



See every bit, byte, and packet[®]

XtraTAP Portable Packet Broker

P10GXXFE-X | 1.19.3

User Manual

Introduction	4
Additional Specifications	4
1 Dashboard	5
1.1 Filter TAP	5
1.2 Span	5
1.3 Breakout	6
1.4 Filter	6
1.5 Aggregate	7
2 System	8
2.1 System Info	9
2.2 General	9
2.3 Admin	9
2.3.1 Groups	10
2.3.2 Users	10
2.3.3 Authentication	11
2.4 Network Settings	12
2.5 Date & Time	13
2.6 Syslog	13
2.7 SNMP	14
2.8 Export Configuration	14
2.9 Import Configuration	15
2.10 Software Upgrade	15
2.11 Reboot	16
3 Filter Mode	17
3.1 Filter Templates	19
3.2 Config Maps	20
3.2.1 Config Maps	21
3.2.2 Ingress	21
3.2.3 Filter	22
3.2.4 Egress	22
3.2.5 Config Map Save	23
3.2.6 Modify a Config Map	23
3.2.7 Config Map Statistics	24
3.2.8 Delete Config Map	24
3.2.9 Config Map Priority	25
3.2.9.1 Method 1	25
3.2.9.2 Method 2	25
3.2.10 Enable and Disable Config Map	26
3.2.10.1 Disable Config Map	26

3.2.10.2 Enable Config Map	26
4 Port Information	27
4.1 Port Configuration	27
4.2 Port Description	27
4.3 Set Speed	28
4.4 Mode	28
4.5 Port Statistics	28
5 Span Mode	29
5.1 Port Configuration	30
5.1.1 Port Description	30
5.1.2 Set Speed	31
5.1.4 Mode	31
5.1.5 Port Statistics	31
6 Breakout Mode	32
6.1 Port Configuration	33
6.1.1 Port Description	33
6.1.2 Set Speed	34
6.1.3 Mode	34
6.1.4 Port Statistics	34
7 Aggregate Mode	35
7.1 Port Configuration	36
7.1.1 Port Description	37
7.1.2 Set Speed	37
7.1.3 Mode	37
7.1.4 Port Statistics	37
8 Filter Tap Mode	38

Copyright © 2022 Garland Technology, LLC. All rights reserved.

No part of this document may be reproduced in any form or by any means without prior written permission of GarlandTechnology, LLC.

The Garland Technology trademarks, service marks ("Marks") and other Garland Technology trademarks are the property of Garland Technology, LLC. PacketMAX Series products of marks are trademarks or registered trademarks of Garland Technology, LLC. You are not permitted to use these Marks without the prior written consent of Garland Technology.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Garland Technology and the customer. All or part of the products, services, and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees, or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Introduction

The XtraTAPTTM: Portable Packet Brokers are purpose-built active network TAPs that support filtering, tap 'breakout,' aggregation, bypass, and regeneration/SPAN modes guaranteeing your tools see every bit, byte, and packet.®

This advanced TAP with Packet Broker functionality provides the ultimate flexibility and ease of use for a range of solutions, from providing media conversion, to easily filtering out the traffic that is not used or filtering only the traffic needed to monitor. Leading to optimized tool performance, with better visibility and reduced processing burden with unneeded data.

Additional Specifications

Voltage: 5V DC +/-5%

Current: < 6 Amps

Max. Power Consumption (Fiber SFP): < 15 Watts

Max Power Consumption (Copper): < 22 Watts

Ambient Temperature: 0C to +40C / +32F to +104F

Operating Re. Humidity: 90% non-condensing

Dimensions (HxWxD): 1.3" x 3.9" x 9.43"

33.02mm x 99.06mm x 239.552mm

Weight: 1.0 lbs

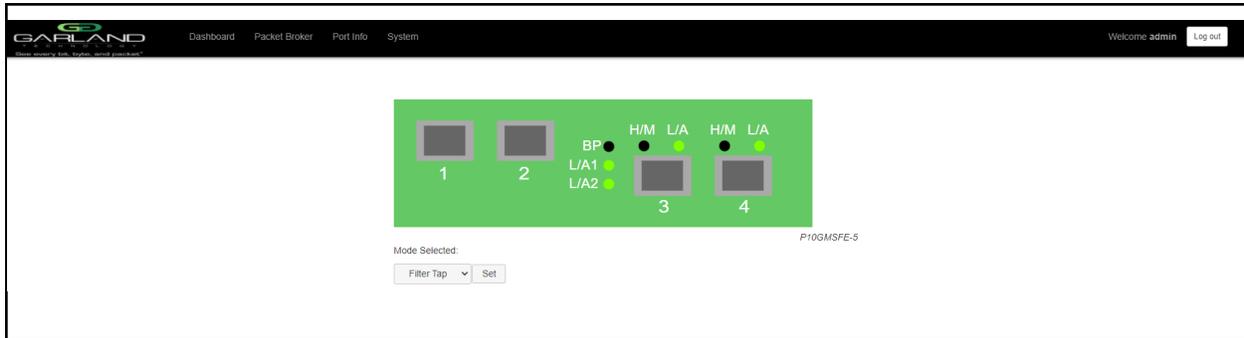
0.4539592 kg



1 Dashboard

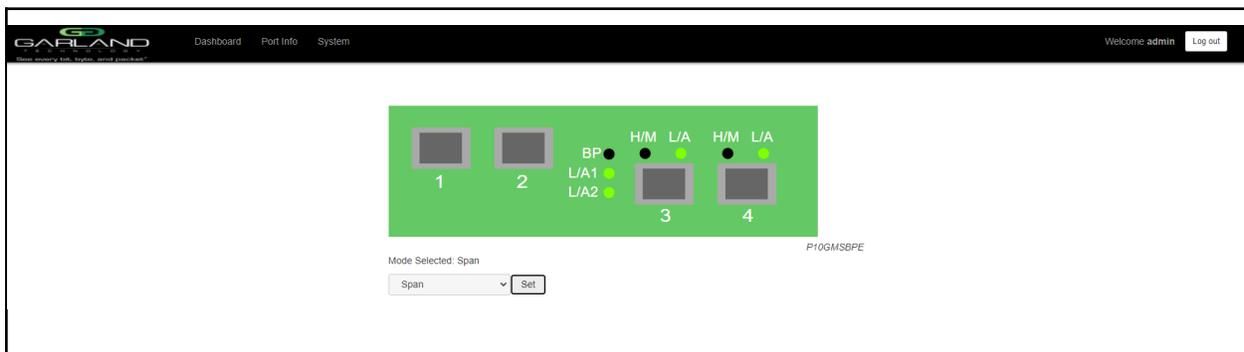
The P10GXXFE-X supports multiple modes of operation, Filter Tap, Span, Breakout, Filter and Aggregate. The dashboard, specifically the port function, menu bar options, and LED operation will vary based on the mode selected.

