GARLAND TECHNOLOGY

See every bit, byte, and packet®

User Guide

P10GSFPBPFE

02/2024

Release Version: 4.29.3

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.

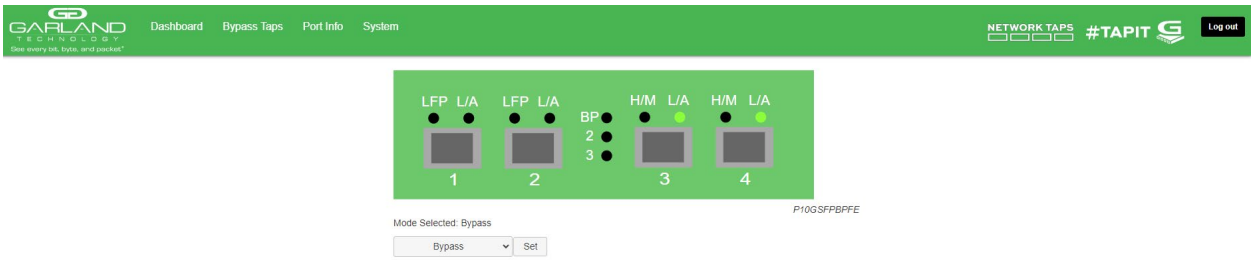
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Table of Contents

Dashboard

This section provides an overview of the dashboard architectures and LED indications. The port assignments and LED indications will change on the dashboard based on the mode configured.
The dashboard provides an exact detail of the unit's faceplate. However, some LED indications that are displayed on the faceplate, are not displayed on the dashboard. The P10GXXBPE supports multiple modes of operation, Bypass, Span, Span Packet Inject, Breakout, Filter, Aggregate, Filter Tap and Bypass Filter.

Bypass Mode

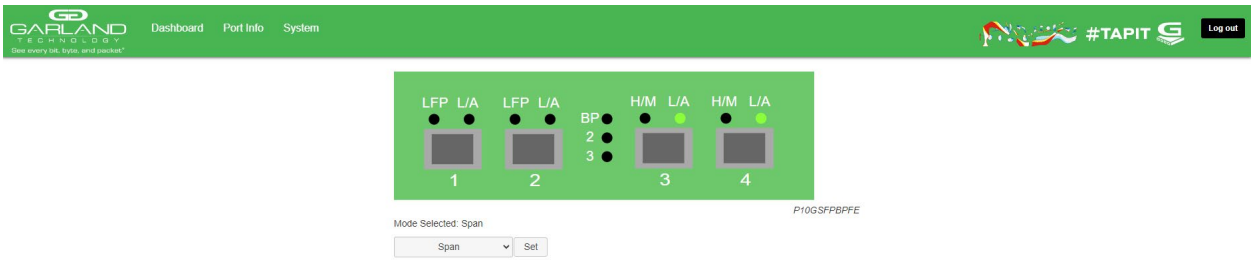


LED Indications

Port 1 L/A1	Network Port Link/Activity LED
Port 2 L/A2	Network Port Link/Activity LED
BP	Bypass LED
Port 3 L/A	Inline Appliance Link/Activity LED
Port 3 H/M	N/A
Port 4 L/A	Inline Appliance Link/Activity LED
Port 4 H/M	N/A

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Span Mode

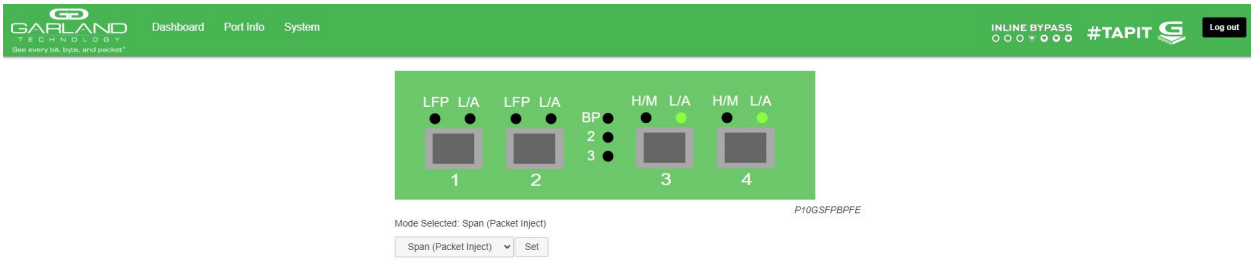


LED Indications

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

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Span (Packet Inject) Mode

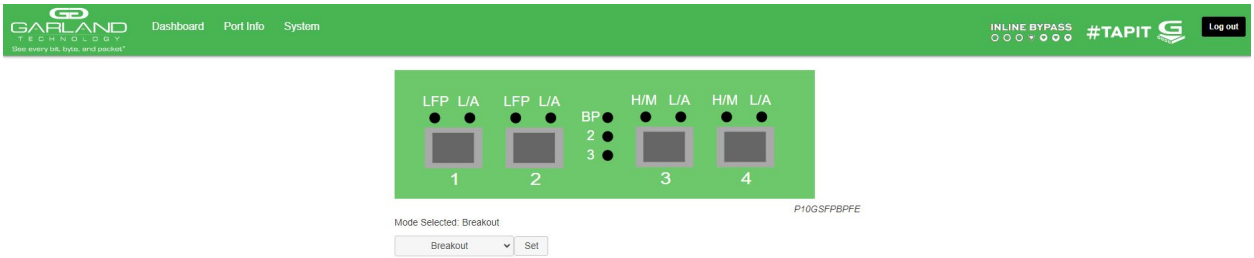


LED Indications

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

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Breakout Mode

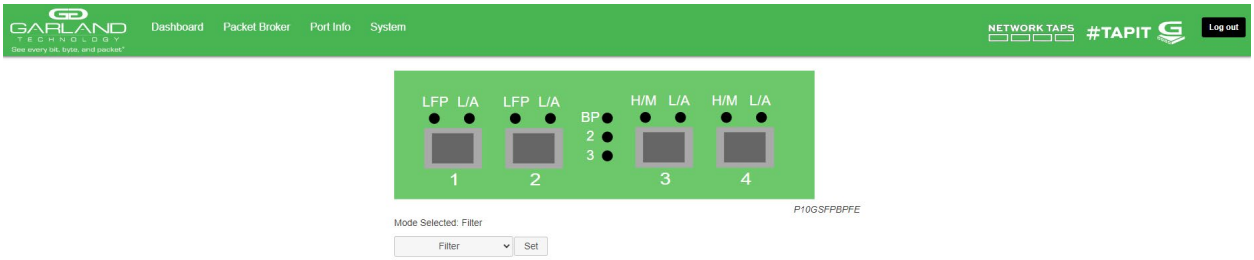


LED Indications

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

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Filter Mode

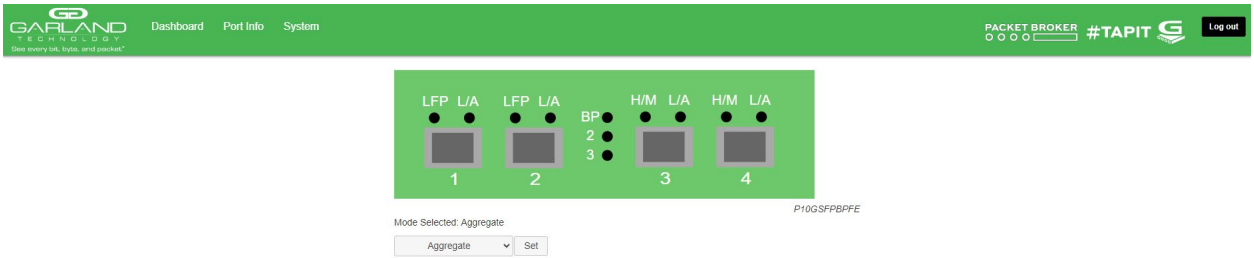


LED Indications

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

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Aggregate Mode

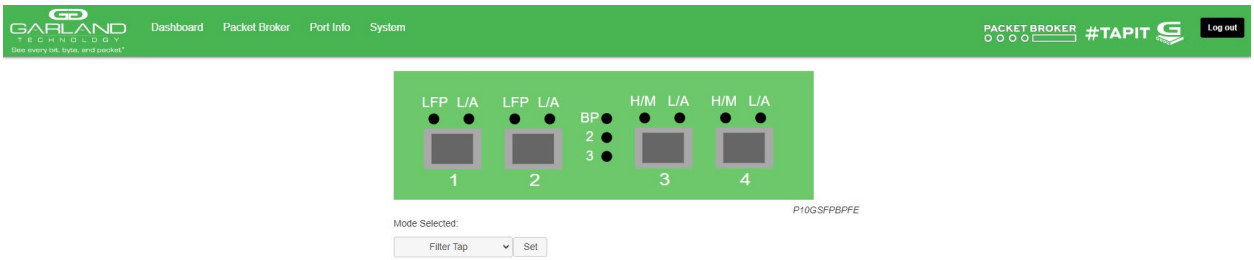


LED Indications

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	Aggregate Port Link/Activity LED
Port 3 H/M	N/A
Port 4 L/A	Aggregate Port Link/Activity LED
Port 4 H/M	N/A

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Filter Tap Mode

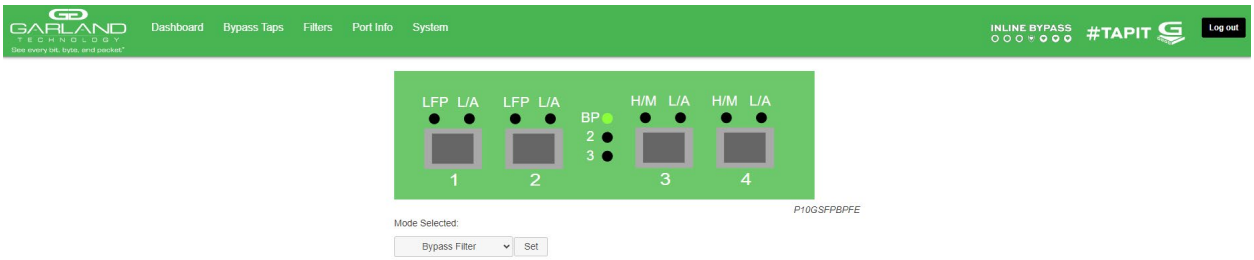


LED Indications

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

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

Bypass Filter Mode



LED Indications

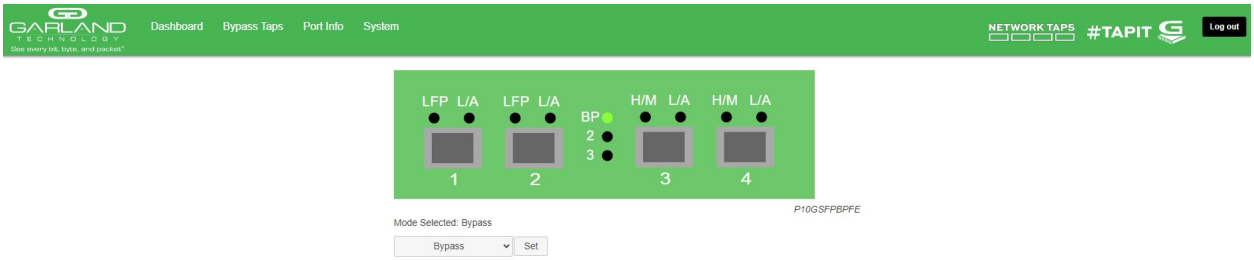
Port 1 L/A1	Network Port Link/Activity LED
Port 2 L/A2	Network Port Link/Activity LED
BP	Bypass LED
Port 3 L/A	Inline Appliance Link/Activity LED
Port 3 H/M	N/A
Port 4 L/A	Inline Appliance Link/Activity LED
Port 4 H/M	N/A

** The L/A1, L/A2, Port 3 L/A and Port 4 L/A LEDs only indicate link in the GUI.*

2. System

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

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



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.

