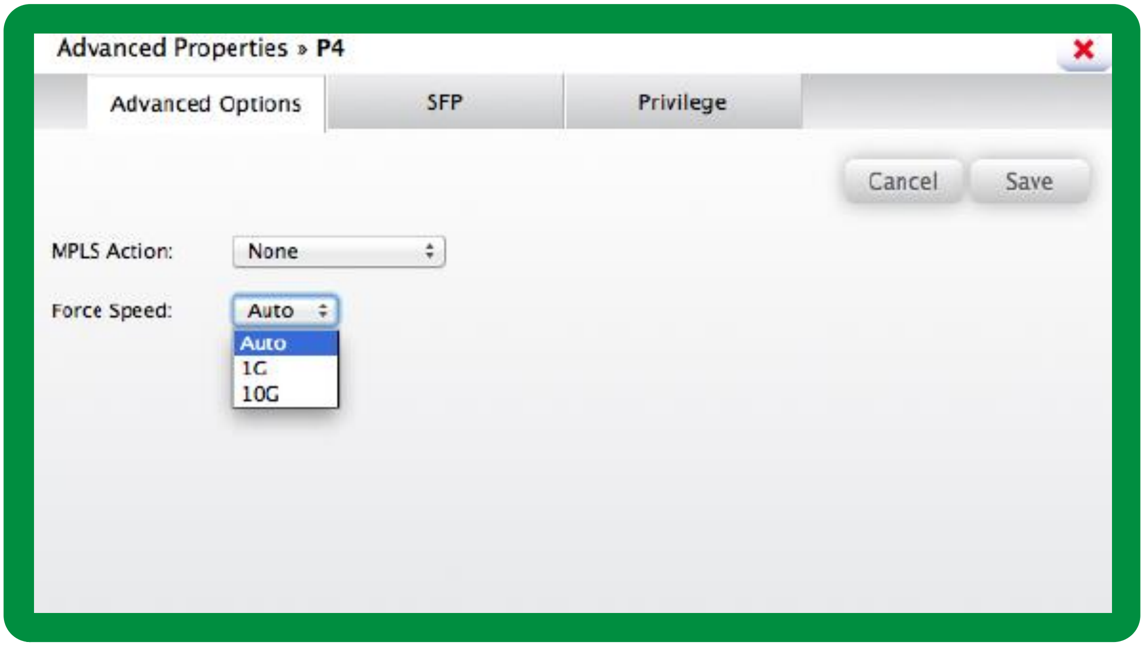


Drag filter templates to create egress filtering for the port.

