GARLAND

TECHNOLOGY

See every bit, byte, and packet®

XtraTAP
Packet Broker
INT10G8XX56-X | 1.18.5

User Manual

Introduction 2

Part numbers 3

1U Chassis Specifications 3

1 Dashboard 4
1.1 System 4
1.2 Packet Broker 4

2 System 5
2.1 System Info 6
2.2 General 6
2.3 Admin 6
2.3.1 Groups 7
2.3.2 Users 7
2.3.3 Authentication 8
2.4 Network Settings 9
2.5 Date & Time 10
2.6 Syslog 10
2.7 SNMP 11
2.8 Export Configuration 11
2.9 Import Configuration 12
2.10 Software Upgrade 12
2.11 Reboot 13

3 Packet Broker 14
3.1 Filter Template 15
3.2 Load Balancing Policy 16
3.3 Load Balancing Group 16
3.4 Config Map 17
3.4.1 Ingress 18
3.4.2 Filter 18
3.4.3 Egress 19
3.4.4 Egress Filter 20
3.4.5 Config Map Save 21
3.4.6 Modify a Config Map 22
3.4.7 Config Map Statistics 22
3.4.8 Delete Config Map 23
3.4.9 Config Map Priority 23
3.4.9.1 Method 1 24
3.4.9.2 Method 2 24

3.4.10 Enable/Disable Config Map 25
3.4.10.1 Disable Config Map 25
3.4.10.2 Enable Config Map 25

4 Port Info 26
4.1 Port Configuration 27
4.1.1 Port Description 27
4.1.2 Set Speed 27
4.1.3 Mode 27
4.1.4 Port Statistics 27

Introduction

The XtraTAP: Packet Broker is a purpose-built hardware device that supports passive network tapping combined with advanced filtering, aggregation, and load balancing, guaranteeing your tools see every bit, byte, and packet.®

Part numbers

INT10G8SR56-5	Multimode 50/50 split fiber TAPs
INT10G8SR56-6	Multimode 60/40 split fiber TAPs
INT10G8SR56-7	Multimode 70/30 split fiber TAPs
INT10G8SR56-8	Multimode 80/20 split fiber TAPs
INT10G8SR56-9	Multimode 90/10 split fiber TAPs
INT10G8LR56-5	Singlemode 50/50 split Fiber TAPs
INT10G8LR56-6	Singlemode 60/40 split Fiber TAPs
INT10G8LR56-7	Singlemode 70/30 split Fiber TAPs
INT10G8LR56-8	Singlemode 80/20 split Fiber TAPs
INT10G8LR56-9	Singlemode 90/10 split Fiber TAPs

1U Chassis Specifications

Support for: SFP(SX, LX and TX) and SFP+ (SR, LR, ER)
Operating Temp: 0 to 40° C or 32 to 104° F
Operating Humidity: 5 to 95%
Dimensions: 21.09” L x 1.719” H x 17.32” W (535.686mm L x 43.6626 mm H x 439.928mm W)
Airflow: 100 IF/m
(2) AC Power Supplies Included

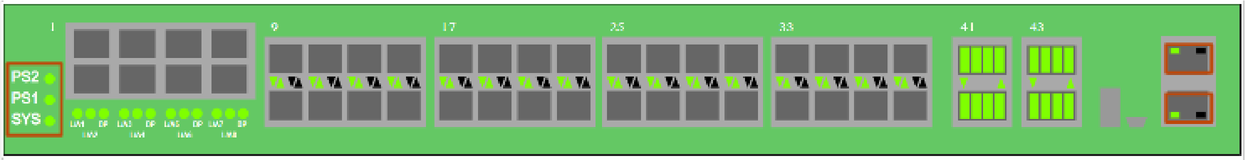
1 Dashboard

The Dashboard of the INT10G8XX56-X consists of the following.

System
Packet Broker

1.1 System

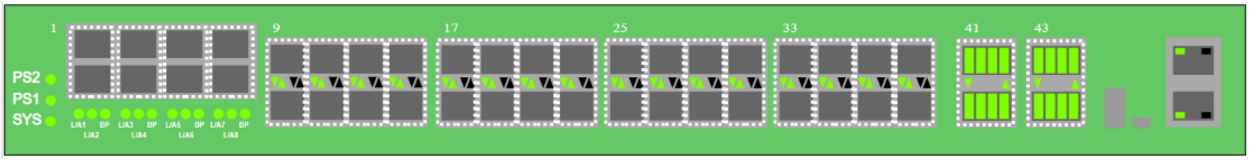
The System Section of the Dashboard consists of the following.



PS2	Power Supply 2 LED
PS1	Power Supply 1 LED
SYS	System LED
Ethernet Interface	Upper Right LED
Serial Interface	Lower Right LED

1.2 Packet Broker

The Packet Broker Section of the Dashboard consists of the following.



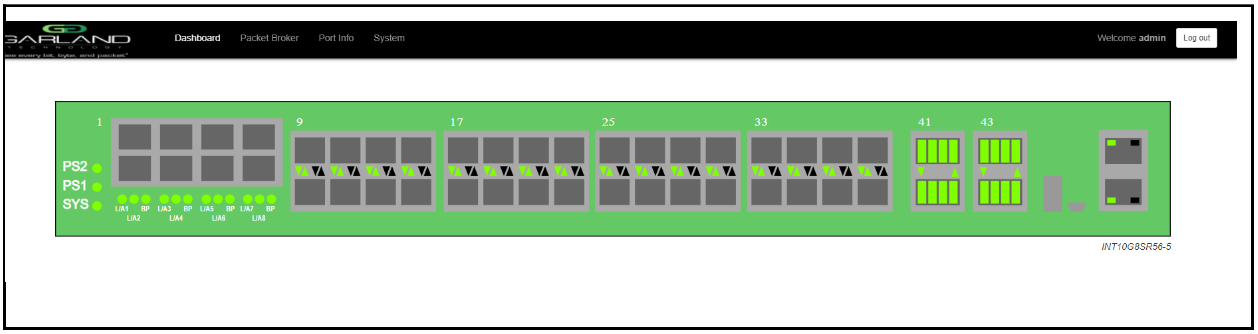
L/A1	Port 1 Link/Activity LED
L/A2	Port 2 Link/Activity LED
BP	Bypass LED N/A
L/A3	Port 3 Link/Activity LED
L/A4	Port 4 Link/Activity LED
BP	Bypass LED N/A
L/A5	Port 5 Link/Activity LED
L/A6	Port 6 Link/Activity LED
BP	Bypass LED N/A
L/A7	Port 7 Link/Activity LED
L/A8	Port 8 Link/Activity LED
BP	Bypass LED N/A