System Info

The System Information panel displays the following.

Chassis Name	Chassis Model	Chassis Serial Number
MAC Address	Software Version	

1. Select System Info.

   The System Information panel will be displayed.

General

The following configuration options may be displayed or modified.

Chassis Name
Key Press Timeout

1. Select General.

   The General System Settings panel will be displayed.

2. Select Edit Configuration.

3. Enter the desired Chassis Name.

4. Enter the desired Key Press Timeout.

5. Select Save to save updates.

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

Admin

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

Users
Groups
Authentication
    Local
    TACACS Primary
    TACACS Secondary

1. Select Admin.

   The Admin Settings panel will be displayed.

Users

The default user is “admin”. Changes to the default user “admin” are allowed and may be deleted. Users displayed on the Admin Settings panel are for local authentication only, not used for TACACS.

1. Select Users + to create a new user.

   The Create New User panel will be displayed.

2. Enter the Username.

A username may be from 5 to 25 characters, a-z, A-Z, 0-9. A username may not contain spaces or special characters.

3. Enter the Password.

A password may be from 5 to 25 characters, a-z, A-Z, 0-9 and special characters ~ ! @ # % ^ _ [ ] { } ? , . = + - *. A *password may not contain spaces.*

4. Select the group for the user.
5. Select Save to save updates.

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

6. Select Cancel to return to the Admin Settings panel.
7. Edit the username, password or assigned group by selecting the pencil.
8. Delete the user by selecting the red X.

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”. There are three defaults groups, admin, OPER and NOC. All three groups may be modified, however only the OPER and NOC groups may be deleted.

1. Select Groups + to create a new group.

The Create New Group panel will be displayed.

2. Enter the Group Name.
3. Select the desired privileges.
4. Select Save to save updates.

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

5. Select Cancel to return to the Admin Settings panel.
6. Modify the group privileges by selecting the pencil.
7. Deleted the group by selecting the Red X.

If a group has at least one user assigned it cannot be deleted.

Authentication

Two authentication options are supported, local or TACACS. TACACS authentication supports two options, primary and secondary. The TACACS primary and secondary options may be enabled or disabled independently. Local or TACACS authentication may be enabled or disabled independently, however, at least one option must be enabled. The TACACS primary or secondary function supports IPv4 only, IPv6 is not supported.

1. Select Authentication Settings.

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

Local Authentication Disable

1. Deselect Local Authentication.

   Local authentication may only be disabled provided that TACACS authentication, primary or secondary has previously been enabled.

2. Select Save.

Local Authentication Enable

1. Select Local Authentication.

2. Select Save.

TACACS Primary Authentication

1. Select Enable Primary.

   The TACACS Primary panel will be displayed.

2. Enter the IP Address, IPv4 or IPv6.

3. Enter the Secret Word, (optional).

4. Select Save to save updates.

5. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

   The TACACS Test panel will appear.

2. Select Primary.

3. Enter the Username.

4. Enter the Password.

5. Select Test.

   The GUI will display the results of the test, "Authentication Test Successful". As well as messages for "authentication:Success", authorization:Success" and "authorization:group:abcdef.

TACACS Ping Test

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 previously enabled.

1. Select TACACS 1 Ping.

The GUI will display the results of the ping, "TACACS 1 Ping Successful".

TACACS Secondary Authentication

1. Select Enable Secondary.

   The TACACS Secondary panel will be displayed.

2. Enter the IP Address, IPv4 or IPv6.
3. Enter the Secret Word, (optional).
4. Select Save to save updates.
5. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

   The TACACS Test panel will appear.

2. Select Secondary.
3. Enter the Username.
4. Enter the Password.
5. Select Test.

   The GUI will display the results of the test, "Authentication Test Successful". As well as messages for "authentication:Success", authorization:Success" and "authorization:group:abcdef.

TACACS Ping Test

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 previously enabled.

1. Select TACACS 2 Ping.

   The GUI will display the results of the ping, "TACACS 2 Ping Successful".

Network Settings

Upon the initial turn up via the serial interface the IPv4 address, IPv4 gateway, IPv6 address and IPv6 gateway may have been already established. The IPv4 and IPv6 management interfaces may be enabled or disabled independently as well as both enabled or disabled simultaneously. If the IPv4 and IPv6 management interfaces are disabled simultaneously, access is only allowed via the serial interface. Any modifications made to any setting option will cause GUI disruption for about 60 seconds. Also note that modifying the management interfaces may cause network disruption if prior consideration and planning have not been performed.

The default system network configurations are as follows:

IPv4 enabled
IPv4 address 10.10.10.200
IPv4 gateway 10.10.10.1
IPv6 is disabled.

Via the GUI, the following options may be displayed, modified, enabled, or disabled.

IPv4 Enable/Disable	IPv4 Address	IPv4 Gateway
IPv6 Enable/Disable	IPv6 Address	IPv6 Gateway
SSL Certificate Loaded		
Using Uploaded SSL Certificate		

1. Select Network Settings.

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

IPv4 / Disable

1. Deselect Enable IPv4.
2. Select Save.

If the IPv6 management interface has not been enabled the GUI will display a message "Disabling IPv4 and IPv6, GUI will disconnect. Are you sure?

3. Select OK.

IPv4 Enable

1. Select Enable IPv4.
2. Enter the desired Address.
3. Enter the desired Gateway.
4. Select Save.

IPv6 Enable

1. Select Enable IPv6.
2. Enter the desired Address.
3. Enter the desired Gateway.
4. Select Save.

IPv6 Disable

1. Deselect Enable IPv6.
2. Select Save.

If the IPv4 management interface has not been enabled the GUI will display a message "Disabling IPv4 and IPv6, GUI will disconnect. Are you sure?

3. Select OK.

Add SSL Certificate

Uploading a custom SSL certificate involves two files. The cert.pem file and key.pem file. The unit will validate these files during the upload. If the files do not match or one of the files are corrupted the unit will abort the upload.

1. Select Add SSL Certificate.

    The Select Certificate and Select Key File panel will appear.

2. Select Choose File for Select Certificate.
3. Select the desired cert.pem file.
4. Select Open.
5. Select the Choose File for Select Key File.
6. Select the desired key.pem file.
7. Select Open.
8. Select Upload.

    The GUI message will be displayed, "Please wait. Browser will refresh after 90 seconds".

9. Verify SSL Certificate Loaded "true".
10. Verify Using Uploaded SSL Certificate "true".

Disable Using Uploaded SSL Certificate

1. Select Edit Settings.
2. Deselect Using Uploaded SSL Certificate.
3. Select Save.

    The GUI message will be displayed,"Saved Settings. Changes will cause network connectivity disruption for about 60 seconds".

4. Refresh Browser.
5. Verify SSL Certificate Loaded "true".
6. Verify Using Uploaded SSL Certificate "false".

Date & Time

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

Timezone
UTC
NTP No Authentication (Symmetric)
NTP Authentication (Symmetric)

Time
Date

1. Select Date & Time.

The Date & Time Settings panel will be displayed.

Timezone

1. Select Edit Settings.
2. Select the desired Timezone using the pull-down panel.
3. Select Save.
4. Select Cancel to return to the Date & Time Settings panel.

UTC

1. Select Edit Settings.
2. Select the desired UTC using the pull-down panel.
3. Select Save.
4. Select Cancel to return to the Date & Time Settings panel.

Manually Set Date & Time

1. Select Edit Settings.
2. Enter the Hours or use the up/down arrows to select.
3. Enter the Minutes or use the up/down arrows to select.
4. Enter the Date, MM/DD/YYYY or use the calendar to select.
5. Select Save.
6. Select Cancel to return to the Date & Time Settings panel.

NTP No Authentication (Symmetric)

The system supports an IPv4 or IPv6 address for NTP timing. If IPv4 is desired, then an IPv4 management interface must be assigned. If IPv6 is desired, then an IPv6 management interface must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

1. Select Edit Settings.
2. Select NTP timing.
3. Enter the IPv4 or IPv6 Address.
4. Verify Authenticate, None.
5. Select Save.

The NTP Status will display “syncing”. Eventually the NTP Status will display “Synced”. This can take several minutes.

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

NTP Authentication (Symmetric)

The system supports an IPv4 or IPv6 address for NTP timing. If IPv4 is desired, then an IPv4 management interface must be assigned. If IPv6 is desired, then an IPv6 management interface must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

1. Select Edit Settings.
2. Select NTP timing.
3. Enter the IPv4 or IPv6 Address.
4. Select Authenticate, Symmetric.
5. Select Encryption Type, (MD5, SHA1, SHA224, SHA256, SHA384, SHA512)
6. Enter the Key Number.
7. Enter the Key.
8. Select Save.

    The NTP Status will display "syncing". Eventually the NTP Status will display "Synced". This can take several minutes.

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

Syslog

The system supports an IPv4 or IPv6 address for Syslog. If IPv4 is desired, then an IPv4 management interface must be assigned. If IPv6 is desired, then an IPv6 management interface must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

1. Select Syslog.

    The Syslog Configuration panel will be displayed.

2. Select Edit Settings.
3. Select Enable Syslog Config.
4. Enable Unit ID, (optional).
5. Enter the Unit ID, (optional).
6. Enter the IPv4 or IPv6 Address.
7. Enter the desired UDP Port Number or use the default, 514.
8. Select Save.
9. Select Cancel to return the Syslog Configuration panel.

Syslog Test

1. Select Syslog Test.

    The GUI message will be displayed,"Syslog Test Successful!".

2. Verify the Syslog Test Message on the Syslog server.

SNMP

The system supports an IPv4 or IPv6 address for SNMP. If IPv4 is desired, then an IPv4 management interface must be assigned. If IPv6 is desired, then an IPv6 management interface must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

The following SNMP configuration options are supported:

V2 Read/Write	
V2 Read Only	
V3 Auth Type	MD5 / SHA
V3 Priv Protocol	DES / AES

1. Select SNMP.

    The SNMP Configuration panel will be displayed.

2. Select Edit Configuration.
3. Select Enable SNMP Config.
4. Enter the desired Access Port number or use the default, 161.
5. Enter the desired Trap Port number or use the default, 162.
6. Enter the IPv4 or IPv6 Address.
7. Select the desired Protocol, (V2 Read/Write or V2 read Only).
8. Enter the desired V2 Community Password.
9. Select the desired Protocol, (V3).
10. Enter the desired V3 User.
11. Enter the desired V3 Auth Password.
12. Enter the desired V3 Priv password.
13. Select Save.
14. Select Cancel to return the SNMP Configuration panel.

SNMP Test

1. Select SNMP Test.

    The GUI message will be displayed,"Test Successful!".

2. Verify the SNMP Test Message on the MIB Browser.

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.

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.

Software Upgrade

This option allows the unit’s firmware to be upgraded. An Upgrade Guide is created as part of the standard documentation for each release. Please refer to the Upgrade Guide for the procedure.

Reboot

This option allows the unit to be rebooted. The traffic will be affected for up to 1 minute.

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.