Figure 57: 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



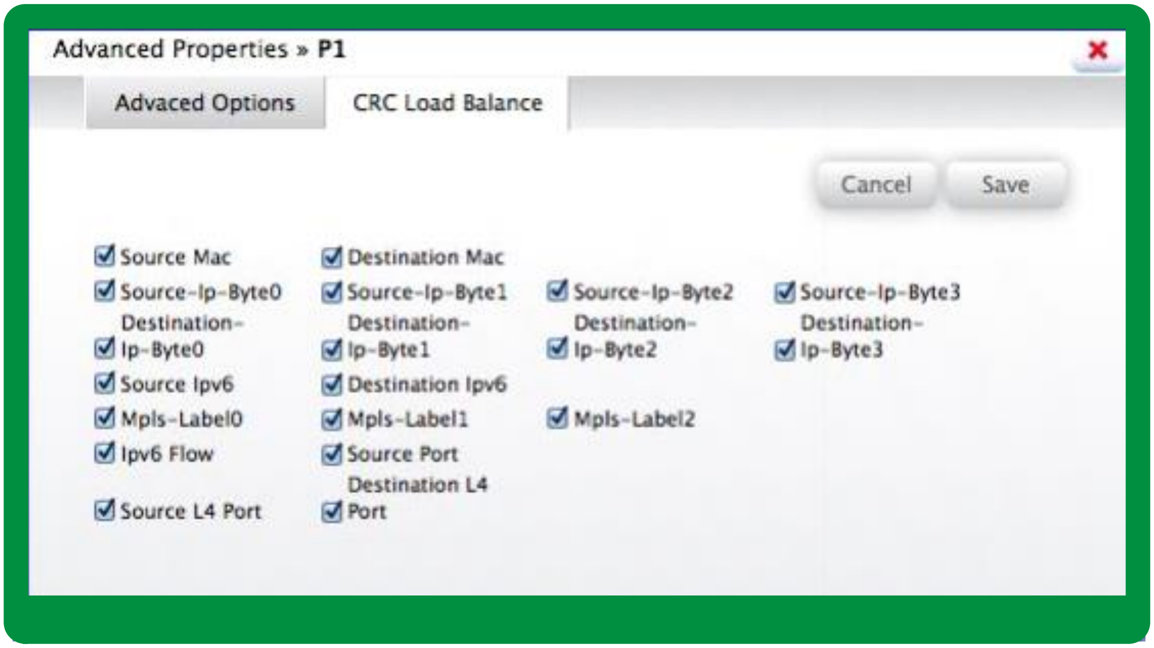
MPLS Action: None

Force Speed: Auto

Figure 58: 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.

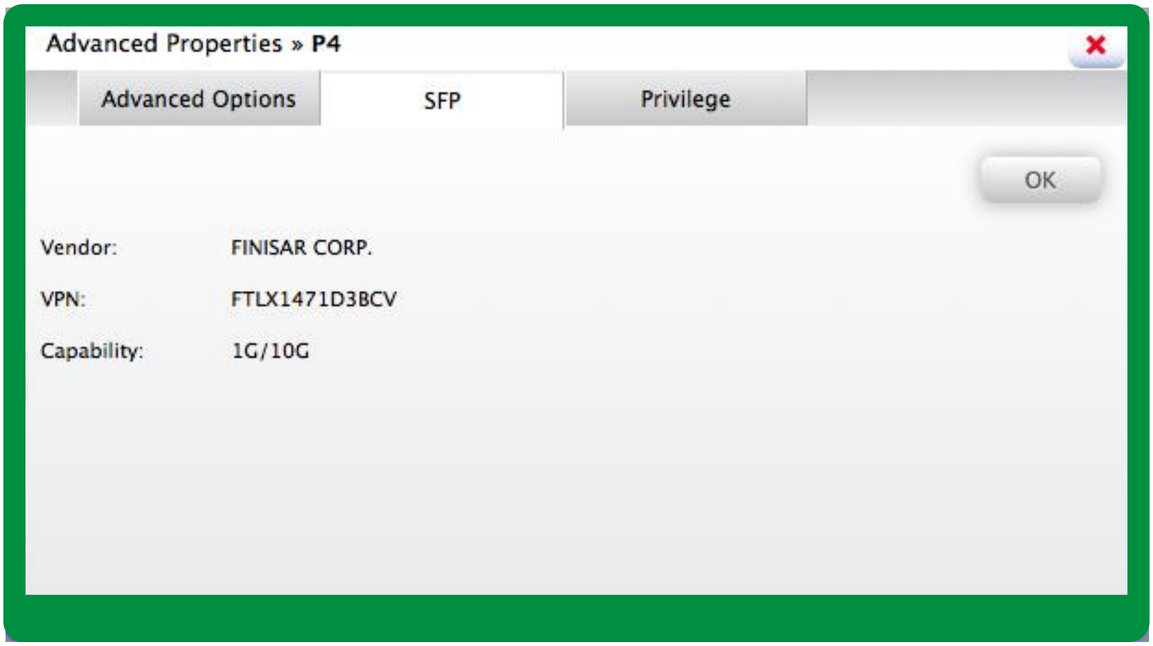
13.1.8 Ports – Advanced Options



☑ Source Mac
☑ Destination Mac
☑ Source-Ip-Byte0
☑ Source-Ip-Byte1
☑ Source-Ip-Byte2
☑ Source-Ip-Byte3
☑ Destination-Ip-Byte0
☑ Destination-Ip-Byte1
☑ Destination-Ip-Byte2
☑ Destination-Ip-Byte3
☑ Source Ipv6
☑ Destination Ipv6
☑ Mpls-Label0
☑ Mpls-Label1
☑ Mpls-Label2
☑ Ipv6 Flow
☑ Source Port
☑ Source L4 Port
☑ Destination L4 Port

Figure 59: CRC Load Balance

13.1.9 Advanced Options – SFP Description



Vendor: FINISAR CORP.