Port 9 thru 43 (odd) Up Arrows	Link/Activity LED
Port 10 thru 44 (even) Down Arrows	Link/Activity LED

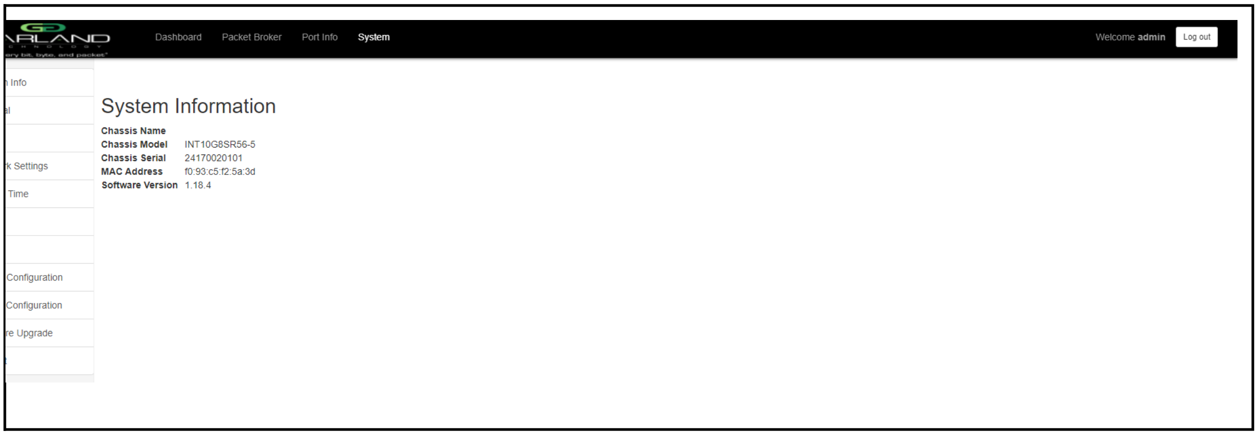
2 System

The following configuration options may be displayed, modified, enabled or disabled under the System panel.

System Info
General
Admin
Network Settings
Date & Time
Syslog
SNMP
Export Configuration
Import Configuration
Software Upgrade
Reboot



1. Select System on the Dashboard Menu bar.



System Information

Chassis Name
Chassis Model INT10G8SR56-5
Chassis Serial 24170020101
MAC Address f0:93:c5:f2:5a:3d
Software Version 1.18.4

The System panel will be displayed. The system configuration options will be displayed on the left side of the panel.

2.1 System Info

The System Information panel displays the following.

Chassis Name
Chassis Model
Chassis Serial Number
MAC Address
Software Version

2.2 General

The following configuration options may be displayed or modified.

Chassis Name
Key Press Timeout

1. Select General.

The panel will display the current configuration.

2. Select Edit Configuration.

3. Enable, disable or modify the desired options.

4. Select Save to save updates.

5. Select Cancel to return to the General System Settings panel.

2.3 Admin

The following configuration options may be displayed, modified, enabled or disabled.

Groups
Users
Local Authentication
TACACS Authentication

1. Select Admin.

The panel will display the current configuration.

The default user is “admin/gtadmin1”. The “admin” user privileges are defined by the default group “admin”. Changes to the default user “admin” and group “admin” are allowed. However, the “admin” user or group “admin” may not be deleted.

2.3.1 Groups

The group defines the authorization for a user or group of users. A group may be used for local or TACACS authorization. In Use “true” means that there is at least one local user assigned to the group. If a group is used by TACACS, the In Use will indicate “false”.

1. Select Groups + to create a new group.

    The Create New Group panel will be displayed.

2. Enter the Group Name.
3. Select the privileges for the new group.
4. Select Save to save updates.
5. Select Cancel to return to the Admin Settings panel.

    The new group will be displayed on the Admin Settings panel.

6. Edit the group privileges by selecting the pencil.
7. Deleted the group by selecting the Red X. If a group has at least one local user assigned it cannot be deleted.

2.3.2 Users

Users displayed on the Admin Settings panel are for local authentication only.

1. Select Users + to create a new user.

    The Create New User panel will be displayed.

2. Enter the Username.
3. Enter the Password.
4. Select the group the user will be assigned.
5. Select Save to save updates.
6. Select Cancel to return to the Admin Settings panel.

    The new local user will be displayed on the Admin Settings panel.

7. Edit the username, password or assigned group by selecting the pencil.
8. Delete the local user by selecting the Red X.

2.3.3 Authentication

Authentication allows for two options, Local or TACACS. Local or TACACS Authentication may be enabled or disabled independently and at least one option must be enabled.

1. Select Authentication Settings.

    The Authentication Settings panel will be displayed. Local Authentication is enabled by default.

2. Select TACACS Authentication to enable.

3. Enter the TACACS Server IP Address.

4. Enter the TACACS Server Secret Word, optional.

5. Select Save to save updates.

6. Select Cancel to return the Admin Settings panel.

7. TACACS Test

    This option may be used to verify the authentication of a TACACS user and password. The TACACS Test option will be active only if TACACS Authentication has been enabled.

    The TACACS Test panel will appear.

7.1 Enter the Username.

7.2 Enter the Password.

7.3 Select Test.

    The GUI will display the results of the authentication of the user and password entered.

8. TACACS Ping

    This option may be used to verify the network connectivity from the unit to the TACACS server. The TACACS Ping option will be active only if TACACS authentication has been enabled.

    The GUI will display the results of the ping test.

2.4 Network Settings

The following configuration options may be displayed, modified, enabled or disabled. Any change made to any network setting option could cause network connectivity disruption for about 60 seconds.

DHCP
IP Address
Mask
Gateway
DNS 1
DNS 2
SSL Certificate Loaded
Using Uploaded SSL Certificate

1. Select Network Settings.

   The Network Settings panel will be displayed with the current configuration.

2. Select Edit Settings.

   The Network Settings panel will appear.

3. Enable, disable or modify the desired options.

4. Enable or disable Using Uploaded SSL Certificate.

   This option may be enabled if a SSL cert.pem file and key.pem file have been uploaded to the unit using the Add SSL Certificate option on the Network Settings panel.