The GUI will display a “rebooting” as well as a “Session timed out. Go to Login screen” message.

4. Select Go.

The Login panel will be displayed.

3. Bypass Mode

In this mode, the network ports 1 and 2 and inline appliance ports 3 and 4 are defined by the system. The network ports are typically connected to network devices such as a server or router. The inline appliance ports are typically connected to an inline appliance or tool to monitor the network traffic. Heartbeat packets are transmitted bidirectionally from the inline appliance ports on the tap through the inline appliance or tool to monitor the health of the device.

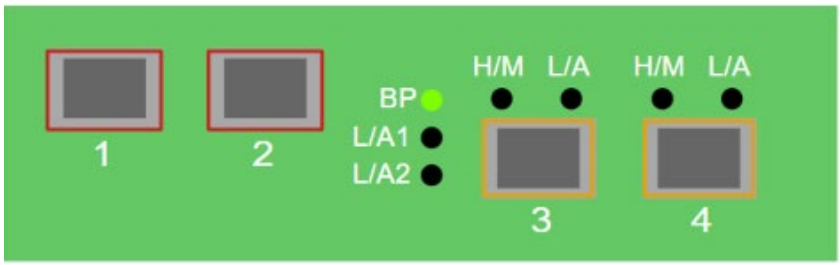
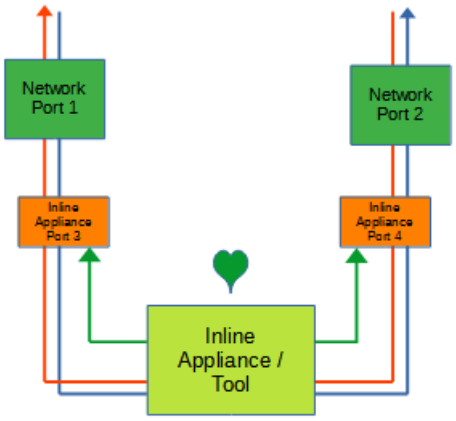
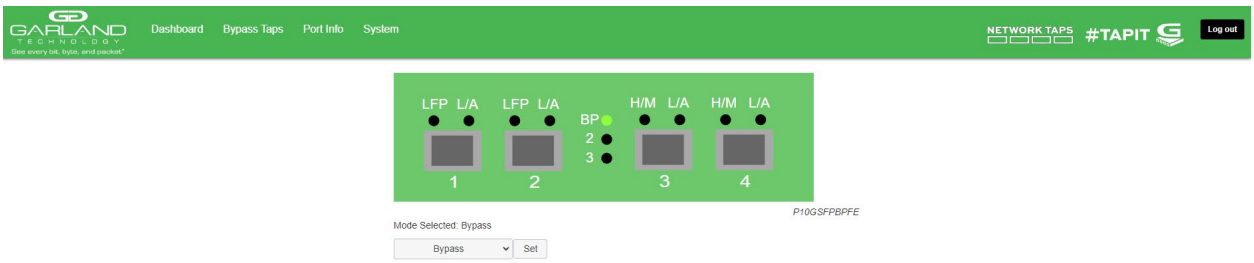


Figure 1 Bypass Mode



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

Bypass Taps Panel	Tap Settings
Bypass Tap Name	Heartbeat Settings



1. Select Bypass Taps on the Dashboard Menu bar.

The Bypass Taps panel will be displayed.

Bypass Tap Name

1. Select the Pencil icon for the desired tap.

   The Tap Name panel will be displayed.

2. Enter the name.

3. Remove the name by placing the cursor in the name panel, backspace or delete the current name.

4. Select the Check to save updates.

5. Select Cancel to return the Bypass Taps panel.

Heartbeat Settings

The following configuration options may be displayed or modified.

No. Of Lost HB Packets
Heartbeats per Second

1. Select Settings on the Bypass Taps panel.

   The Configure Heartbeat Settings panel will be displayed with the current configuration.

2. Enter the No. Of Lost HB Packets. Default is 10.

   This is the number of heartbeats that must be lost on the inline appliance ports before any tap will switch to bypass.

3. Enter the Heartbeats per Second. Default is 10.

   This is the number of heartbeats per second applied to the inline appliance ports for all taps.

4. Select Save to save updates.

5. Select Cancel to return the Bypass Taps panel.

Taps Settings

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

Tap Modes
Fail Mode
LFP
Reverse Bypass

1. Edit the Tap Settings, by placing the cursor on the tap and double-press the left mouse button.

   The Tap panel will be displayed.

2. Select Edit Tap Settings.

   The Configure Inline Appliance panel will be displayed.

3. Select the Tap Mode.

Active — Allows the tap to automatically switch from inline to bypass if an issue occurs with the inline appliance port(s), loss of link or heartbeats. When the issue with the inline appliance port(s) is resolved, link and heartbeats restored, the tap will automatically switch back to inline.

Figure 2 Bypass Mode (Inline)

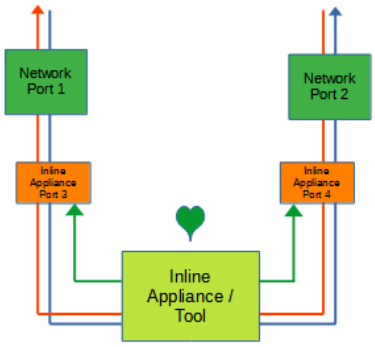
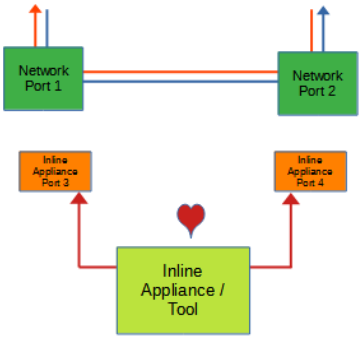
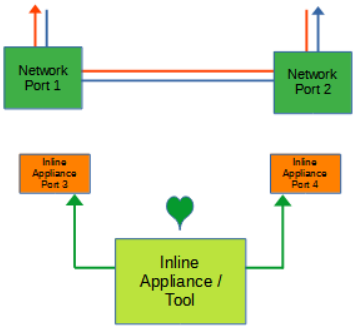


Figure 3 Bypass Mode (Bypass)



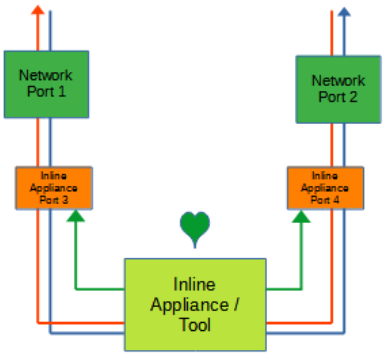
Force Bypass — If selected, the tap will switch the traffic between the network ports with no regard for the inline appliance port(s), links, or heartbeats. Typically used during maintenance activities.

Figure 4 Bypass Mode (Force Bypass)



Force Inline — If selected, the tap bypass option is disabled. If an issue occurs with the inline appliance port(s), loss of link or heartbeats, the traffic will go down.

Figure 5 Bypass Mode (Force Inline)

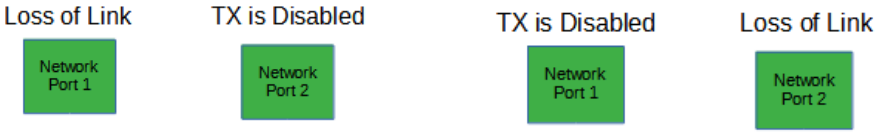


4. Select the Fail Mode.

Closed — If power is lost to the unit. The traffic will drop between the network ports.

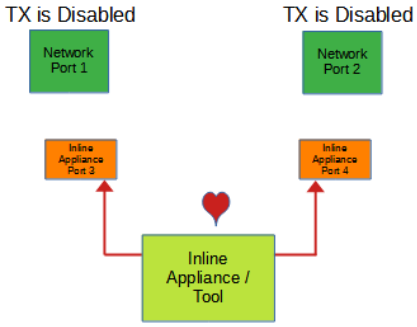
5. LFP — If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 6 Bypass Mode (LFP)



6. Reverse Bypass — If enabled and the inline appliance port(s) fail, loss of link or heartbeats. The TX will be disabled on both network ports. The RX for both network ports remain on.

Figure 7 Bypass Mode (Reverse Bypass)



7. Select Accept to save updates. Save must additionally be selected on the Bypass Taps panel.

8. Select Cancel to return the Bypass Taps panel.

4. Span Mode

In this mode, the network port 1 and span ports 2, 3 and 4 are defined by the system. Port 1 is an ingress only port. Ports 2, 3 and 4 are egress only ports.

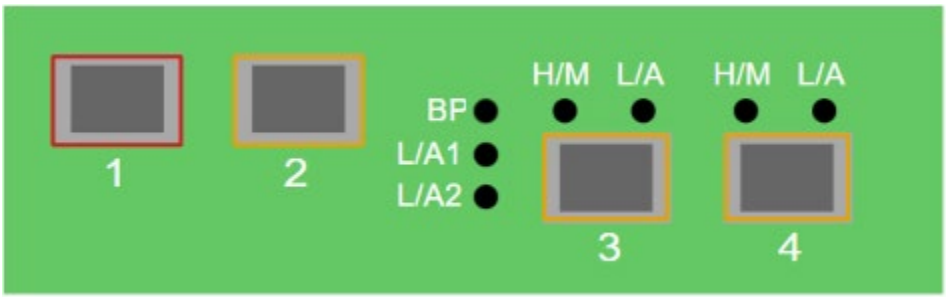
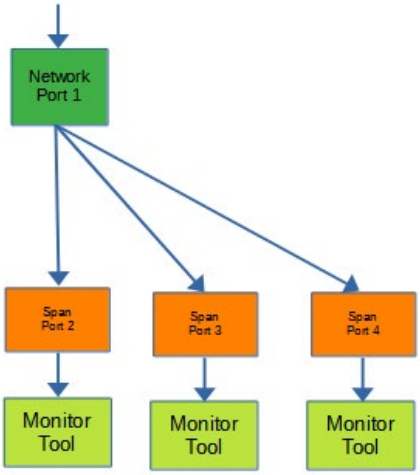


Figure 8 Span Mode



5. Span Packet Inject Mode

In this mode, the network port 1 and span packet inject ports 2, 3 and 4 are defined by the system. Port 1 is an ingress and egress port. The traffic ingressed in port 1 is egressed out ports 2, 3 and 4. The traffic ingressed in ports 2, 3 and 4 are egressed out port 1.

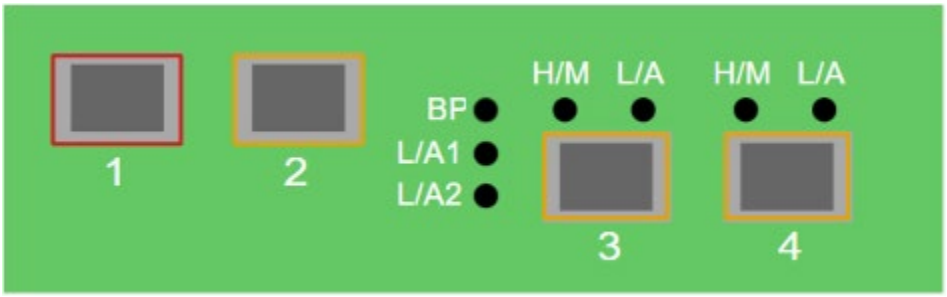
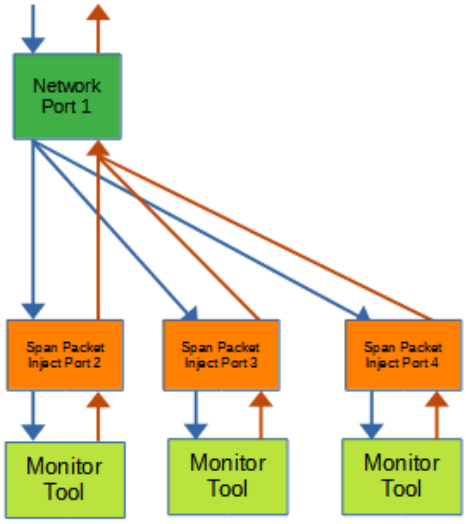


Figure 9 Span Packet Inject Mode



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. The traffic ingressed in port 1 is egressed out port 3. The traffic ingressed in port 2 is egressed out port 4.