1.1 Filter TAP



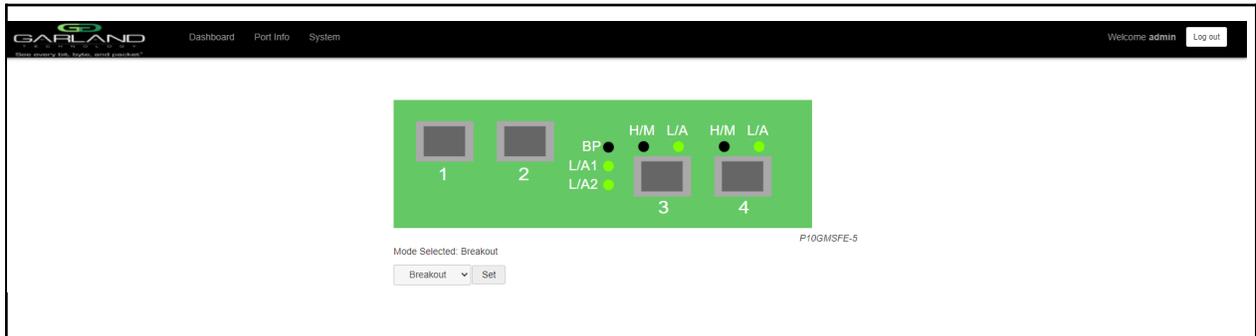
Port 1 - L/A1	Network Port Link/Activity LED
Port 2 - L/A2	Network Port Link/Activity LED
BP	N/A
Port 3 - L/A	Breakout / Aggregate Port Link/Activity LED
Port 3 - H/M	N/A
Port 4 - L/A	Breakout / Aggregate Port Link/Activity LED
Port 4 - H/M	N/A

1.2 Span



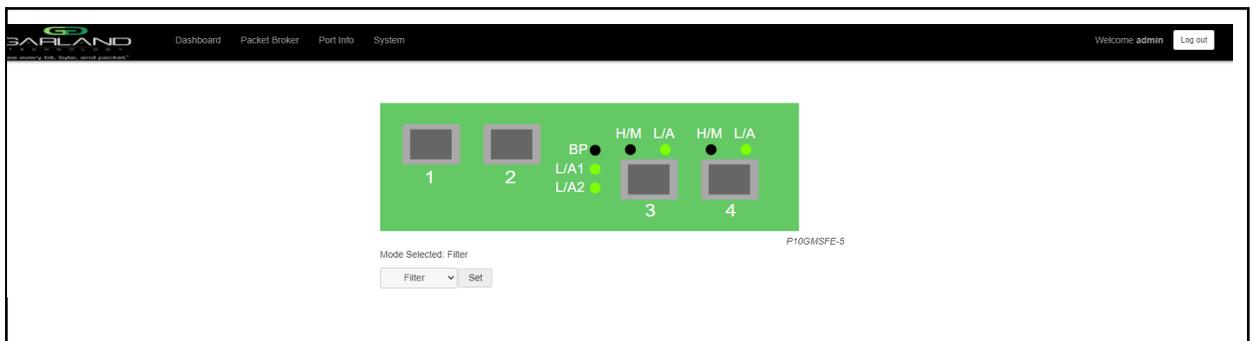
Port 1 - L/A1	Network Port Link/Activity LED
Port 2 - L/A2	Span Port Link/Activity LED
BP	N/A
Port 3 - L/A	Span Port Link/Activity LED
Port 3 - H/M	N/A
Port 4 - L/A	Span Port Link/Activity LED
Port 4 - H/M	N/A

1.3 Breakout



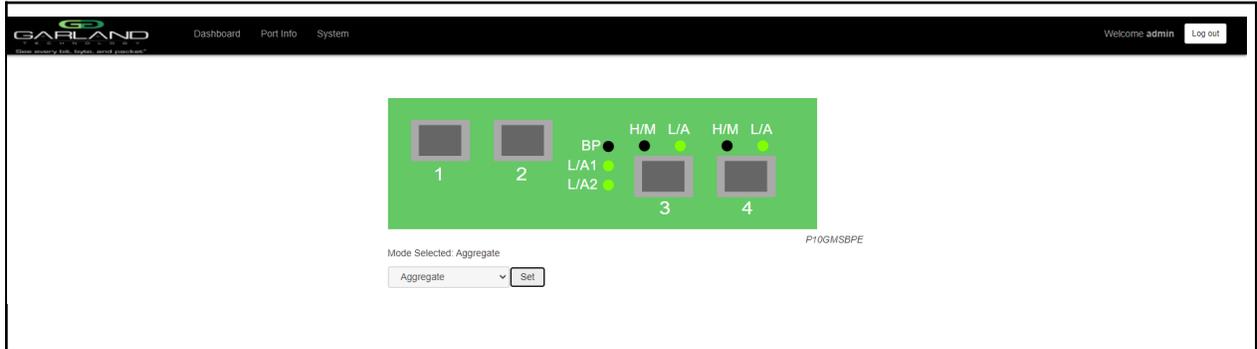
Port 1 - L/A1	Network Port Link/Activity LED
Port 2 - L/A2	Network Port Link/Activity LED
BP	N/A
Port 3 - L/A	Breakout Port Link/Activity LED
Port 3 - H/M	N/A
Port 4 - L/A	Breakout Port Link/Activity LED
Port 4 - H/M	N/A

1.4 Filter



Port 1 - L/A1	Filter Port Link/Activity LED
Port 2 - L/A2	Filter Port Link/Activity LED
BP	N/A
Port 3 - L/A	Filter Port Link/Activity LED
Port 3 - H/M	N/A
Port 4 - L/A	Filter Port Link/Activity LED
Port 4 - H/M	N/A

1.5 Aggregate



Port 1 - L/A1
 Port 2 - L/A2
 BP
 Port 3 - L/A
 Port 3 - H/M
 Port 4 - L/A
 Port 4 - H/M

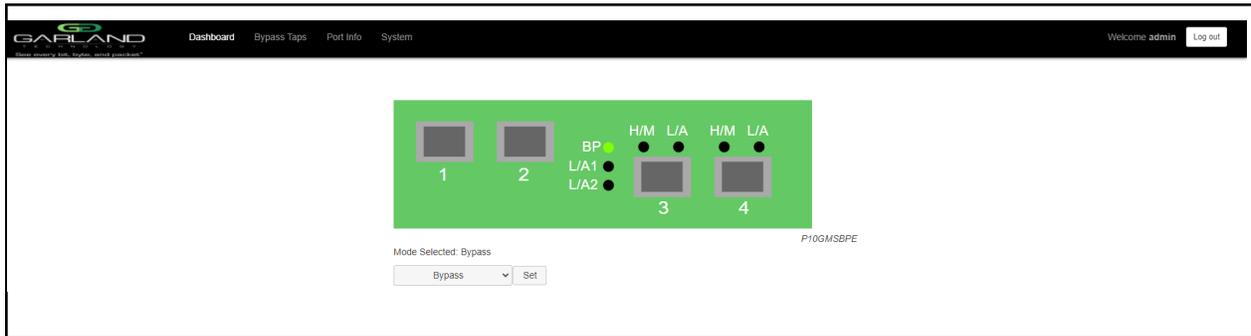
Network Port Link/Activity LED
 Network Port Link/Activity LED
 N/A
 Aggregate Port Link/Activity LED
 N/A
 Aggregate Port Link/Activity LED
 N/A

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.



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 the 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	DNS 1
IP Address	DNS 2
Mask	SSL Certificate Loaded
Gateway	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 an SSL cert.pem and key.pem files 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 an 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	Time
UTC	Date
NTP IP Address	
NTP Pool	

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	Syslog Server IP Address
Protocol	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	
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.