5. Select Save to save updates.

6. Select Cancel to return the Network Settings panel.

7. Add SSL Certificate.

   Uploading a custom SSL certificate involves two files. The cert.pem file and key.pem file. The unit will consider these files during the upload. If the files do not match or one of the files are corrupted the unit will abort the upload. The Result Messages will be displayed in the GUI. Adding a SSL certificate will cause the GUI to restart. This could take up to 90 seconds. It may be required to refresh or restart the web browser.

8. Select Add SSL Certificate.

   The Select Certificate and Select Key File panel will appear.

9. Select Choose File for Select Certificate.

10. Select the desired cert.pem file.

11. Select Open.

12. Select the Choose File for Select Key File.

13. Select the desired key.pem file.

14. Select Open.

15. Select Upload.

16. Select Restart Import to select a different cert.pem or key.pem file.

17. Select Cancel to return to the Network Settings panel.

2.5 Date & Time

The following configuration options may be displayed, modified, enabled or disabled.

Timezone
UTC
NTP IP Address
NTP Pool
Time
Date

1. Select Date & Time.

   The Date & Time Settings panel will be displayed with the current configuration.

2. Select Edit Settings.

   The Date & Time Settings panel will be displayed.

3. Enable, disable or modify the desired options.

4. Select Save to save updates.

5. Select Cancel to return the Date & Time Settings panel.

2.6 Syslog

The following configuration options may be displayed, modified, enabled or disabled.

Unit ID
Protocol
Syslog Server IP Address
Protocol Port Number

1. Select Syslog.

   The Syslog Configuration panel will be displayed with the current configuration.

2. Select Edit Settings.

3. Enable Syslog Config.

4. Enable, disable or modify the desired options.

5. Select Save to save updates.

6. Select Cancel to return the Syslog Configuration panel.

7. Sys Log Test may be selected to send a test message to the server.

2.7 SNMP

The following configuration options may be displayed, modified, enabled or disabled.

V2 Read/Write	V2 read Only	V3 MD5/DES	V3 SHA/AES
Access Port	Access Port	Access Port	Access Port
Trap Port	Trap Port	Trap Port	Trap Port
Trap IP Address	Trap IP Address	Trap IP Address	Trap IP Address
Community Password	Community Password	User	User
		Auth Password	Auth Password
		Priv Password	Priv Password

1. Select SNMP.

   The SNMP Configuration panel will be displayed with the current configuration.

2. Select Edit Configuration.

   The SNMP Configuration panel will be displayed.

3. Select Enable SNMP Config.

4. Enable, disable or modify the desired options.

5. Select Save to save updates.

6. Select Cancel to return the Syslog Configuration panel.

7. SNMP Test may be selected to send a test trap to the server.

2.8 Export Configuration

This option creates a configuration file (exportCfg.json) that may be used to recover a unit. The exportCfg.json file may be renamed if desired. The exportCfg.json file does not contain Usernames, Passwords, Groups or Network Settings.

1. Select Export Configuration.

   The Export Configuration panel will be displayed.

2. Select Export.

   The exportCfg.json file will be downloaded to the default download destination of the browser.

2.9 Import Configuration

This option allows a previously created configuration file (exportCfg.json) to be uploaded to the unit. The Chassis Model is the only option that is considered and must match, otherwise, the unit will reject the exportCfg.json file.

1. Select Import Configuration.

   The Import Configuration panel will be displayed.

2. Select Choose File.

3. Select the desired exportCfg.json file.

4. Select Open.

5. Select Upload.

   The unit will automatically verify the selected exportCfg.json file.

6. Select Configure.

   The unit will import and load the exportCfg.json. An “import done” message will be displayed when complete. A reboot is not required.

2.10 Software Upgrade

This option allows the unit’s firmware to be upgraded. The existing unit configuration will not be affected and maintained during the upgrade. It may be required to refresh or restart the web browser after the firmware upgrade is complete.

1. Select Software Upgrade.

   The Update Firmware panel will be displayed.

2. Select Choose File.

3. Select the desired firmware file.

4. Select Open.

   The new firmware file will be displayed.

5. Select Upload.

   The unit will validate the firmware file.

   The unit will install the firmware file.

   The unit will reboot.

6. After the upgrade is complete. The GUI will refresh to the Login panel.

2.11 Reboot

This option allows the unit to be rebooted. The traffic will be affected for up to 3 minutes.

1. Select Reboot.

   The Reboot Device panel will be displayed.

2. Select Reboot.

   The unit will present an “Are you sure?” message.

3. Select OK.

   A “rebooting” message will be displayed.

   A “Session timed out. Go to Login screen” message will be displayed.

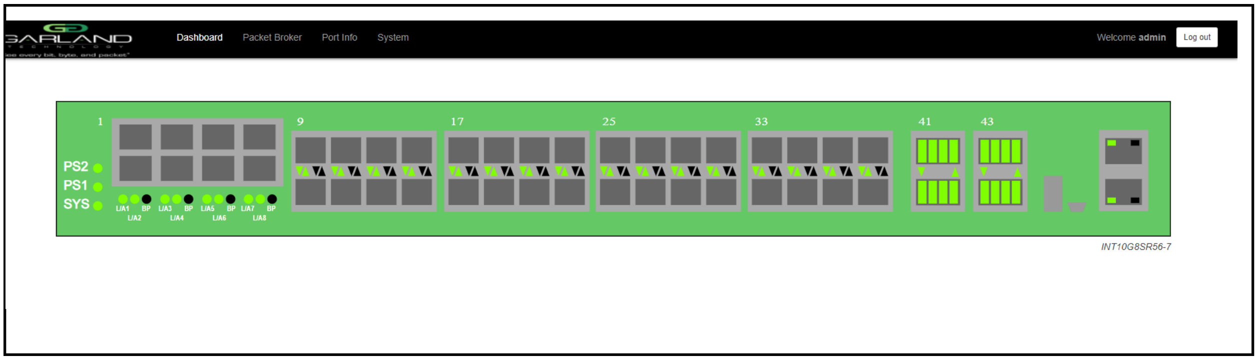
4. Select Go.

   The Login panel will be displayed.