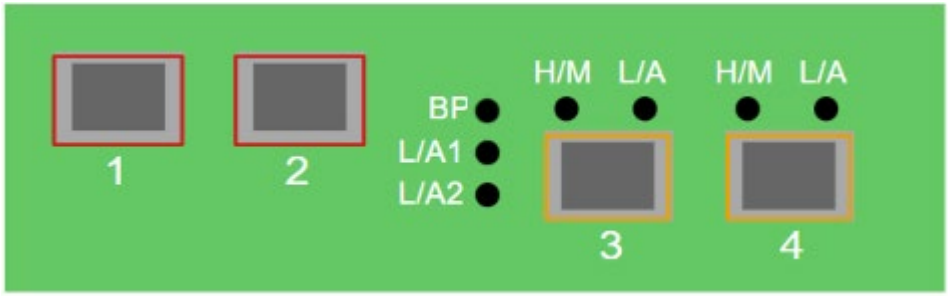


Figure 10 Breakout Mode

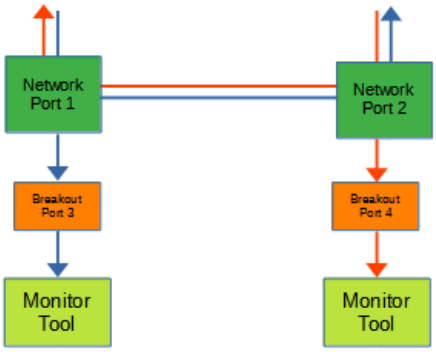
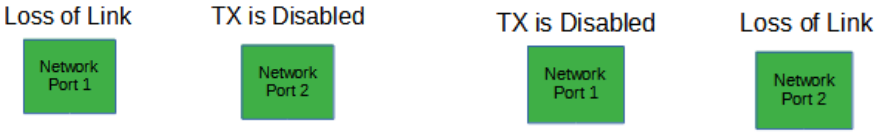


Figure 11 Breakout Mode (LFP)



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.

7. 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.

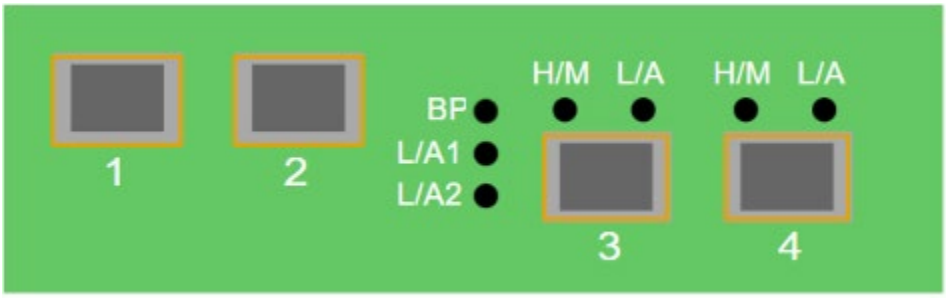
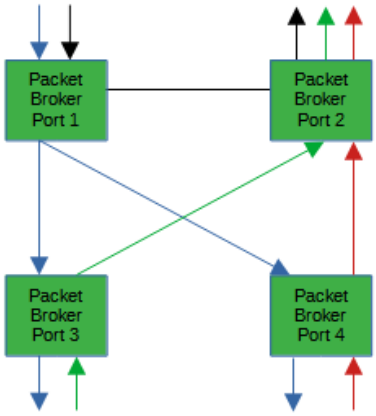


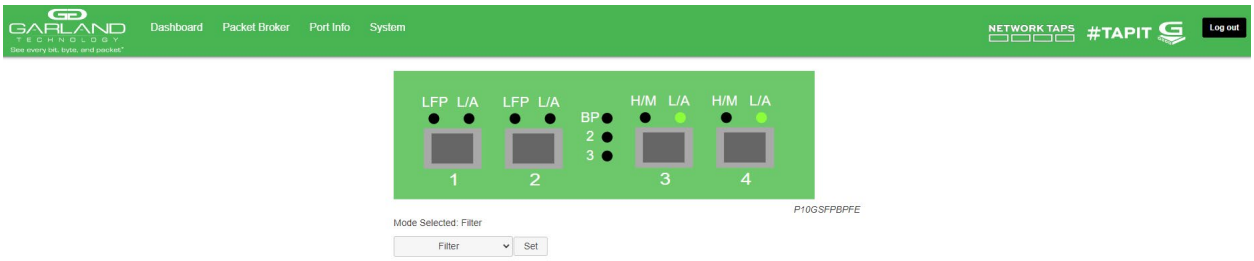
Figure 12 Filter Mode



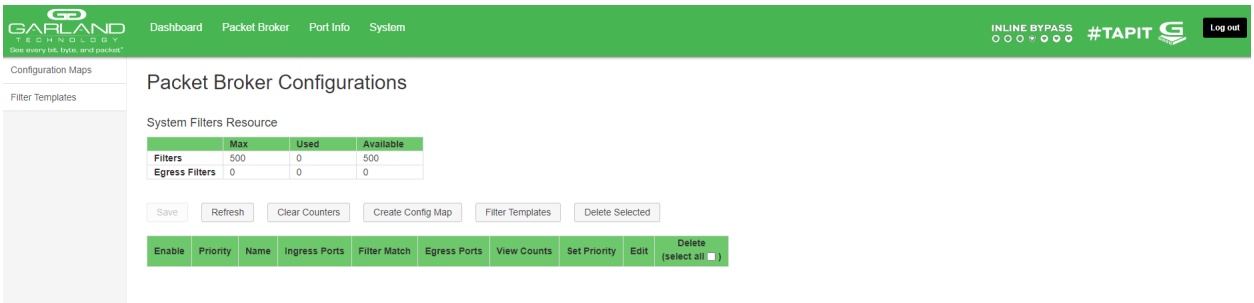
Packet Broker

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.

Filter Templates

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 IPv4 Address / Source IP Mask
   Destination IPv4 Address / Destination IP Mask
   Source IPv6 Address / Source IP Mask — *IPv6 is not supported for this model*
   Destination IPv6 Address / Destination IP Mask — *IPv6 is not supported for this model*
   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.

Config Map

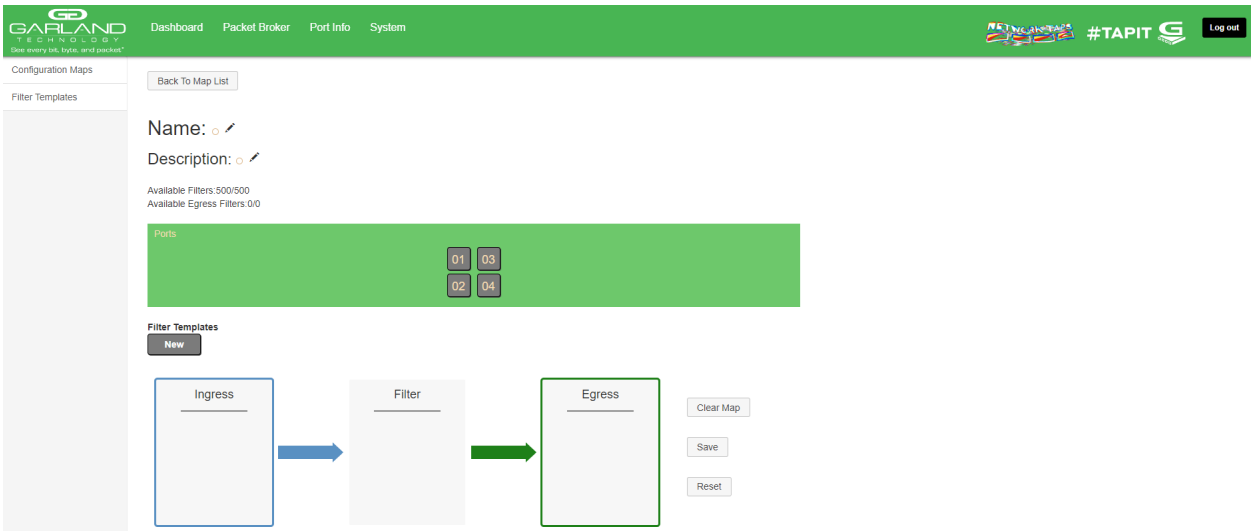
Config maps are unidirectional connections between ingress port(s) to egress port(s) and/or a load balancing group.

1. Select Configuration Maps.

   The Packet Broker Configurations panel will be displayed.

2. Select Create Config Map.

   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.



3. 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.

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

5. Select the Check to apply.

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

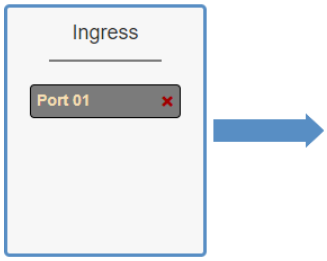
7. Place the cursor in the Description panel and enter the description, optional.

8. Select the Check to apply updates.

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 13 Ingress



2. Remove a port by selecting the red X.

Filters

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 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 14 Filter

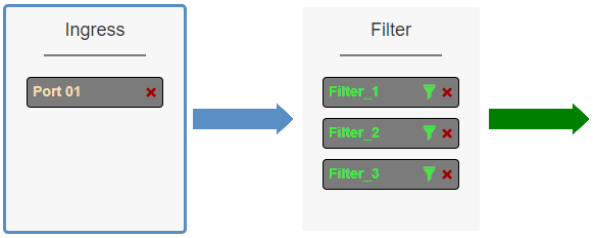
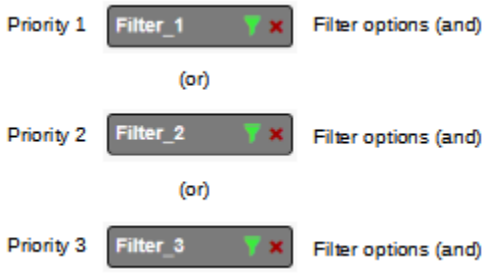


Figure 15 Filter System Considerations



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.

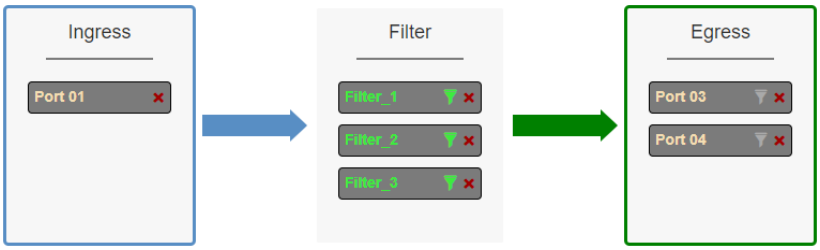
4. Select Accept once all desired options have been modified.