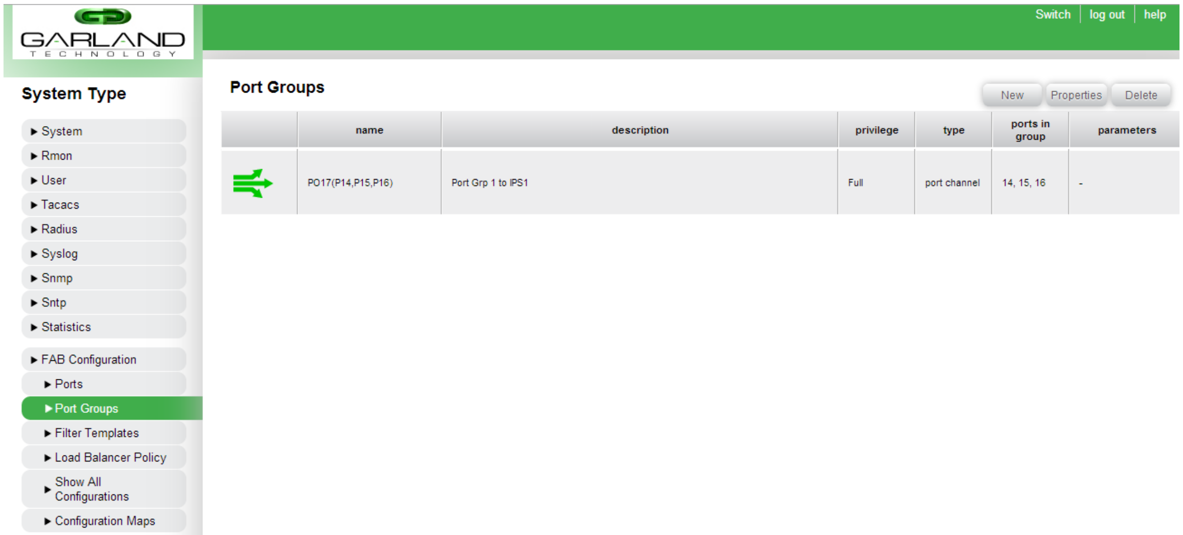
VPN: FTLX1471D3BCV

Capability: 1G/10G

Figure 60: 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



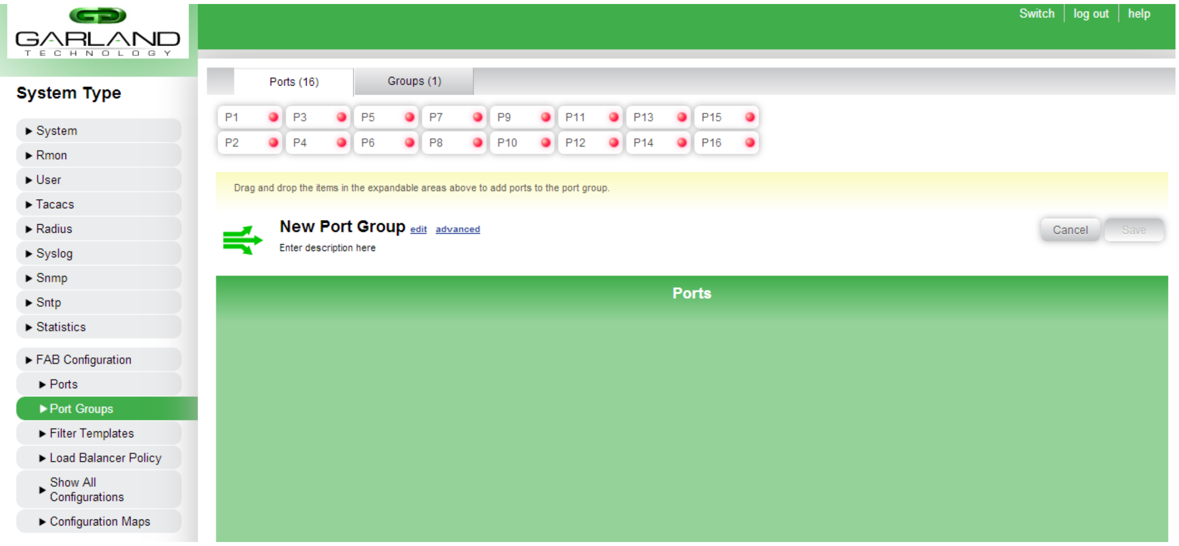
Port Groups

	name	description	privilege	type	ports in group	parameters
⇉	PO17(P14,P15,P16)	Port Grp 1 to IPS1	Full	port channel	14, 15, 16	-

Figure 61: Port Groups

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

13.2.1 New Port Groups



Drag and drop the items in the expandable areas above to add ports to the port group.

New Port Group

Enter description here

Figure 62: 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.

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.