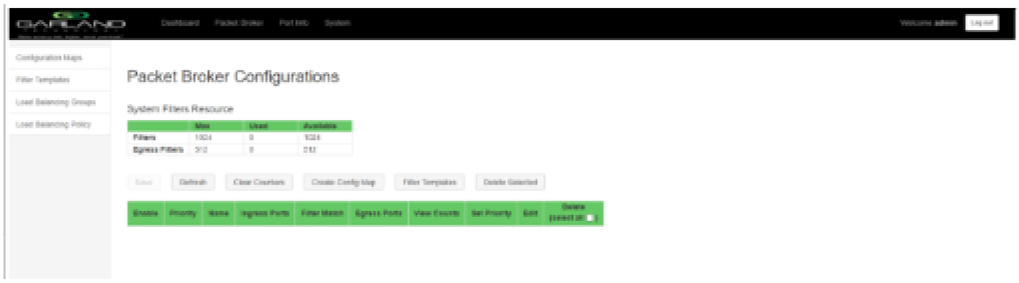
3 Packet Broker

The packet broker section consists of ports 1 through 44.The following configuration options may be displayed, modified, enabled or disabled.

Configuration Maps	Load Balance Policy
Filter Templates	Load Balance Groups



1. Select Packet Broker on the Dashboard menu bar.



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	0	1024
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)

The Packet Broker Configurations panel will be displayed.

3.1 Filter Template

Filter templates may be created as a pass-all, pass-by, or deny-by. Pass by and deny by templates may include multiple matching options to filter traffic. The options are considered by the system as (and) options. Thus, for traffic to pass or be denied it must match all defined options. Once a template is created it will appear on the Create Config Map panel and may be used to create an ingress or egress filter. Template options may be modified when applied to a config map. Any option modification made will not change the original template. It is advisable to rename a filter applied to a config map if the original template options were modified.

1. Select Filter Templates on the Packet Broker Configurations panel.

   The Filter Templates panel will be displayed.

2. Select Create Template.

   The Create New Filter Template panel will be displayed.

3. Enter the template name. If no name is entered the system will automatically apply a name as follows, tmplt, tmplt(2), tmplt(3), etc.

4. Enter the description, optional.

5. Select the Template Type, Pass All, Pass By or Deny By.

6. If pass by or deny by was selected in Step 5, the options will be displayed as follows.

   Source MAC Address / Source MAC Mask
   Destination MAC Address / Destination MAC Mask
   Ether Type
   Source IP Address / Source IP Mask
   Destination IP Address / Destination IP Mask
   Inner VLAN ID
   Outer VLAN ID
   DSCP
   IP Protocol
   L4 Source Port or Range
   L4 Destination Port or Range

7. Select Save Template once all desired option modifications have been completed.

8. The new filter template will appear on the Filter Templates panel.

9. The filter template may be modified by selecting the template name.

10. The filter template may be deleted by selecting the red X.

3.2 Load Balancing Policy

The load balancing policy determines the hashing applied to all load balancing groups. The load balancing policy options are as follows and may be applied as L3 and/or L4 or L2.

Ipv4 Source
Ipv4 Destination
L4 Source Port
L4 Destination Port

MAC Source
MAC Destination

1. Select Load Balancing Policy on the Packet Broker Configurations panel.

   The Load Balancing Policy panel will be displayed.

2. Select the desired load balancing policy options.

3. Select Save to save updates.

4. Select Cancel to disregard changes.

3.3 Load Balancing Group

Load balancing groups are used as an egress option on config maps. The traffic applied to the ports assigned to a load balancing group will follow the hashing per the load balancing policy. Ports may be added or removed from load balancing groups as desired. However, if ports are added or removed from a load balancing group that is used in a config map, the config map load balancing group will be also modified, the reverse is also applied. Previously created load balancing groups will appear on the Create Config Map panel.

1. Select Load Balancing Groups on the Packet Broker Configurations panel.

   The Load Balancing Groups panel will be displayed.

2. Select Create Group.

   The Create New Load Balance Group panel will be displayed.

3. Enter the name. If no name is entered the system will automatically apply a name as follows, lbg, lbg(2), lbg(3), etc.

4. Enter the description, optional.

5. Add ports by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the New L.B. Group panel and release. Repeat for all desired ports. Ports may be added in any combination.

6. Remove a port by placing the cursor on the port in the New L.B. Group panel and double press the left mouse button.

7. Select Save to save updates.

8. Select Cancel to return to the Load Balancing Groups panel.

The load balancing group will be displayed on the Load Balancing Groups panel. The assigned ports will also be displayed.

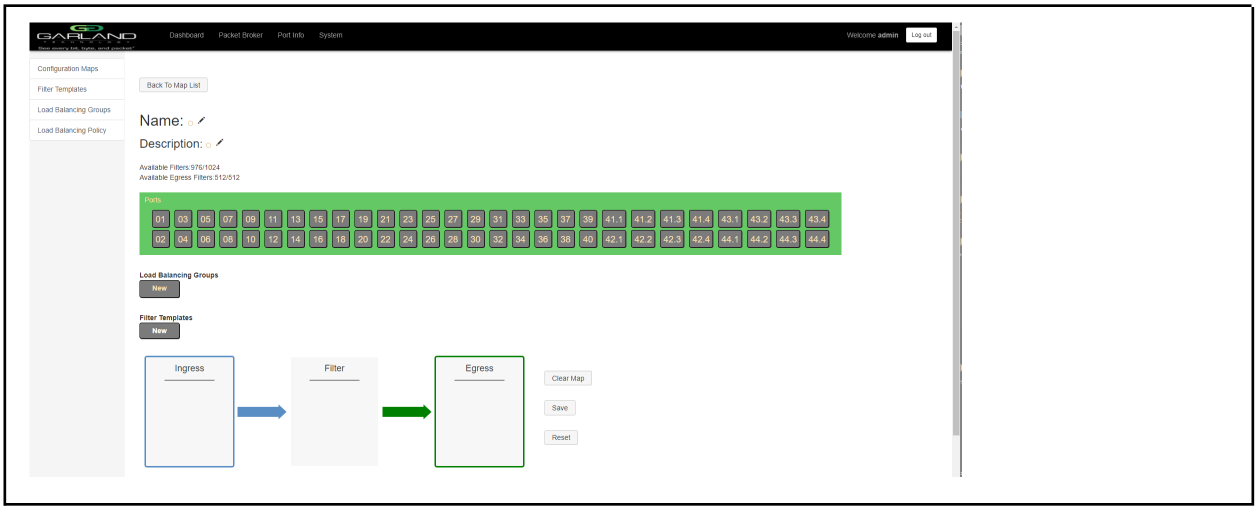
9. Edit the load balancing group by selecting the Edit for the desired group.

10. Deleted the load balancing group group by selecting the red X. Load balancing groups may not be deleted if used on a config map.