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

Egress

1. Add an egress port by placing the cursor on the desired port. Select 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 16 Egress Port(s)



2. Remove a port by selecting the red X.

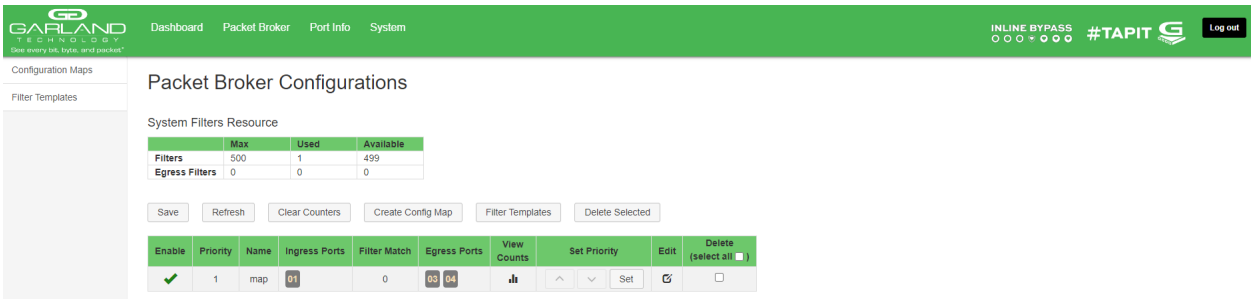
Config Map Save

1. Select Save to save the current configuration.

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

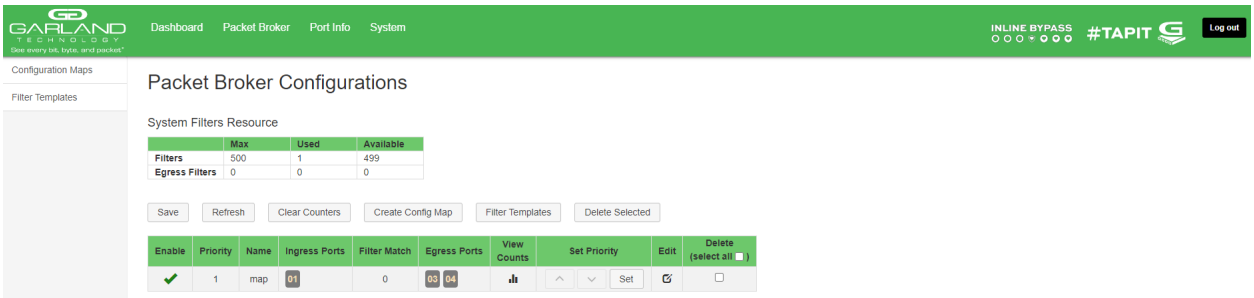
2. Select OK to save the Config Map.

3. Select Cancel to disregard.



Modify a Config Map

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



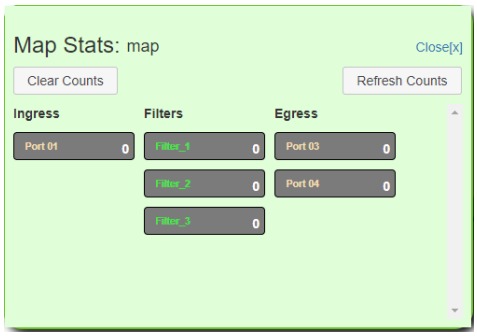
Config Map Statistics

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.



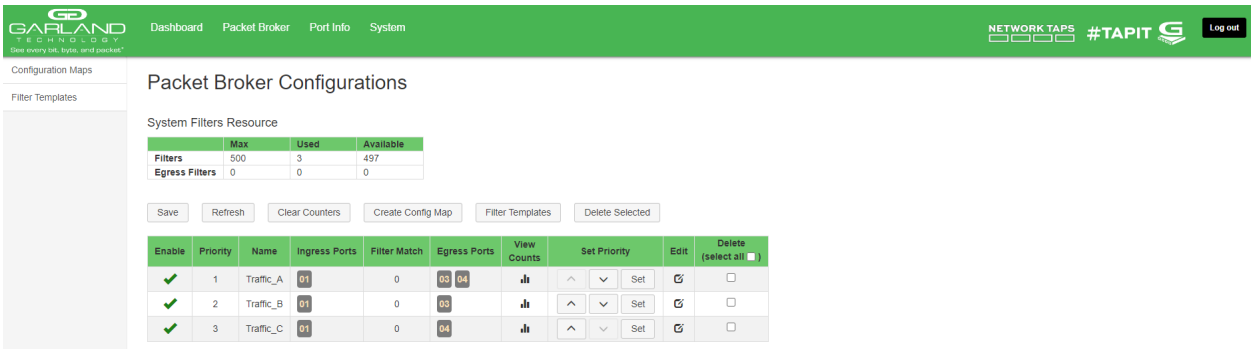
4. Select Refresh Counts to refresh the statistics.

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

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

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.

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

Figure 17 Config Map System Considerations

Method 1

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

2. Select Save to save updates.

Method 2

1. Select Set.

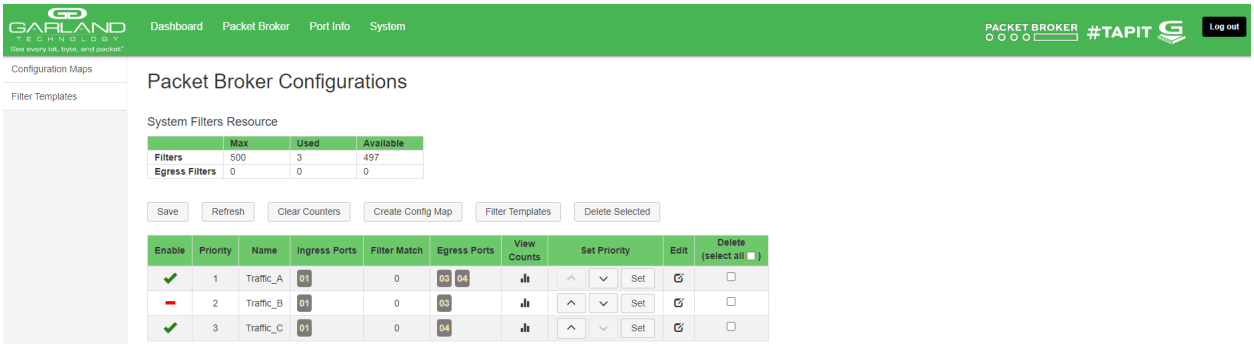
    The Set Priority panel will be displayed.

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.



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.

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.

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.

    The red dash will change to a green check.

3. Select Save.

8. 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. The traffic ingressed port 1 is egressed out ports 3 and 4. The traffic ingressed in port 2 is egressed out ports 3 and 4.

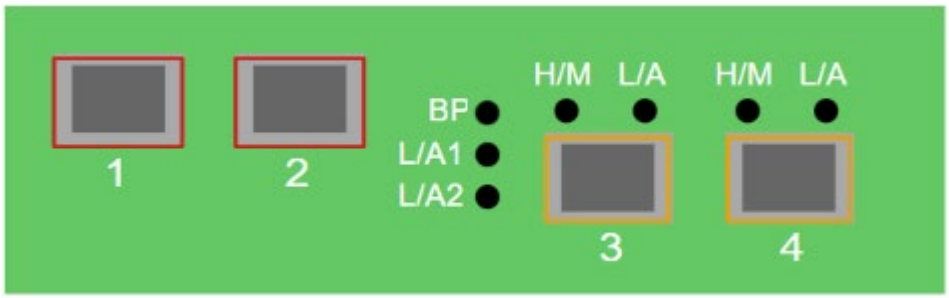


Figure 18 Aggregate Mode

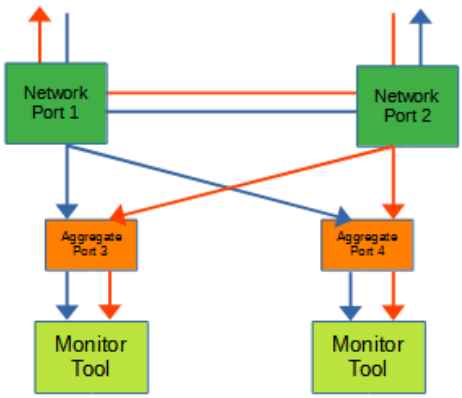
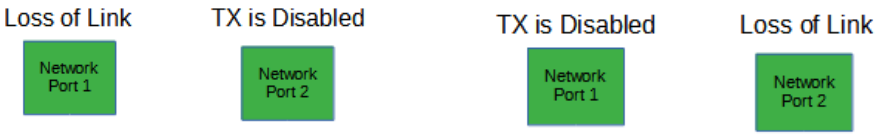


Figure 19 Aggregate Mode (LFP)



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.

9. 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.

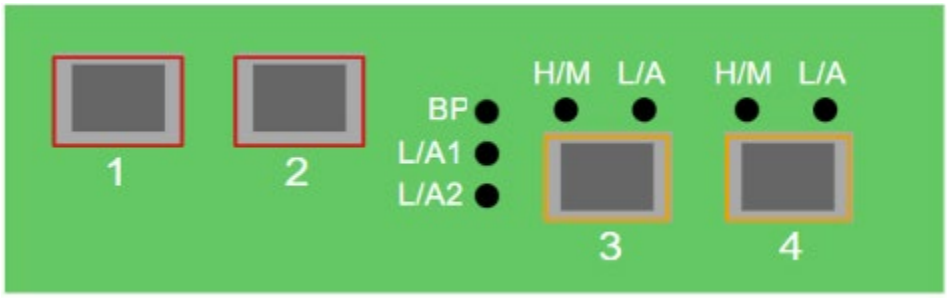


Figure 20 Filter Tap Mode

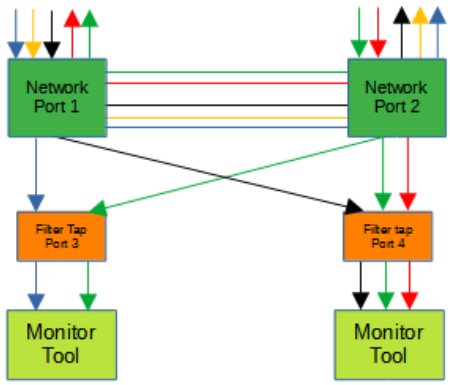
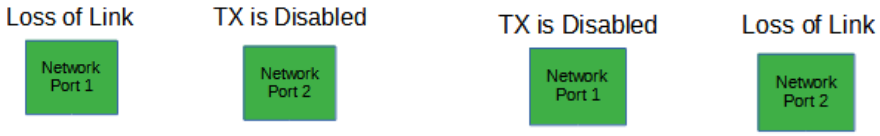


Figure 21 Filter Tap Mode (LFP)