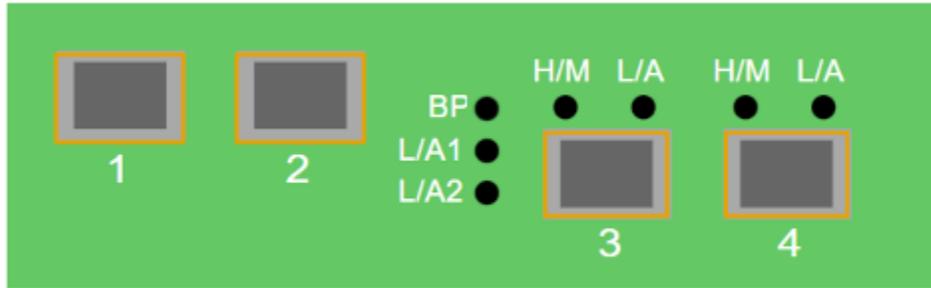
A “Session timed out. Go to Login screen” message will be displayed.

4. Select Go.

The Login panel will be displayed.

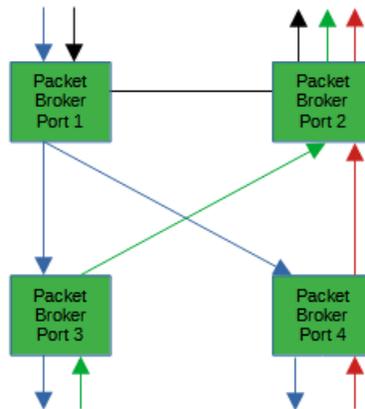
3 Filter Mode

In this mode, the unit functions as a 4 port packet broker. The traffic that is passed between the ports is determined by the config map(s) and filter(s) created. Config maps may be created between all four ports as desired.



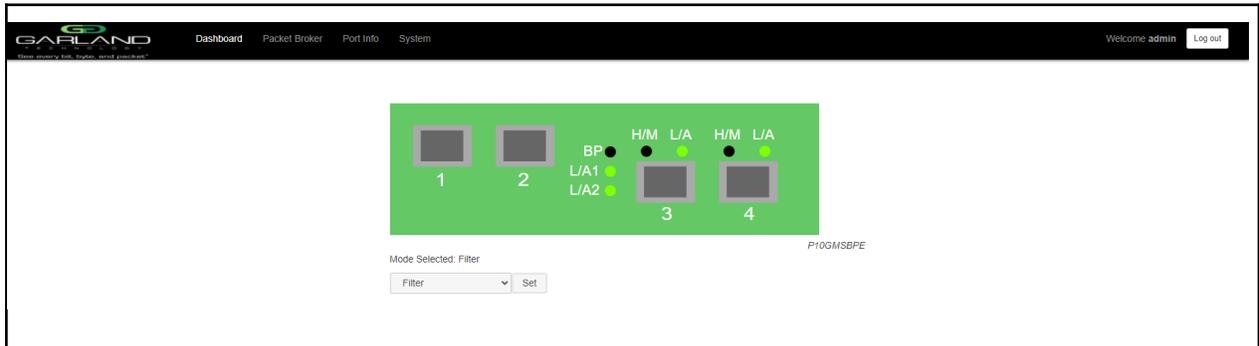
Port 1 (Packet Broker)
 Port 2 (Packet Broker)
 Port 3 (Packet Broker)
 Port 4 (Packet Broker)

Figure 1 Filter Mode

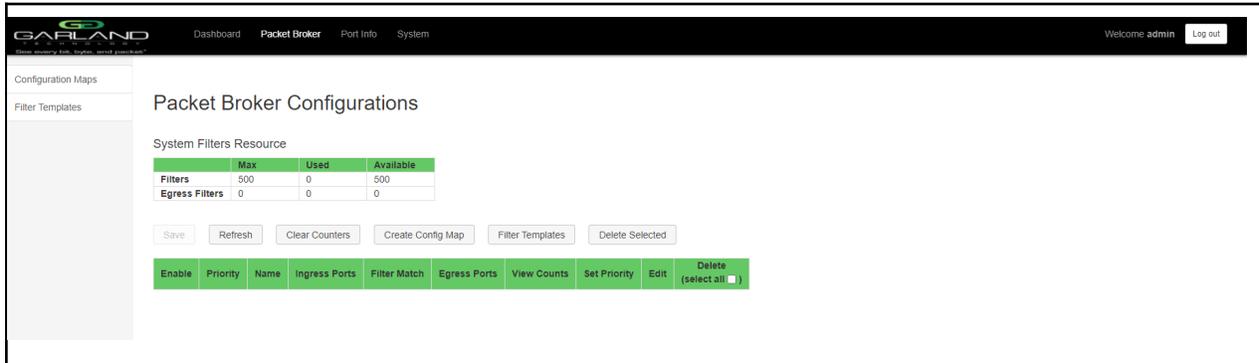


The following configuration options may be displayed, modified, enabled, or disabled under the Packet Broker panel.

- Filter Templates
- Config Maps
- Statistics



1. Select Packet Broker on the Dashboard Menu bar.



3.1 Filter Templates

Filter templates may be created as a pass-all, pass-by, or deny-by. Pass by or 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 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 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.

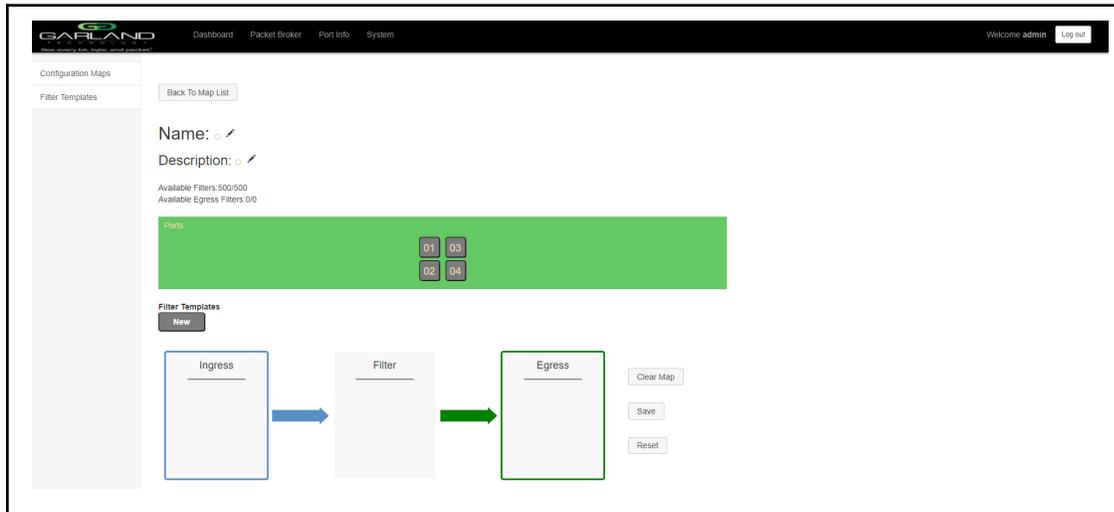
- Source MAC Address / Source MAC Mask
- Destination MAC Address / Destination MAC Mask
- Ether Type
- Source IP Address / Source IP Mask
- Destination IP Address / Destination IP Mask
- Inner VLAN ID
- Outer VLAN ID
- DSCP
- IP Protocol
- L4 Source Port or Range
- L4 Destination Port or Range

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 Config Maps

Config maps are unidirectional connections between an ingress port to an egress port(s).