3.4 Config Map

Config maps are unidirectional connections between ingress port(s) to egress port(s) and/or a load balancing group. Ports 1 thru 8 are connected in pairs, 1-2, 3-4, 5-6 and 7-8 via optical splitters. Ports 1 thru 8 may be assigned as an ingress port on a config map. However, ports 1 thru 8 may never be used as an egress port on a config map. If the unit should lose power, traffic connected per the optical splitter pairs, 1-2, 3-4, 5-6 and 7-8 will remain up.

1. Select Create Config Map on the Packet Broker Configurations panel.



Name:

Description:

Available Filters:976/1024
Available Egress Filters:512/512

Load Balancing Groups

Filter Templates

The Create Config Map panel will be displayed. Any previously created load balancing groups or filter templates will be displayed along with the new options. Any port shaded gray can be used for a config map, any port shaded black may not be used.

2. Select the Name pencil icon to apply a name, optional. If no name is entered the system will automatically apply a name to the config maps as follows, map, map(1), map(2) etc.

3. Place the cursor in the Name panel and enter the name.

4. Select the Check to apply.

5. Select the Description pencil to apply a description, optional.

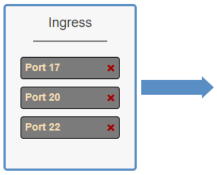
6. Place the cursor in the Description panel and enter the description.

7. Select the Check to apply updates.

3.4.1 Ingress

1. Add an ingress port by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Ingress panel and release. Ports may be added in any combination. If multiple ports are added, then the traffic from all ingress ports will be aggregated.

Figure 1 Ingress



2. Remove a port by selecting the red X.

3.4.2 Filter

1. Add filters by placing the cursor on the desired filter template. A previously created filter template or the new filter template option may be selected. Select with the left mouse button. Drag the filter template to the Filter panel and release. The filter template will become an actual filter once the config map is saved.

Filters may be added in any combination. If multiple filters are added, then the top filter is the highest priority. The filters are considered from top to bottom. A filter may be selected and moved up or down depending on priority preference.

Figure 2 Filter

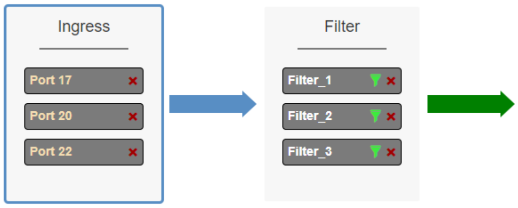
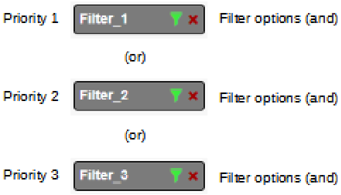


Figure 3 Filter System Considerations



2. Filter templates may be modified by selecting the green filter icon for the desired template.

The Edit Filter panel will be displayed.

Any option modification made will not change the origional template. It is advisable to rename a filter if the original filter template options were modified.

3. Enter the filter name, optional. If no name is entered the system will automatically apply a name to the filter as follows, iFlt, iFlt(2), iFlt(3) etc.

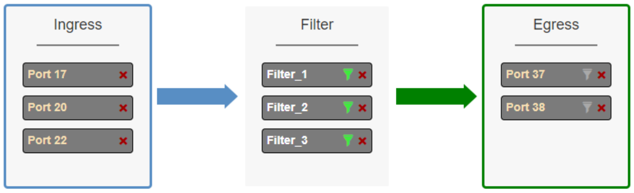
4. Select Accept once all desired options have been modified.

5. Remove a Filter Template by selecting the red X.

3.4.3 Egress

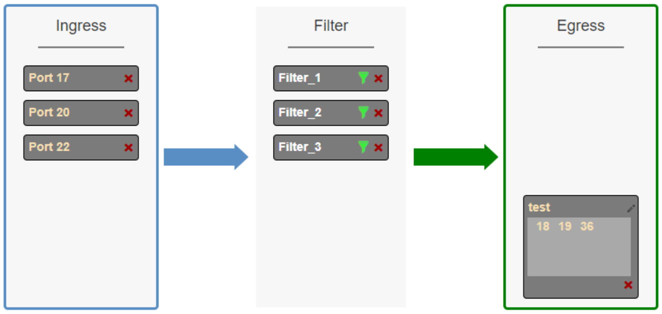
1. Add an egress port by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Egress panel and release. Repeat for all desired ports. If multiple ports are added, then 100% of the traffic will be sent to each port.

Figure 4 Egress Port(s)



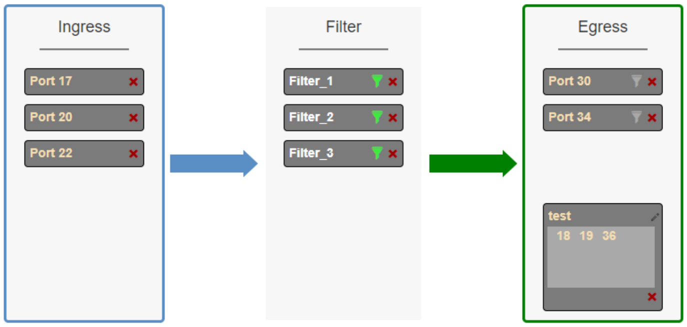
2. Add a load balancing group by placing the cursor on a previously created load balancing group or new load balancing group. Select with the left mouse button. Drag the load balancing group to the Egress panel and release. Ports may be added or removed from any load balancing group. If ports are added or removed from a previously created load balancing group, the origional load balancing group will also be modified.

Figure 5 Egress Load Balancing Group



3. One load balancing group plus separate port(s) may be applied. The traffic applied to the ports assigned to the load balancing group will follow the hashing per the load balancing policy. 100% of the traffic will be sent to each of the separate port(s).

Figure 6 Egress Load Balancing Group and Port(s)

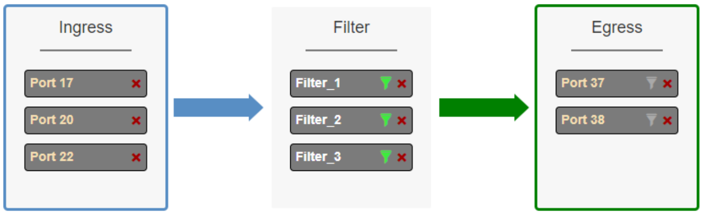


4. Remove a port or load balancing group by selecting the red X.

3.4.4 Egress Filter

1. Select the gray filter icon on the desired egress port.

Figure 7 Egress Filter



The Port XX Egress Filters panel will be displayed.