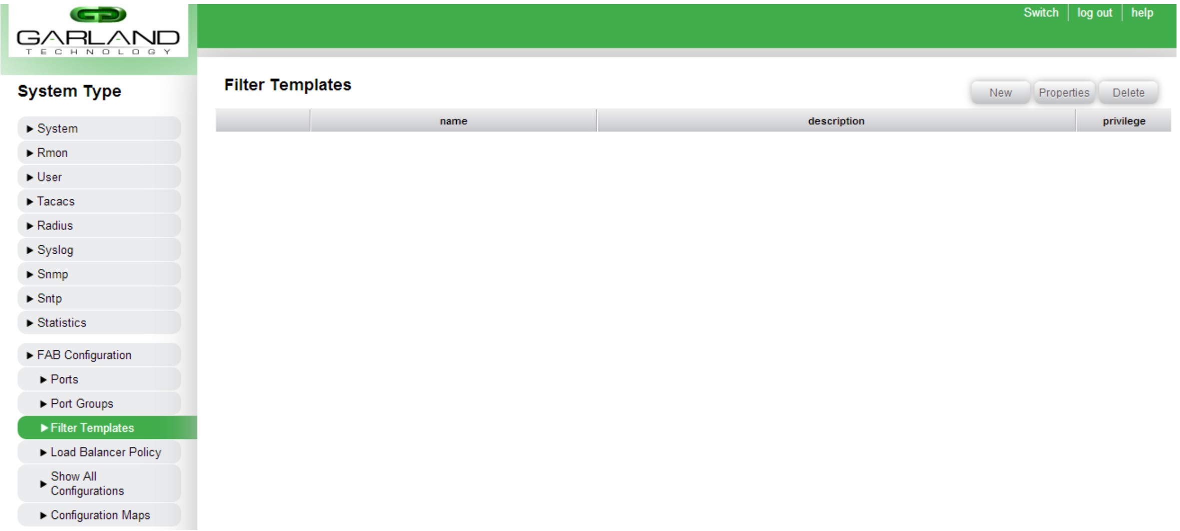
After the desired ports have been added to the port group, it is necessary to click the "Save" button to save the configuration to the device.

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.



	name	description	privilege

Figure 63: 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.

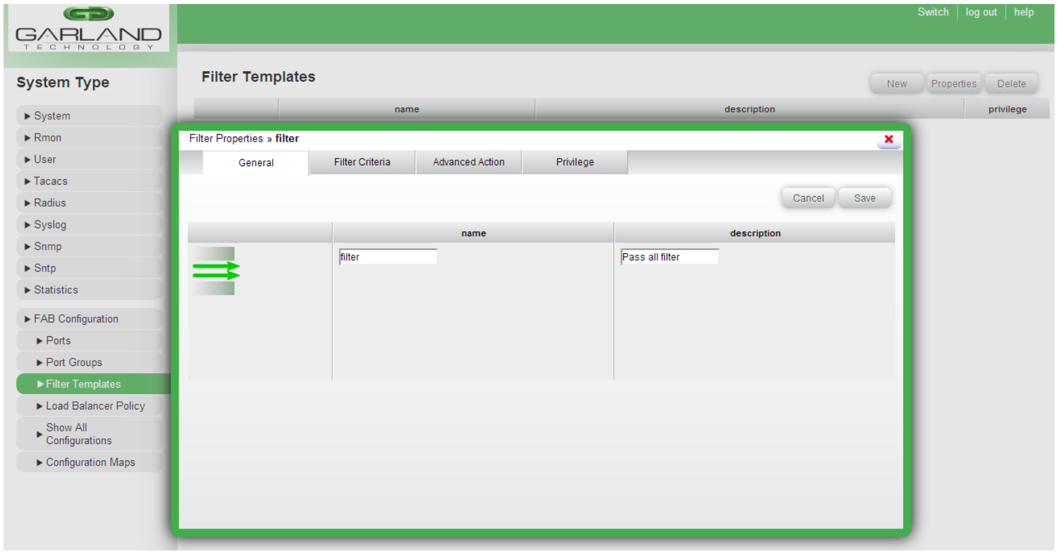
When users create a new filter template, they can define a filter name and its description under the General Tab.

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.