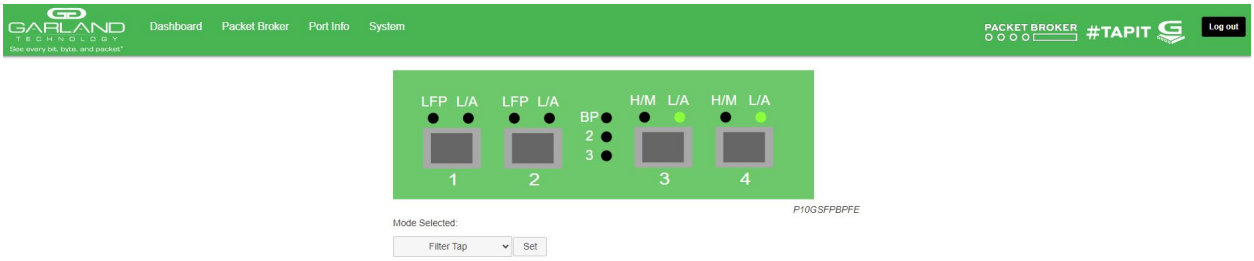


If a link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

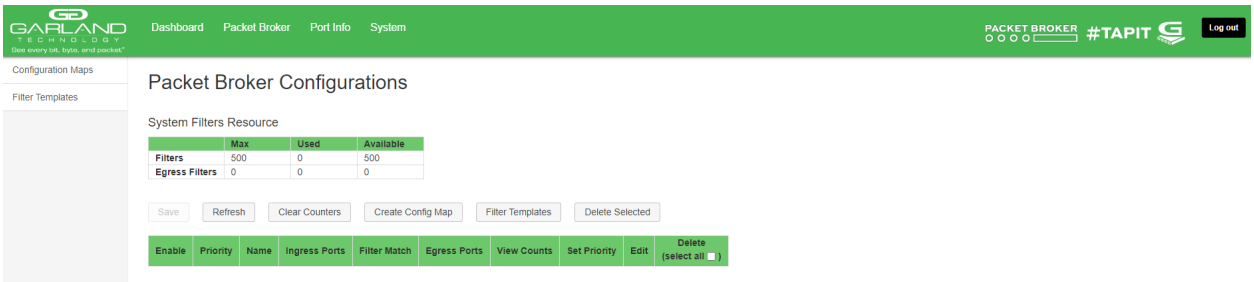
Packet Broker

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.

Filter Templates

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 IPv4 Address / Source IP Mask
   Destination IPv4 Address / Destination IP Mask
   Source IPv6 Address / Source IP Mask *IPv6 is not supported for this model*
   Destination IPv6 Address / Destination IP Mask *IPv6 is not supported for this model*
   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.

Config Maps

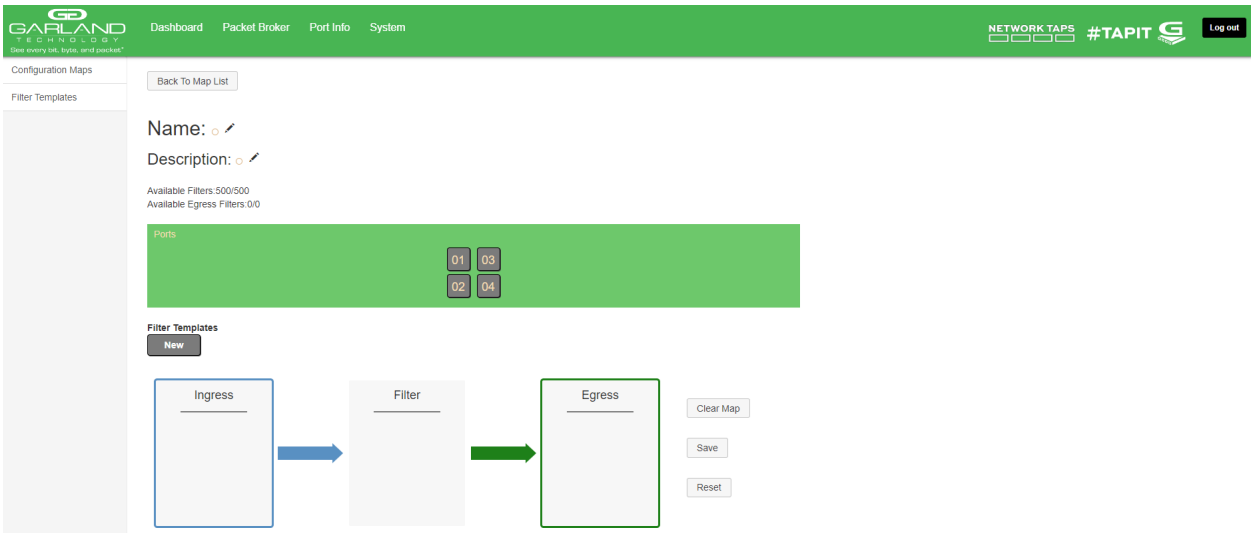
Config maps are unidirectional connections between ingress port(s) to egress port(s) and/or a load balancing group.

1. Select Configuration Maps.

   The Packet Broker Configurations panel will be displayed.

2. Select Create Config Map.

   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.

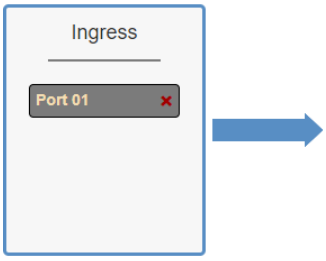


3. Select the Name pencil icon to apply a name, optional. If no name is entered the system will automatically apply a name to the config maps as follows, map, map(1), map(2) etc.
4. Place the cursor in the Name panel and enter the name.
5. Select the Check to apply.
6. Select the Description pencil to apply a description, optional.
7. Place the cursor in the Description panel and enter the description, optional.
8. Select the Check to apply updates.

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 22 Ingress



2. Remove a port by selecting the red X.

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 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 23 Filter

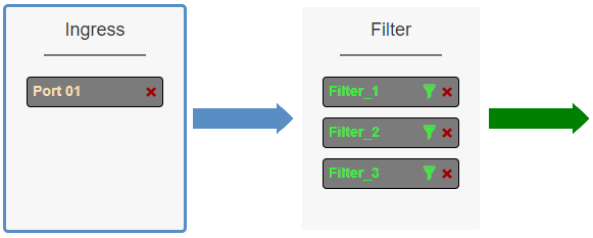
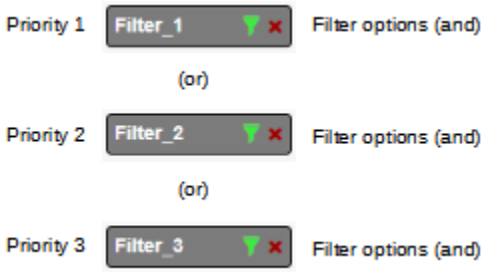


Figure 24 Filter System Considerations



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.

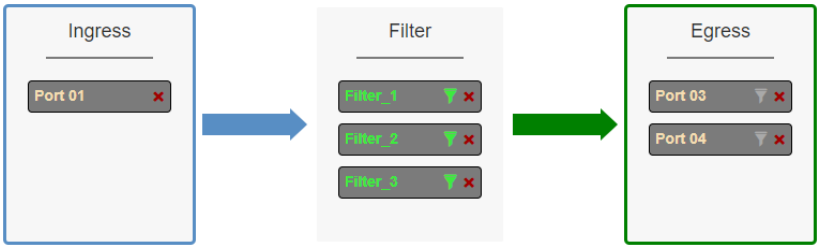
4. Select Accept once all desired options have been modified.

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

Egress

1. Add an egress port(s) 3 and/or 4 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 ports 3 and 4 are added, then 100% of the traffic will be sent to each port.

Figure 25 Egress Port(s)



2. Remove a port by selecting the red X.

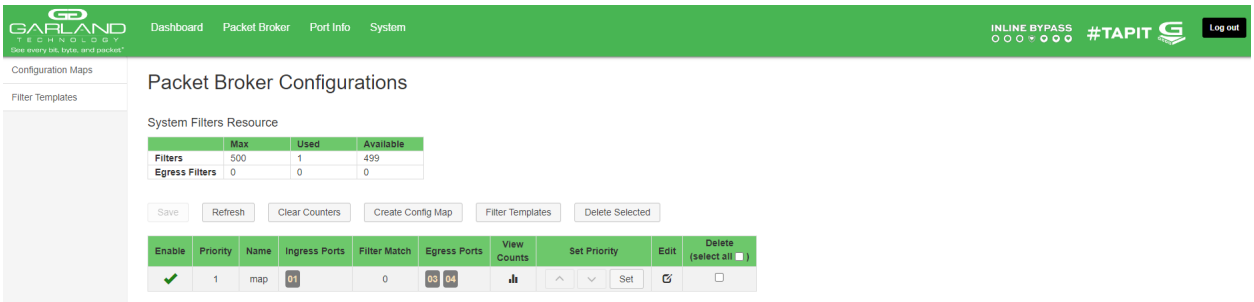
Config Map Save

1. Select Save to save the current configuration.

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

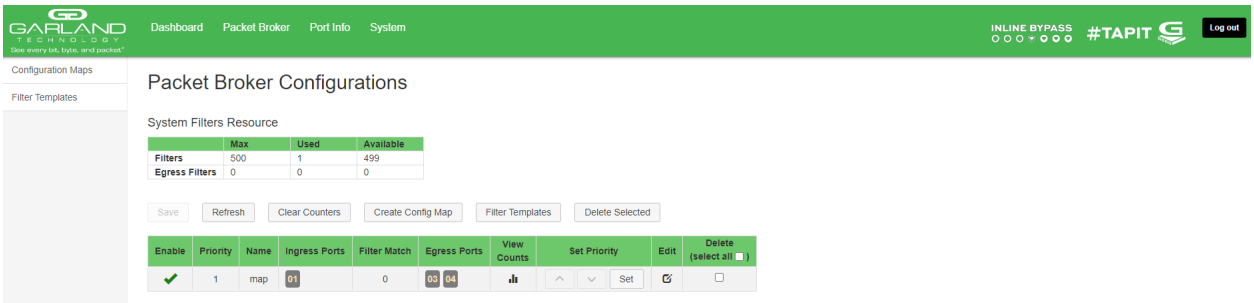
2. Select OK to save the Config Map.

3. Select Cancel to disregard.



Modify a Config Map

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



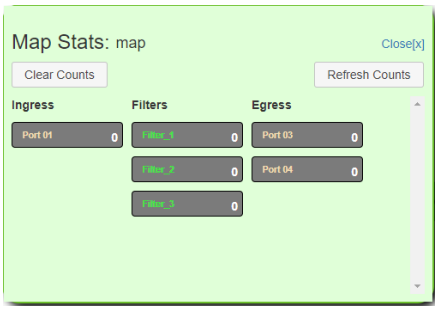
Config Map Statistics

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.

6. Select Close to return to the Packet Broker Configurations panel.

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.