2. Add filters by placing the cursor on the desired filter template. A previously created filter template or the new filter template option may be selected. Select with the left mouse button. Drag the filter template to the Port XX Egress Filters panel and release. The filter template will become an actual egress filter once the config map is saved.

Filters may be added in any combination. If multiple filters are added, then the top filter is the highest priority. The filters are considered from top to bottom. A filter may be selected and moved up or down depending on priority preference.

Figure 8 Port XX Egress Filters

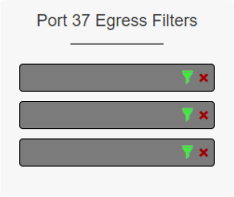
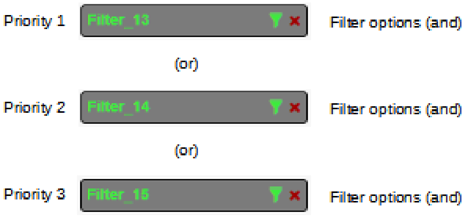


Figure 8 Egress Filter System Considerations



3. If new is selected, the Edit Filter panel will displayed.

4. Enter the filter name, optional. If no name is entered the system will automatically apply a name to the egress filter as follows, eFltPXX, eFltPXX(2), eFltPXX(3) etc.

4. Select Accept once all desired options have been modified.

5. Remove a filter template by selecting the red X.

3.4.5 Config Map Save

1. Select Save to save the current configuration.

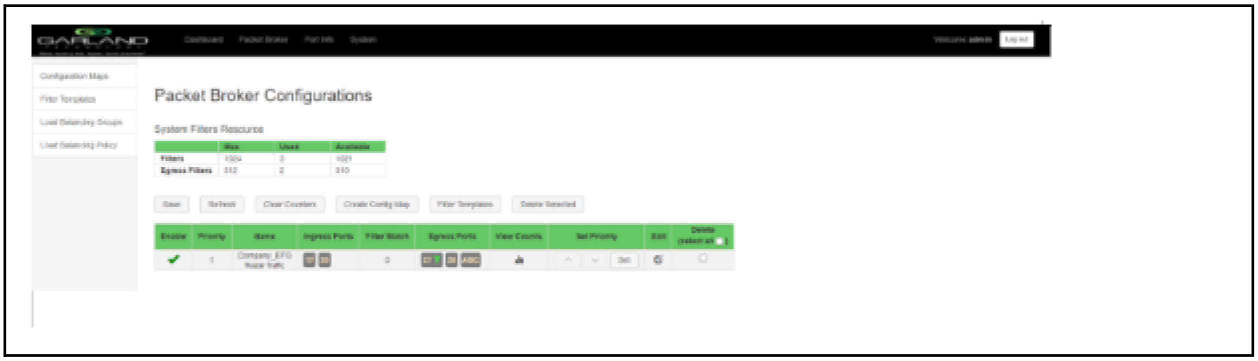
The “Save this configuration? (May take a few seconds.)” panel will be displayed.

2. Select OK to save the Config Map.

3. Select Cancel to disregard.

3.4.6 Modify a Config Map

1. Modify a config map by selecting the Edit icon. Modifications may be made using the create sections previously discussed.



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	2	510

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Company_EFG Route Traffic	17 20	3	27 26 ABC		Set		□

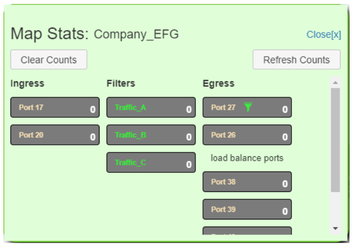
3.4.7 Config Map Statistics

Config map statistics are displayed in the filter match column for each config map. The number displayed represents all packets that have passed through the config map.

1. Select Refresh to refresh the config map statistics.

2. Select Clear Counters to clear and refresh the config map statistics.

3. Select the View Counts icon to display individual statistics for ingress ports, filters, egress ports and load balancing group ports.



Map Stats: Company_EFG

Ingress	Filters	Egress
Port 17 0	Traffic_A 0	Port 27 0
Port 20 0	Traffic_B 0	Port 26 0
	Traffic_C 0	load balance ports
		Port 38 0
		Port 39 0

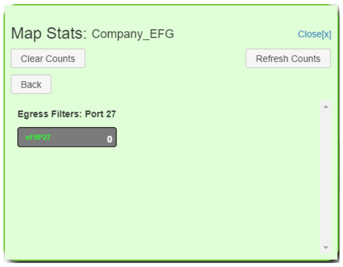
4. Select Refresh Counts to refresh the statistics.