13.4 NEW FILTER TEMPLATES

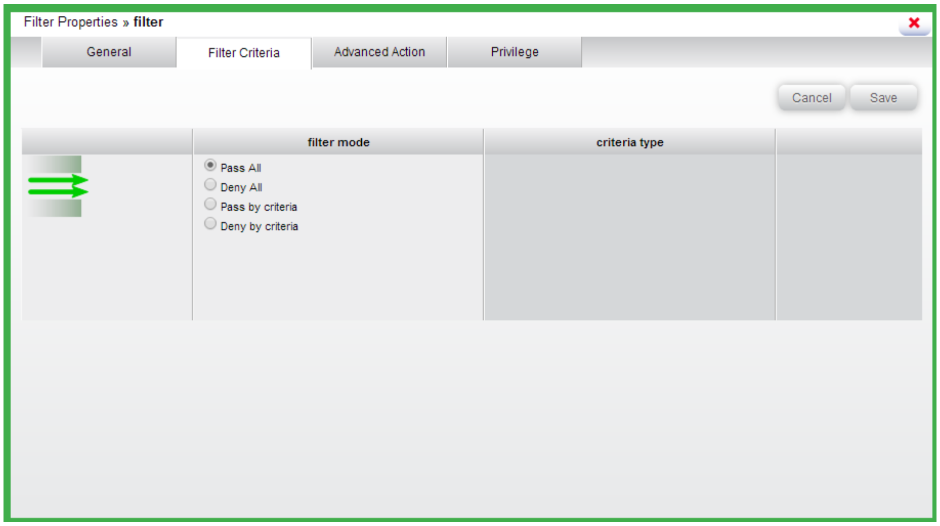


name	description
filter	Pass all filter

Figure 64: 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.

13.5 NEW FILTER TEMPLATE



● Pass All
○ Deny All
○ Pass by criteria
○ Deny by criteria

Figure 65: 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.

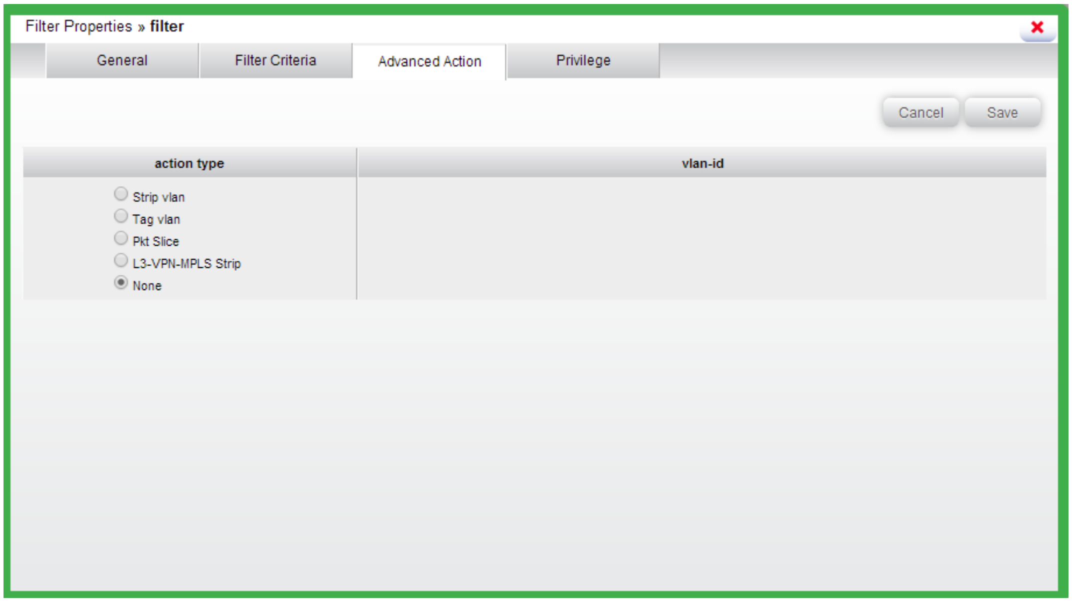
1. Layer 2

2. Layer 3/4 (ipv4)

3. IPv6

4. User defined byte (UDB)

13.6 ADVANCED



action type	vlan-id
○ Strip vlan ○ Tag vlan ○ Pkt Slice ○ L3-VPN-MPLS Strip ● None	

Figure 66: 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 on this screen.

Note: There may only be one output port per port group when L3 MPLS stripping is enabled.

History

Version	Author	Date Effective	Nature of Change
1.5	George Bouchard	November 10, 2012	Misc. changes
1.6	George Bouchard	July 10, 2015	Misc. changes
1.7	George Bouchard	April 18, 2016	New Features and Misc. Changes
2.0	George Bouchard	May 23. 2016	Minor corrections
2.2	George Bouchard	July 19, 2016	Minor corrections