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



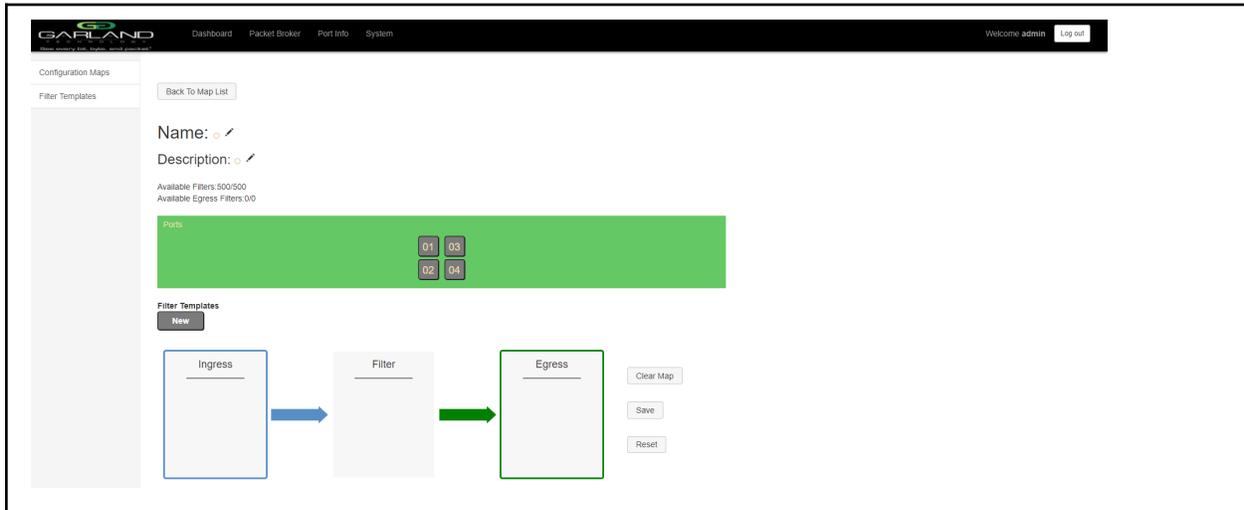
The Create Config Map panel will be displayed. Any previously created filter templates will be displayed along with the new options. Any port shaded gray can be used for a config map, any port shaded black may not be used.

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, optional.
7. Select the Check to apply updates.

3.2.1 Config Maps

Config maps are unidirectional connections between an ingress port to an egress port(s).

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



The Create Config Map panel will be displayed. Any previously created 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.

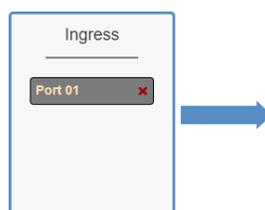
6. Place the cursor in the Description panel and enter the description, optional.

7. Select the Check to apply updates.

3.2.2 Ingress

1. Add an ingress port(s) 1 and/or 2 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 ports 1 and 2 are added, then the traffic from the ports will be aggregated.

Figure 2 Ingress



2. Remove a port by selecting the red X.

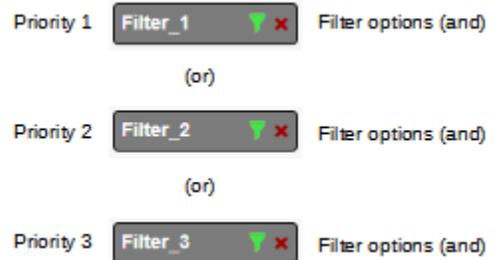
3.2.3 Filter

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 it. 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 3 Filter



Figure 4 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 original 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.

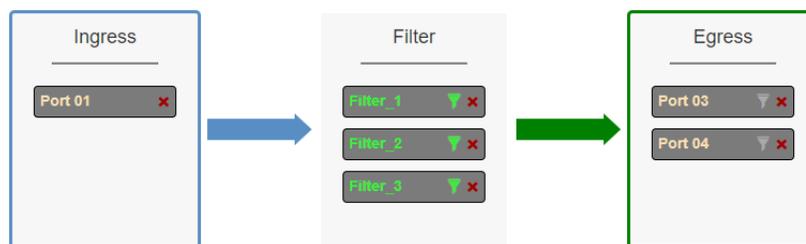
4. Select Accept once all desired options have been modified.

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

3.2.4 Egress

1. Add an egress port(s) by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Egress panel and release. Ports may be added in any combination. If multiple ports are added, then 100% of the traffic will be sent to each port.

Figure 5 Egress Port(s)



2. Remove a port by selecting the red X.

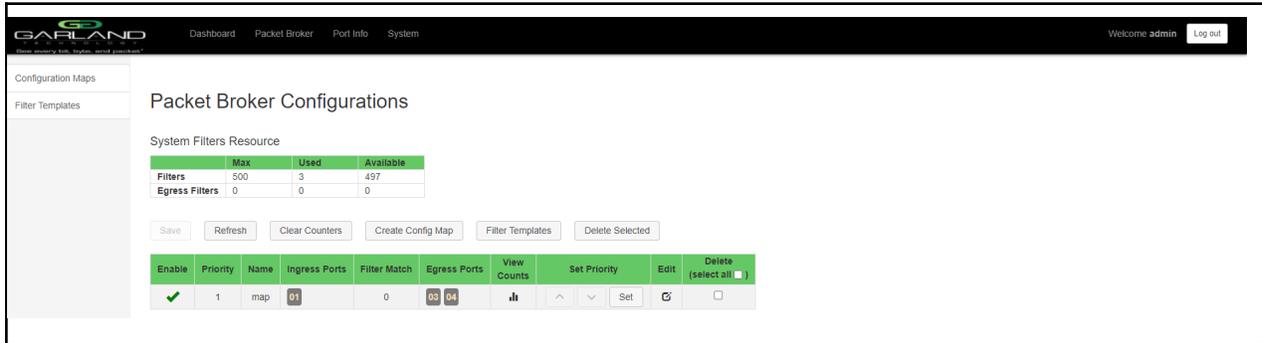
3.2.5 Config Map Save

1. Select Save to save the current configuration.

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

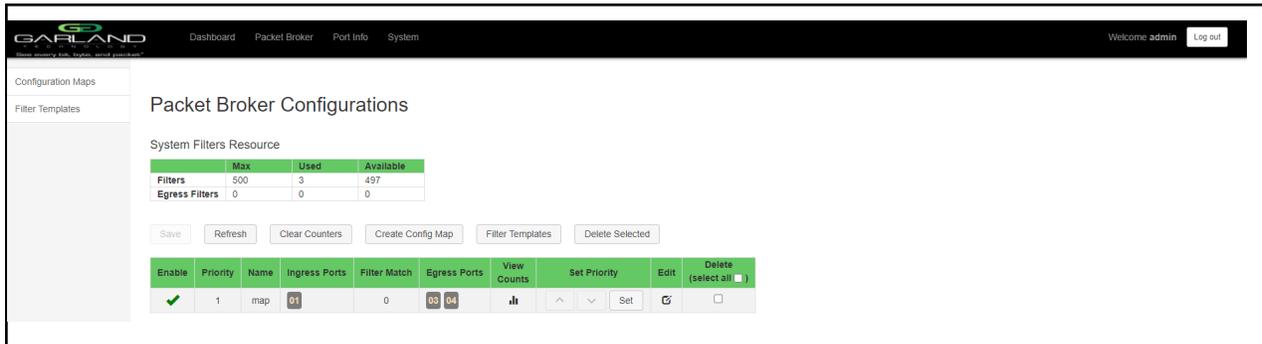
2. Select OK to save the Config Map.