5. Select Clear Counts to clear and refresh the statistics.

6. Select the Egress Filter icon to display the egress filter statistics.

7. Select Refresh Counts to refresh the statistics.

8. Select Clear Counts to clear and refresh the statistics.



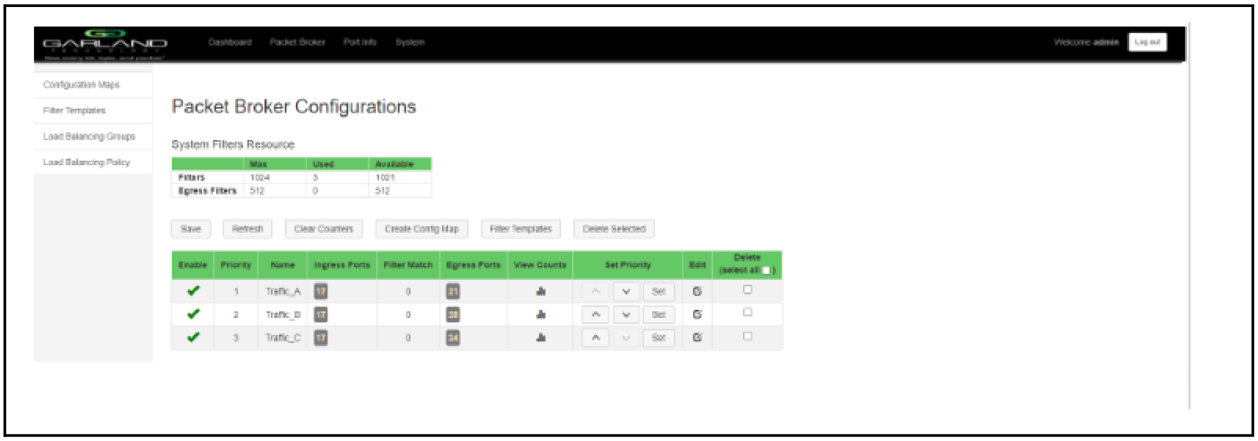
Map Stats: Company_EFG

Egress Filters: Port 27

eFilt27 0

3.4.8 Delete Config Map

1. Select the Delete in the Delete column for the desired config map(s).



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

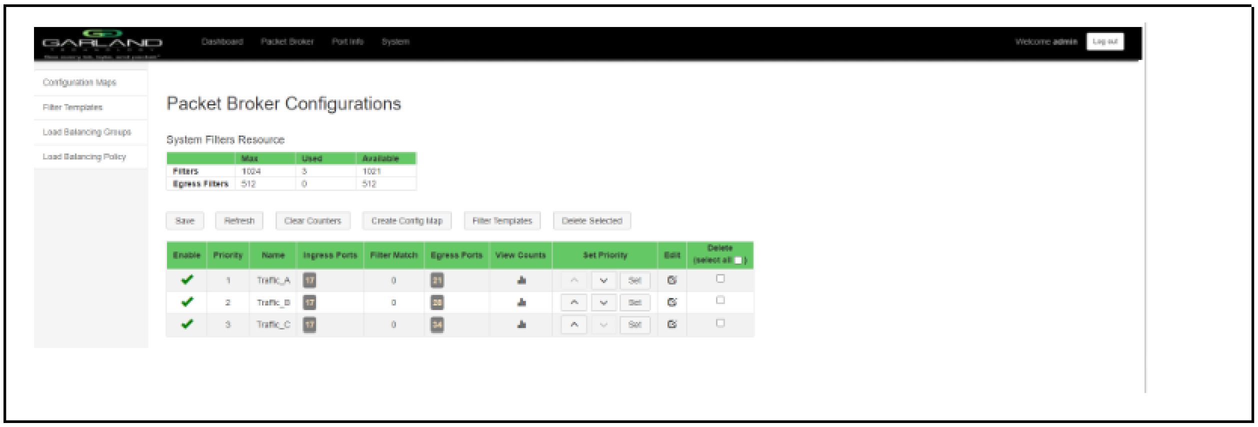
Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Trafic_A	17	0	21		^ ˅ Set		□
✓	2	Trafic_B	17	0	28		^ ˅ Set		□
✓	3	Trafic_C	17	0	34		^ ˅ Set		□

2. The Select All option may be selected to delete all config maps.

3. Select Delete Selected.

3.4.9 Config Map Priority

The config map priority needs to be considered when the same ingress port(s) is used in multiple config maps to send traffic to multiple egress options, ie, different port(s) or load balancing groups. In this case, the config map with the highest priority will be considered first. In the following example there are three config maps with ingress port 17. The Traffic_A config map is the highest priority 1, the Traffic_B config map is the next priority 2 and finally the Traffic_C is the next priority 3.



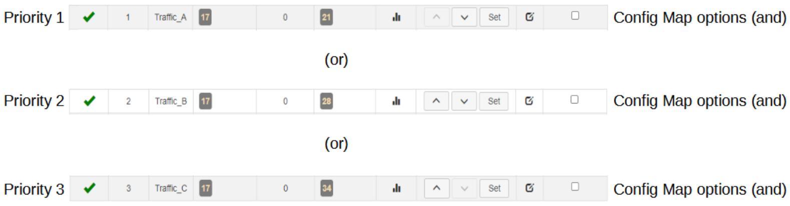
Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Trafic_A	17	0	21		^ ˅ Set		□
✓	2	Trafic_B	17	0	28		^ ˅ Set		□
✓	3	Trafic_C	17	0	34		^ ˅ Set		□

Figure 9 Config Map System Considerations



Priority 1	✓	1	Traffic_A	17	0	21	▮	^ v	Set	☐	□	Config Map options (and)
Priority 2	✓	2	Traffic_B	17	0	28	▮	^ v	Set	☐	□	Config Map options (and)
Priority 3	✓	3	Traffic_C	17	0	34	▮	^ v	Set	☐	□	Config Map options (and)

The Priority of a config map may be changed to a higher or lower value using two methods.

3.4.9.1 Method 1

1. Select the up or down arrow for the config map.

2. Select Save to save updates.

3.4.9.2 Method 2

1. Select Set.

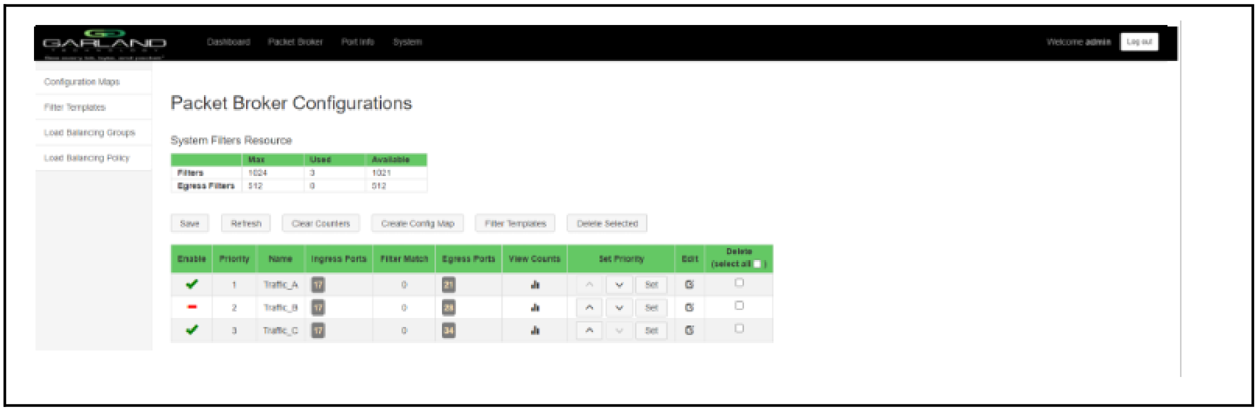
The Set Priority panel will be displayed.

2. Enter the priority in the Set New Priority panel.

3. Select Set to accept the priority value.

4. Select Cancel to disregard.

5. Select Save to save updates.



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Traffic_A	17	0	21	▮	^ v Set	☐	□
−	2	Traffic_B	17	0	28	▮	^ v Set	☐	□
✓	3	Traffic_C	17	0	34	▮	^ v Set	☐	□

3.4.10 Enable/Disable Config Map

Config maps may be enabled or disabled as desired. If a config map is enabled, it is in the database and available for traffic. If a config map is disabled, it is in the database and not available for traffic. If the config map has a green check, then it is enabled. If the config map has a red dash, then it is disabled.