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

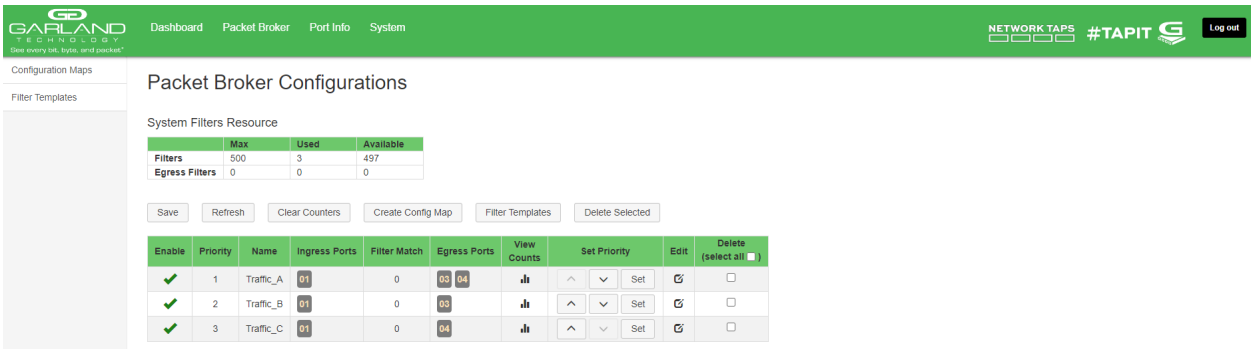


Figure 26 Config Map System Considerations

Method 1

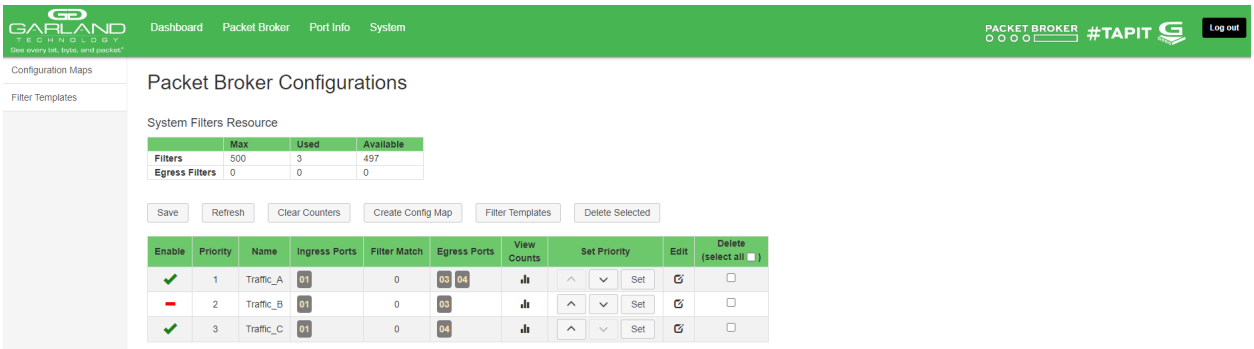
1. Select the up or down arrow for the config map.
2. Select Save to save updates.

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.



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.

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.

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.

    The red dash will change to a green check.

3. Select Save.

10. Bypass Filter Mode

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

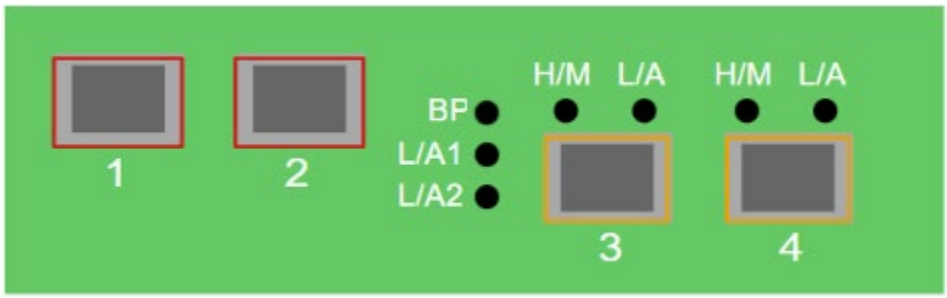
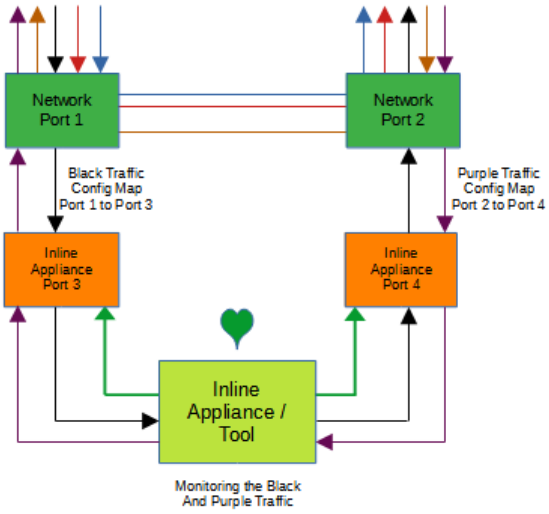


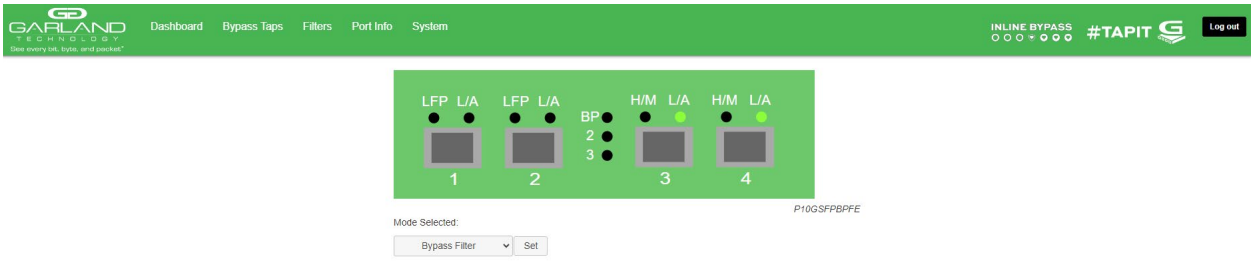
Figure 27 Bypass Filter Mode



Bypass Taps

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

Bypass Taps Panel	Tap Settings
Bypass Tap Name	Heartbeat Settings



1. Select Bypass Taps on the Dashboard Menu bar.

The Bypass Taps panel will be displayed.

Bypass Tap Name

1. Select the Pencil icon for the desired tap.

    The Tap Name panel will be displayed.

2. Enter the name.

3. Remove the name by placing the cursor in the name panel, backspace or delete the current name.

4. Select the Check to save updates.

5. Select Cancel to return the Bypass Taps panel.

Heartbeat Settings

The following configuration options may be displayed or modified.

No. Of Lost HB Packets
Heartbeats per Second

1. Select Settings on the Bypass Taps panel.

    The Configure Heartbeat Settings panel will be displayed with the current configuration.

2. Enter the No. Of Lost HB Packets. Default is 10.

    This is the number of heartbeats that must be lost on the inline appliance ports before any tap will switch to bypass.

3. Enter the Heartbeats per Second. Default is 10.

    This is the number of heartbeats per second applied to the inline appliance ports for all taps.

4. Select Save to save updates.

5. Select Cancel to return the Bypass Taps panel.

Taps Settings

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

Tap Modes
Fail Mode
LFP
Reverse Bypass

1. Edit the Tap Settings, by placing the cursor on the tap and double-press the left mouse button.

    The Tap panel will be displayed.

2. Select Edit Tap Settings.

    The Configure Inline Appliance panel will be displayed.

3. Select the Tap Mode.

Active — Allows the tap to automatically switch from inline to bypass if an issue occurs with the inline appliance port(s), loss of link or heartbeats. When the issue with the inline appliance port(s) is resolved, link and heartbeats restored, the tap will automatically switch back to inline.

Figure 28 Bypass Filter Mode (Inline)

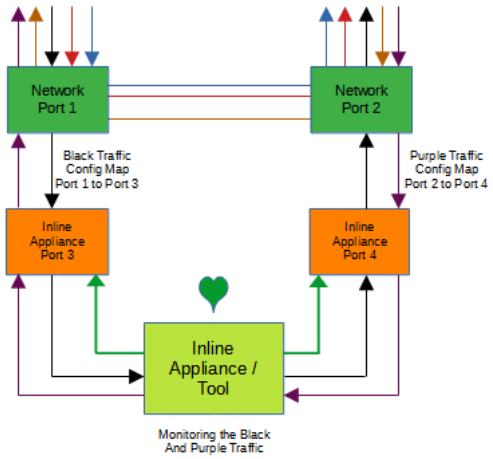
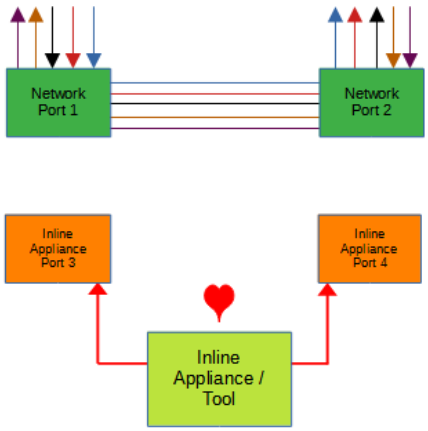
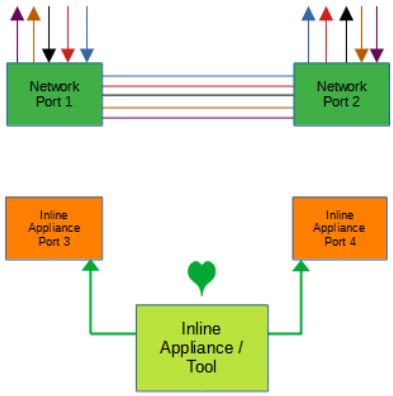


Figure 29 Bypass Filter Mode (Bypass)



Force Bypass — If selected, the tap will switch the traffic between the network ports with no regard for the inline appliance port(s), links, or heartbeats. Typically used during maintenance activities.

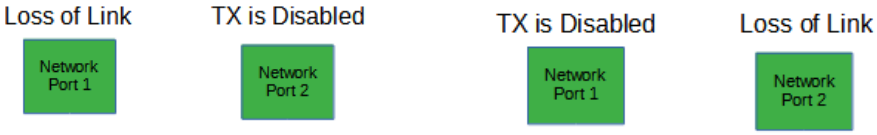
Figure 30 Bypass Filter Mode (Force Bypass)



4. Select the Fail Mode.

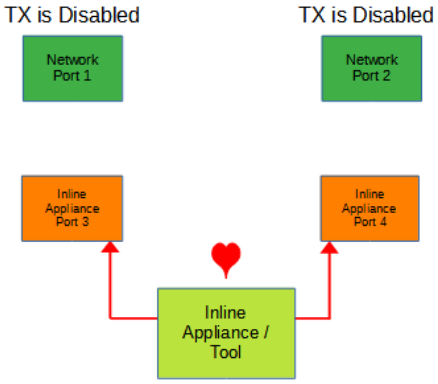
Closed	If power is lost to the unit. The traffic will drop between the network ports.
5. LFP	If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 31 Bypass Filter Mode (LFP)



6. Reverse Bypass	If enabled and the inline appliance port(s) fail, loss of link or heartbeats. The TX will be disabled on both network ports. The RX for both network ports remain on.

Figure 32 Bypass Filter Mode (Reverse Bypass)



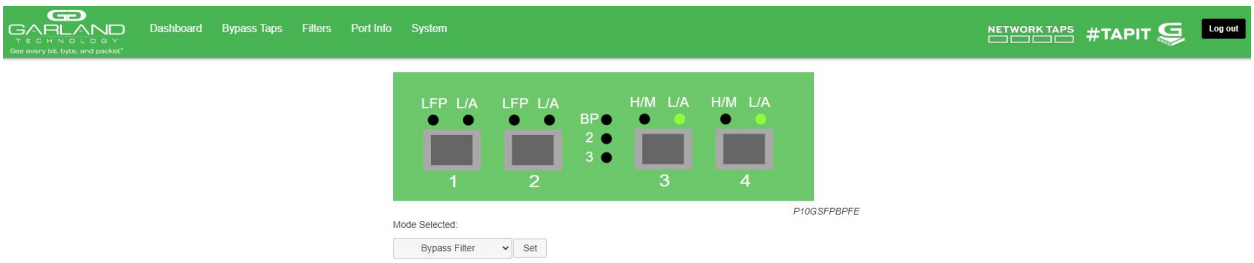
7. Select Accept to save updates. Save must additionally be selected on the Bypass Taps panel.