3. Select Cancel to disregard.



3.2.6 Modify a Config Map

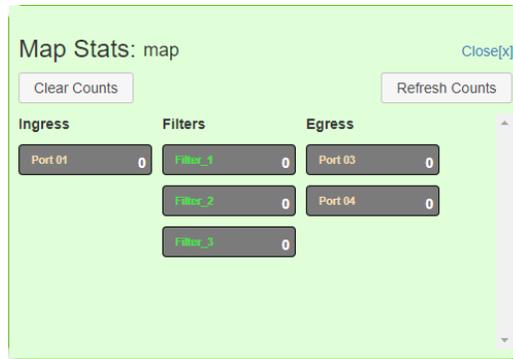
1. Modify a config map by selecting the Edit icon. Modifications may be made using the create sections previously discussed.



3.2.7 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.

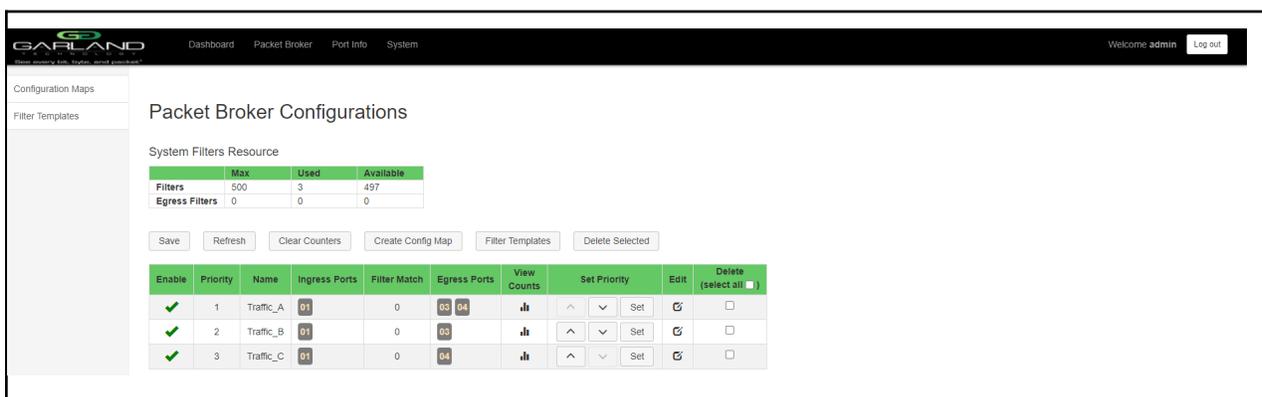
1. Select Refresh to refresh the config map statistics.
2. Select Clear Counters to clear and refresh the config map statistics.
3. Select the View Counts icon to display individual statistics.



4. Select Refresh Counts to refresh the statistics.
5. Select Clear Counts to clear and refresh the statistics.
9. Select Close to return to the Packet Broker Configurations panel.

3.2.8 Delete Config Map

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



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

3.2.9 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 ports. 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 1. 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.

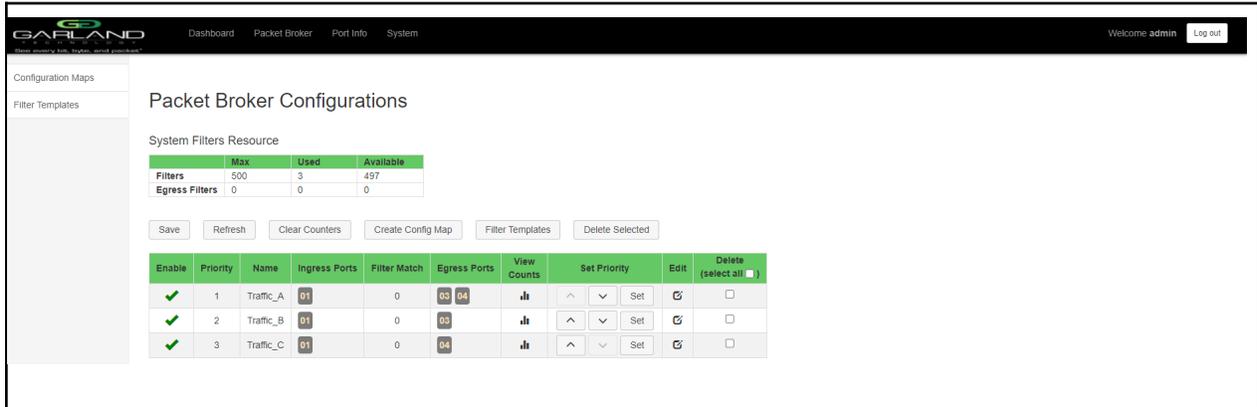


Figure 7 Config Map System Considerations



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

3.2.9.1 Method 1

1. Select the up or down arrow for the config map.
2. Select Save to save updates.

3.2.9.2 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.

3.2.10 Enable and 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.

The screenshot shows the 'Packet Broker Configurations' page. At the top, there's a 'System Filters Resource' table:

	Max	Used	Available
Filters	500	3	497
Egress Filters	0	0	0

Below this are buttons: Save, Refresh, Clear Counters, Create Config Map, Filter Templates, and Delete Selected.

The main table lists configurations:

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all)
<input checked="" type="checkbox"/>	1	Traffic_A	01	0	03 04	▮	^ v Set	✎	<input type="checkbox"/>
<input type="checkbox"/>	2	Traffic_B	01	0	03	▮	^ v Set	✎	<input type="checkbox"/>
<input checked="" type="checkbox"/>	3	Traffic_C	01	0	04	▮	^ v Set	✎	<input type="checkbox"/>

3.2.10.1 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.

3.2.10.2 Enable Config Map

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

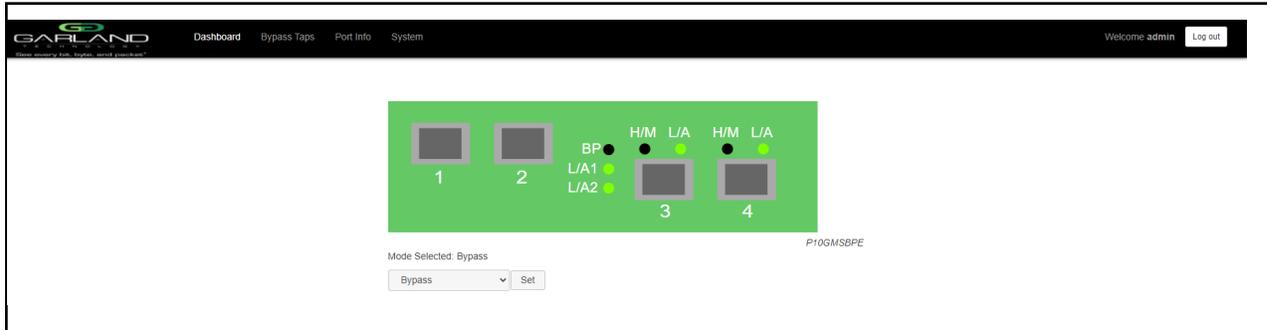
The red dash will change to a green check.