3.4.10.1 Disable Config Map

1. Select the green check for the config map in the Enable column.

   The green check will change to a red dash.

2. Select Save.

3.4.10.2 Enable Config Map

1. Select the red dash for the config map in the Enable column.

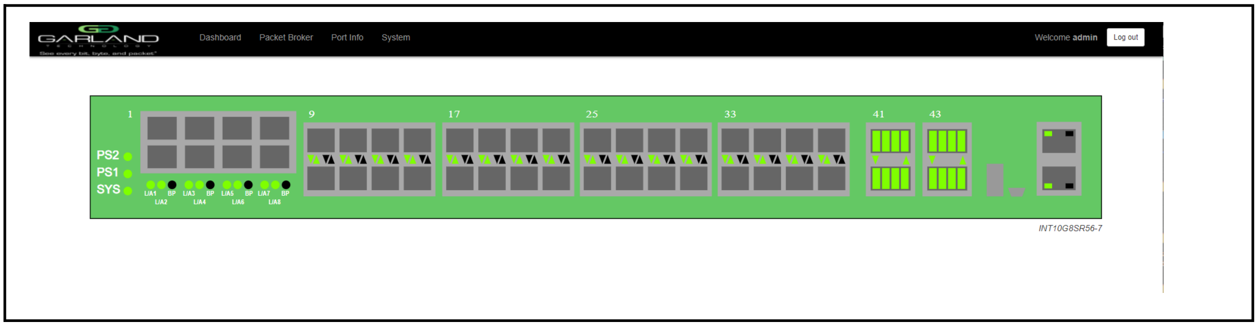
   The red dash will change to a green check.

2. Select Save.

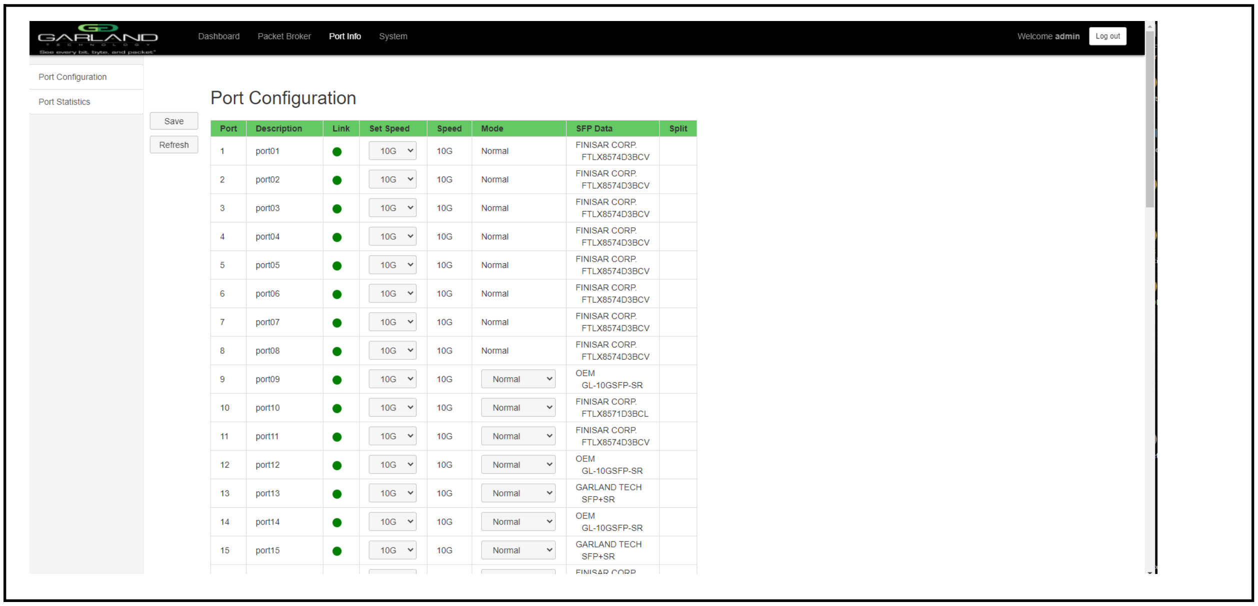
4 Port Info

The following configuration options may be displayed, modified, cleared or refreshed under the Port Info panel.

Port Number
Port Description
Link
Set Speed
Speed
Mode
SFP Data
Split
Port Statistics



1. Select Port Info on the Dashboard menu bar.



Port Configuration

Port	Description	Link	Set Speed	Speed	Mode	SFP Data	Split
1	port01	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
2	port02	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
3	port03	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
4	port04	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
5	port05	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
6	port06	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
7	port07	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
8	port08	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
9	port09	●	10G	10G	Normal	OEM GL-10GSFP-SR	
10	port10	●	10G	10G	Normal	FINISAR CORP. FTLX8571D3BCL	
11	port11	●	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
12	port12	●	10G	10G	Normal	OEM GL-10GSFP-SR	
13	port13	●	10G	10G	Normal	GARLAND TECH SFP+SR	
14	port14	●	10G	10G	Normal	OEM GL-10GSFP-SR	
15	port15	●	10G	10G	Normal	GARLAND TECH SFP+SR	

The Port Configuration panel will be displayed.

4.1 Port Configuration

The port configuration is displayed by default. The Port Description, Set Speed and Mode may be modified. All other options are displayed only. However, they may be updated by selecting Refresh.

4.1.1 Port Description

1. Modify the port description by placing the cursor on Port Description for the desired port and press the left mouse button.

   The Edit Description panel will be displayed.

2. Place the cursor in the description field and enter the new description.

3. Select Set to save updates.

4. Select Cancel to return to the Port Configuration panel.

4.1.2 Set Speed

1. Modify the port speed by selecting the pull down panel for the desired port.

2. Select the desired speed.

3. Select Save to save updates.

4.1.3 Mode

1. Modify the port mode by selecting the pull down panel for the desired port.

2. Select the desired mode. The available port modes are Normal, Loopback, Listen Only and Force Link.

3. Select Save to save updates.

4.1.4 Port Statistics

The following statistics may be displayed on the Port Statistics panel.

Port number
Receive Packets
Receive Discards
Receive Errors
Transmit Packets
Transmit Discards
Transmit Errors

1. Select Port Statistics on the Port Configuration panel.

   The Port Statistics panel will be displayed.

2. Update the statistics by selecting Refresh.

3. Clear and refresh the statistics by selecting Clear.