2. Select Save.

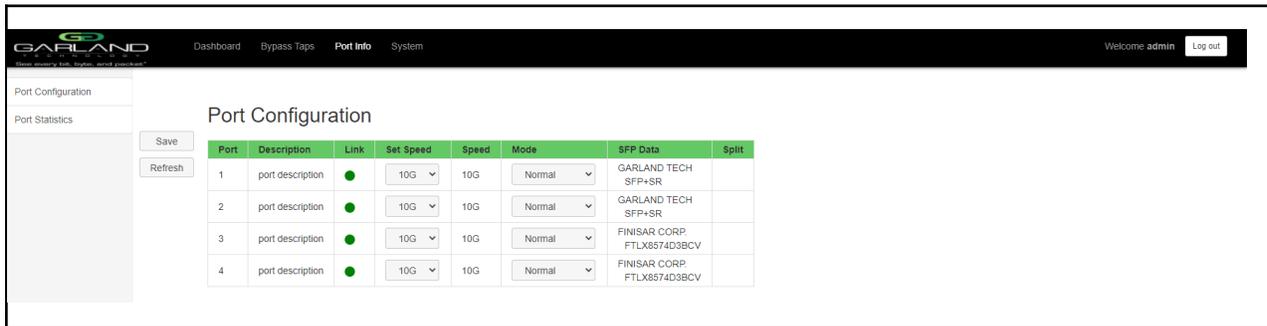
4 Port Information

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

- | | |
|---------------------|--------------------|
| 1. Port Number | 6. Mode |
| 2. Port Description | 7. SFP Data |
| 3. Link | 8. Split |
| 4. Set Speed | 9. Port Statistics |
| 5. Speed | |



1. Select Port Info on the Dashboard menu bar.



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.

4.2 Port Description

1. Modify the port description by placing the cursor on Port Description for the desired port and pressing 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.

4.3 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.

4.4 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.

4.5 Port Statistics

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

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

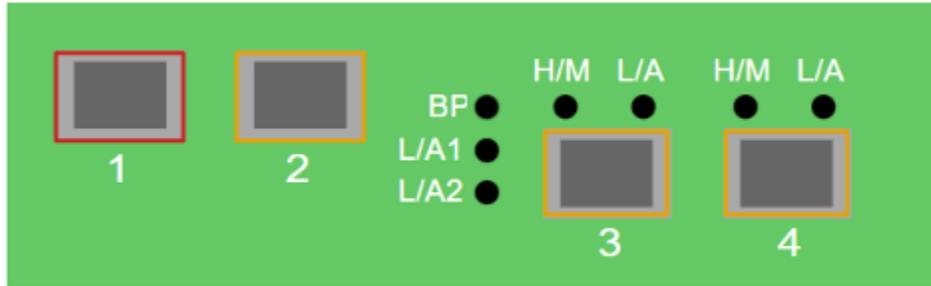
1. Select Port Statistics on the Port Configuration panel.

The Port Statistics panel will be displayed.

2. Update the statistics by selecting Refresh.
3. Clear and refresh the statistics by selecting Clear.

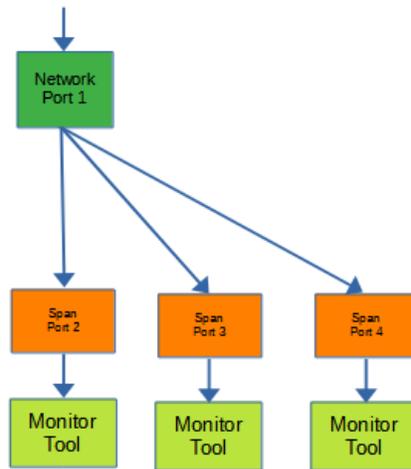
5 Span Mode

In this mode, the network port 1 and span ports 2, 3, and 4 are defined by the system.



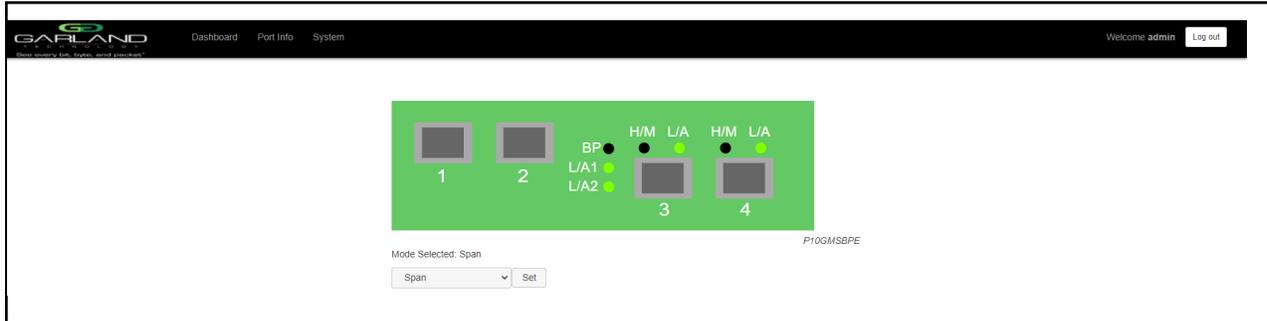
Port 1 (Network)
 Port 2 (Span)
 Port 3 (Span)
 Port 4 (Span)

Figure 1 Span Mode



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

- | | |
|------------------|-----------------|
| Port Number | Speed |
| Port Description | Mode |
| Link | SFP Data |
| Set Speed | Port Statistics |



1. Select Port Info on the Dashboard Menu bar.



The Port Configuration panel will be displayed.

5.1 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.

5.1.1 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.

5.1.2 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.

5.1.4 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.

5.1.5 Port Statistics

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

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

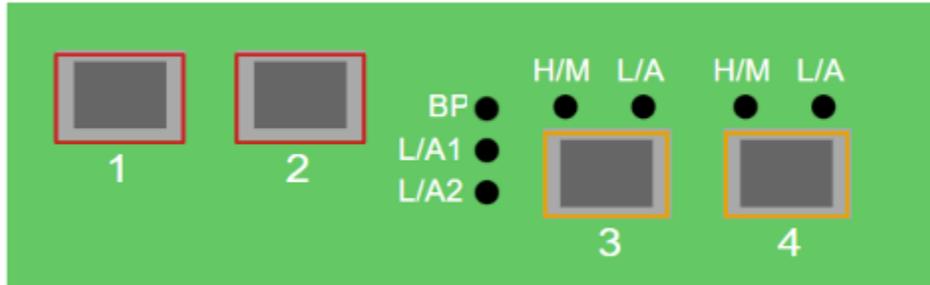
1. Select Port Statistics on the Port Configuration panel.

The Port Statistics panel will be displayed.

2. Update the statistics by selecting Refresh.
3. Clear and refresh the statistics by selecting Clear.

6 Breakout Mode

In this mode, the network ports 1 and 2 and breakout ports 3 and 4 are defined by the system. LFP is supported on the network ports in this mode.



Port 1 (Network)
 Port 2 (Network)
 Port 3 (Breakout)
 Port 4 (Breakout)

Figure 1 Breakout Mode

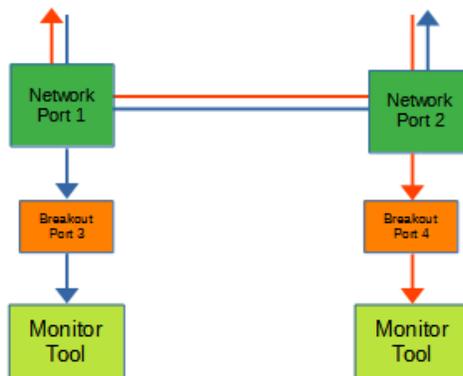


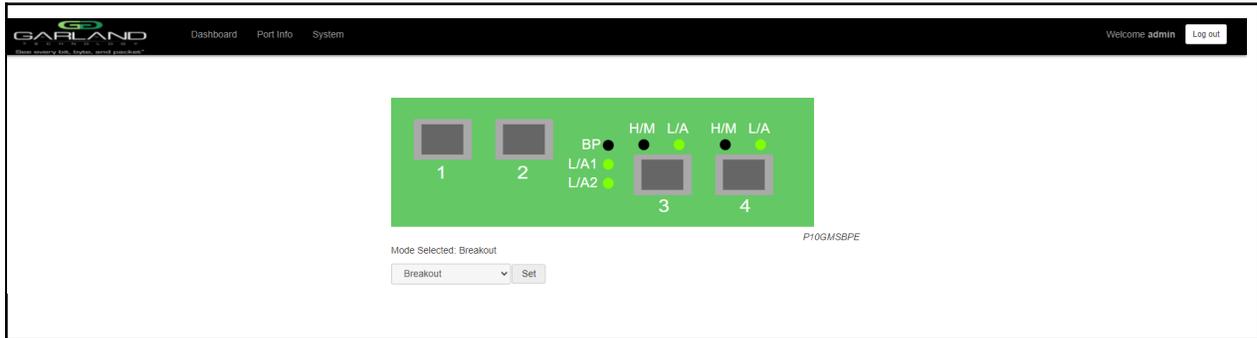
Figure 2 Breakout Mode (LFP)



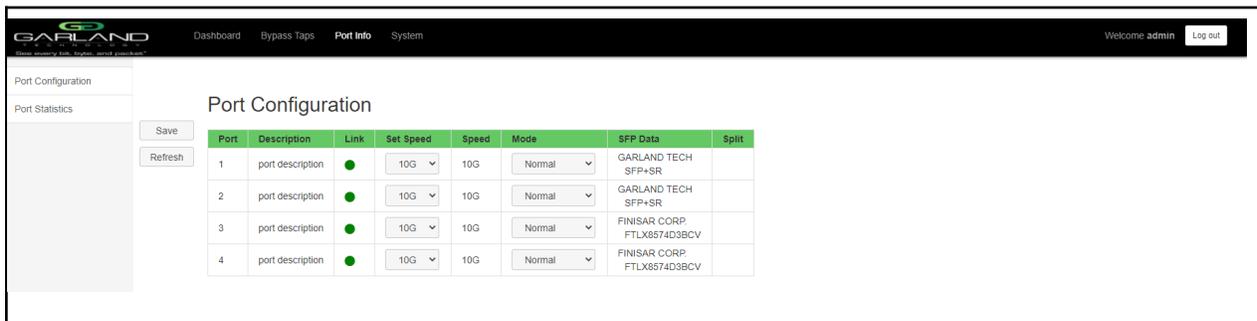
If a link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

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

- | | |
|------------------|-----------------|
| Port Number | Speed |
| Port Description | Mode |
| Link | SFP Data |
| Set Speed | Port Statistics |



1. Select Port Info on the Dashboard Menu bar.



The Port Configuration panel will be displayed.

6.1 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.

6.1.1 Port Description

1. Modify the port description by placing the cursor on Port Description for the desired port and pressing 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.

6.1.2 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.

6.1.3 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.

6.1.4 Port Statistics

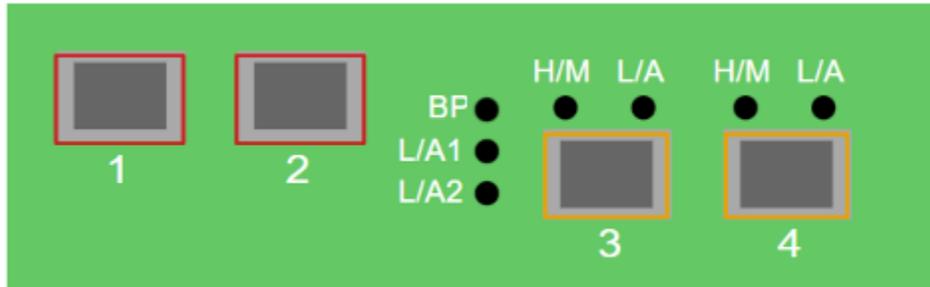
The following statistics may be displayed on the Port Statistics panel.

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

7 Aggregate Mode

In this mode, the network ports 1 and 2 and aggregate ports 3 and 4 are defined by the system. LFP is supported on the network ports in this mode.



Port 1 (Network)
 Port 2 (Network)
 Port 3 (Aggregate)
 Port 4 (Aggregate)

Figure 1 Aggregate Mode

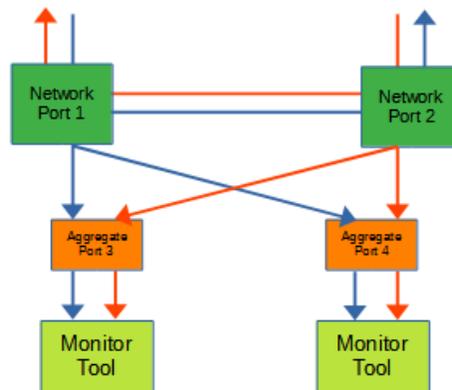
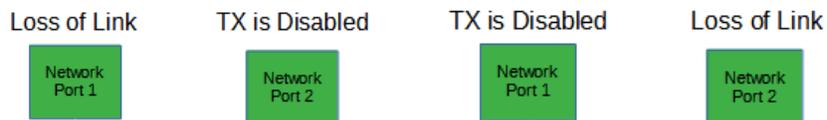


Figure 2 Aggregate Mode (LFP)

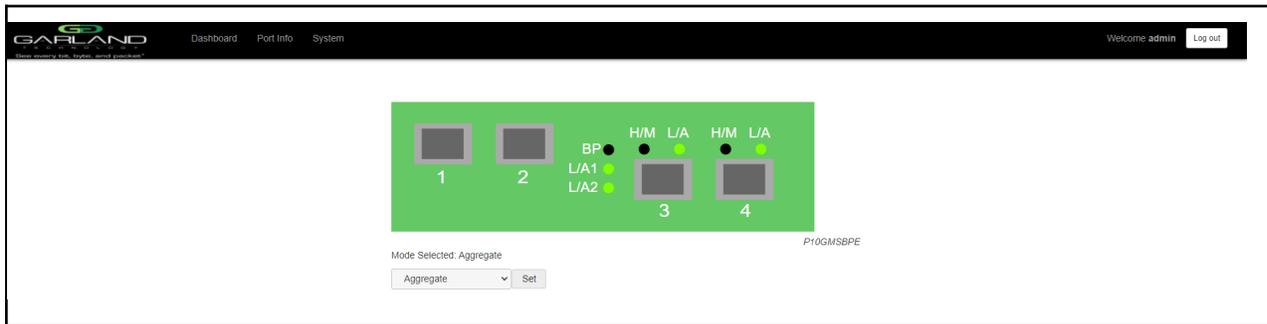


If a link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

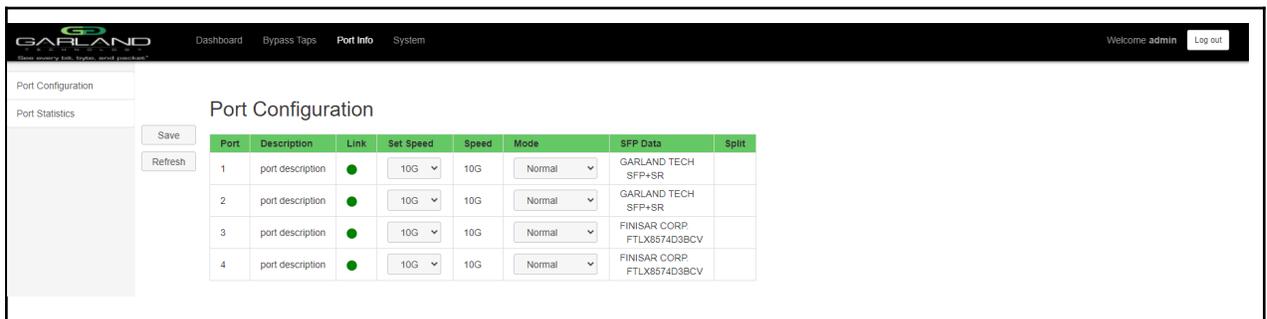
The following configurations may be displayed, modified, cleared, or refreshed under the Port Info panel.

Port Number
Port Description
Link
Set Speed

Speed
Mode
SFP Data
Port Statistics



1. Select Port Info on the Dashboard Menu bar.



The Port Configuration panel will be displayed.

7.1 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.

7.1.1 Port Description

1. Modify the port description by placing the cursor on Port Description for the desired port and pressing 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.

7.1.2 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.

7.1.3 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.

7.1.4 Port Statistics

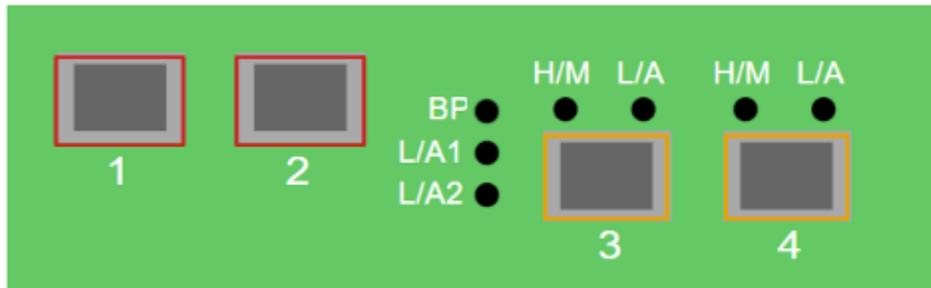
The following statistics may be displayed on the Port Statistics panel.

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

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.

8 Filter Tap Mode

In this mode, the network ports 1 and 2 and filter tap ports 3 and 4 are defined by the system, however, there are no default config maps created between network ports 1 and 2 and filter tap ports 3 and 4. The traffic that is passed to the filter ports is determined by the config map(s) and filter(s) created. Config maps may be created from network port 1 to filter tap port(s) 3 and/or 4 as well as, network port 2 to filter tap port(s) 3 and/or 4. LFP is supported on the network ports in this mode.



Port 1 (Network)
Port 2 (Network)
Port 3 (Filter Tap)
Port 4 (Filter Tap)

Figure 1 Filter Tap Mode

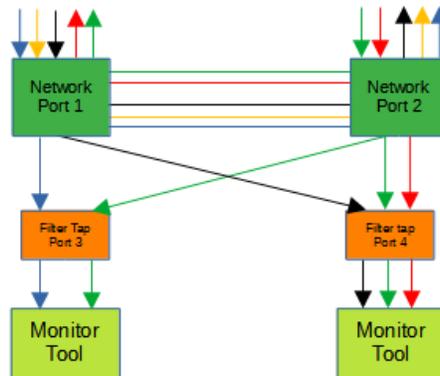


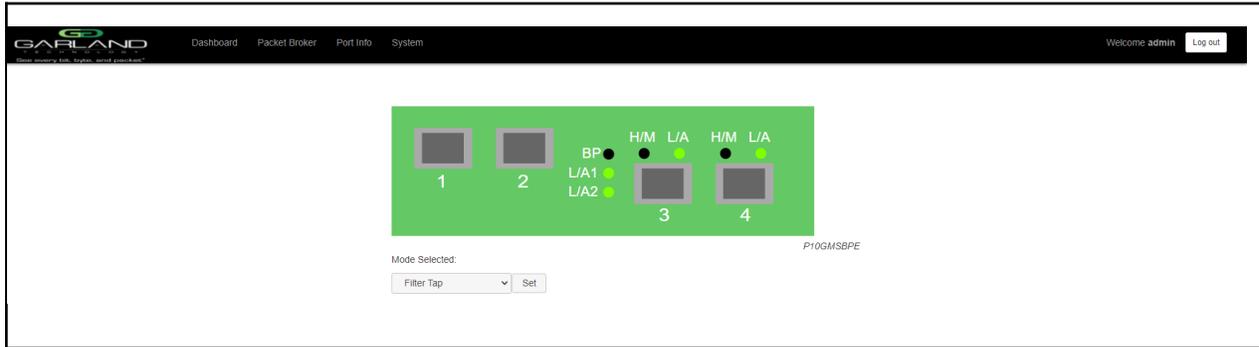
Figure 2 Filter Tap Mode (LFP)



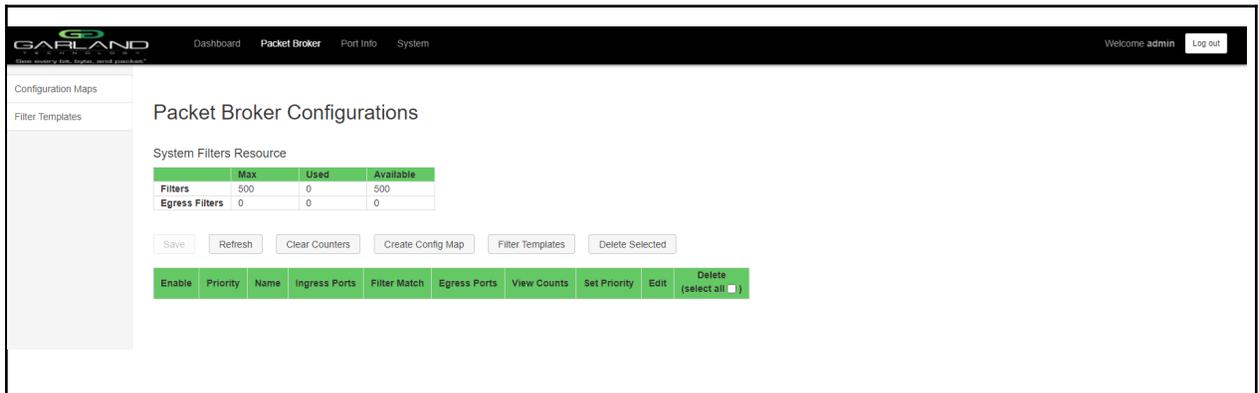
If a link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

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

- Filter Templates
- Config Maps
- Statistics



1. Select Packet Broker on the Dashboard Menu bar.



The Packet Broker Configurations panel will be displayed.

For information on Filter Templates, please go to [Ch 3.1: Filter Templates](#)

For information on Config Maps, please go to [Ch 3.2: Config Maps](#)