8. Select Cancel to return the Bypass Taps panel.

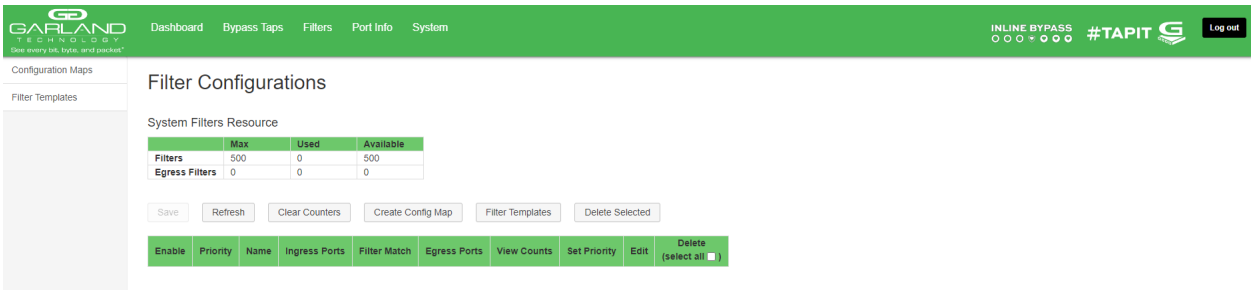
Filters

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

Filter Templates
Config Maps
Statistics



1. Select Filters on the Dashboard Menu bar.



The Filter Configurations panel will be displayed.

Filter Templates

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 IPv4 Address / Source IP Mask
   Destination IPv4 Address / Destination IP Mask
   Source IPv6 Address / Source IP Mask — *IPv6 is not supported for this model*
   Destination IPv6 Address / Destination IP Mask — *IPv6 is not supported for this model*
   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.

Config Map

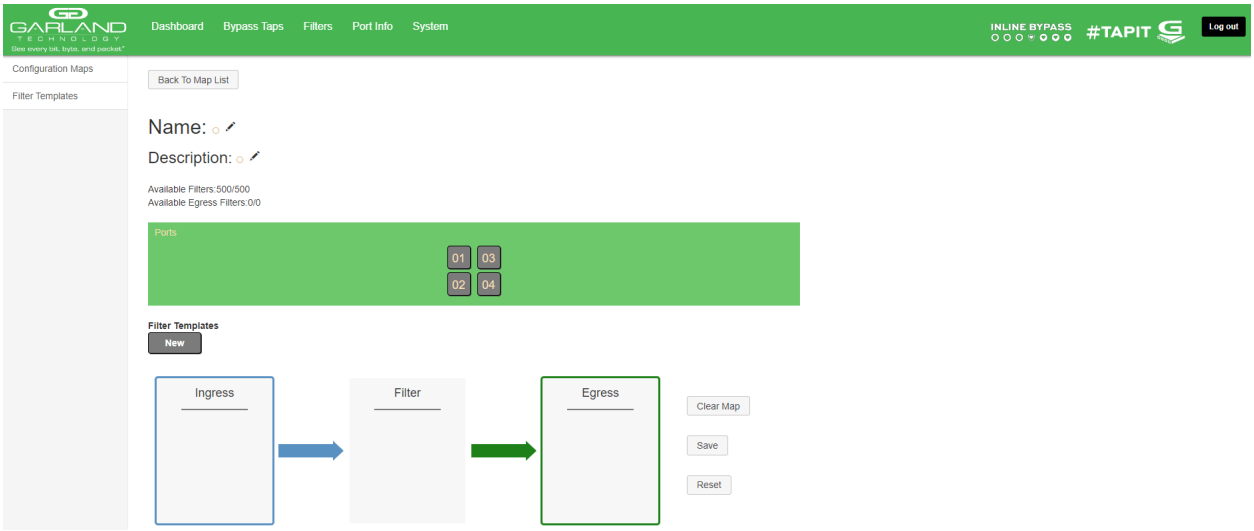
Config maps are unidirectional connections between ingress port(s) to egress port(s) and/or a load balancing group.

1. Select Configuration Maps.

   The Packet Broker Configurations panel will be displayed.

2. Select Create Config Map.

   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.

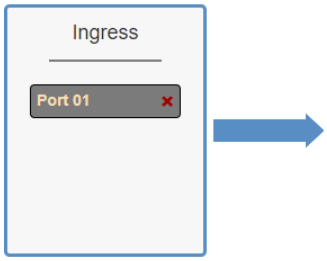


3. Select the Name pencil icon to apply a name, optional. If no name is entered the system will automatically apply a name to the config maps as follows, map, map(1), map(2) etc.
4. Place the cursor in the Name panel and enter the name.
5. Select the Check to apply.
6. Select the Description pencil to apply a description, optional.
7. Place the cursor in the Description panel and enter the description, optional.
8. Select the Check to apply updates.

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 33 Ingress



2. Remove a port by selecting the red X.

Filters

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 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 34 Filter

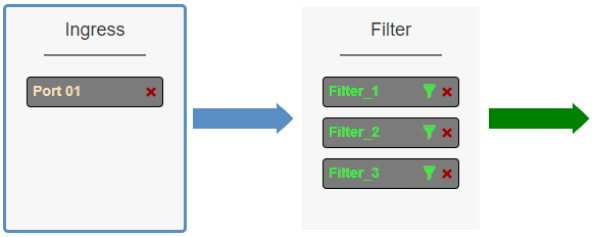
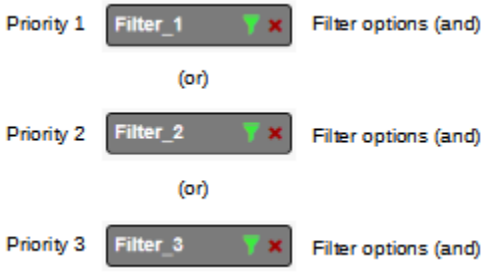


Figure 35 Filter System Considerations



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.

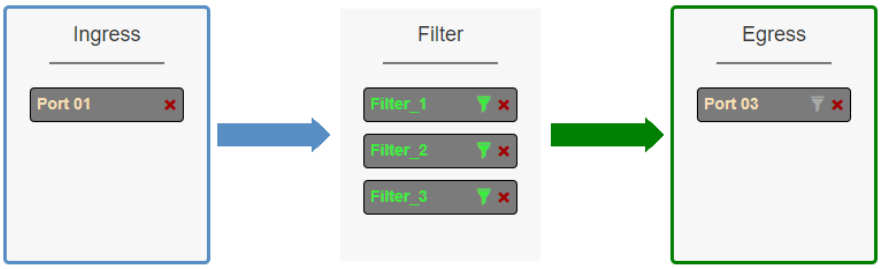
4. Select Accept once all desired options have been modified.

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

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.

Figure 36 Egress Port



2. Remove a port by selecting the red X.

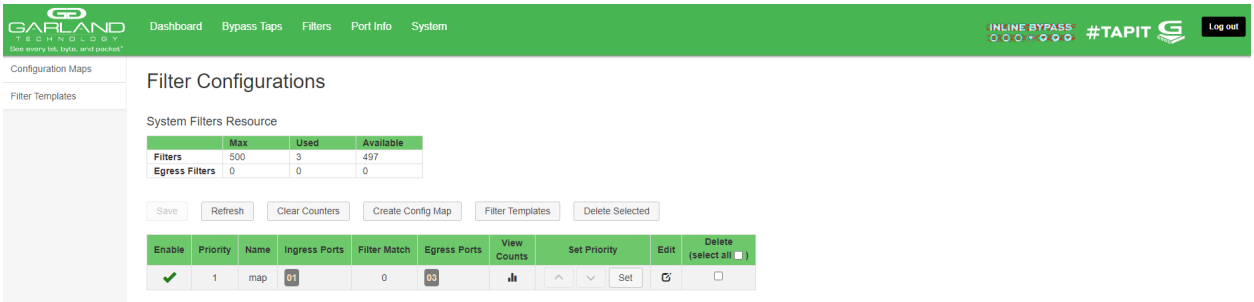
Config Map Save

1. Select Save to save the current configuration.

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

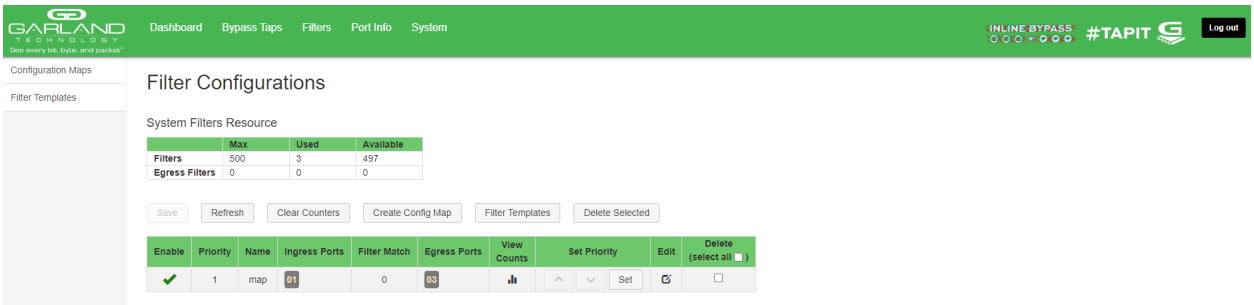
2. Select OK to save the Config Map.

3. Select Cancel to disregard.



Modify a Config Map

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



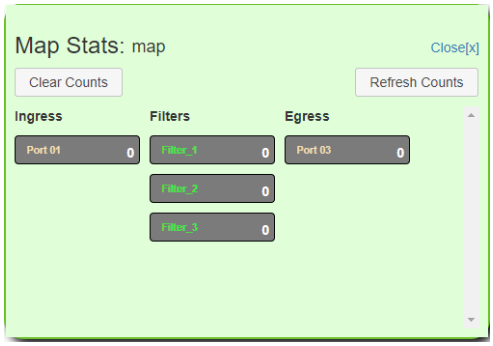
Config Map Statistics

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.



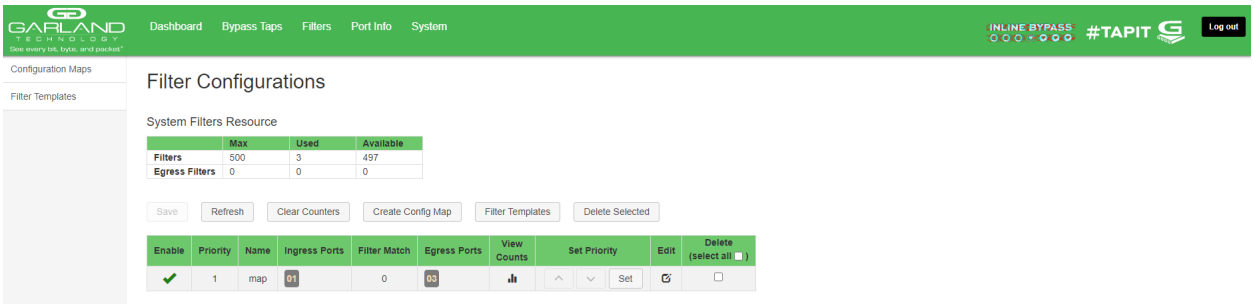
4. Select Refresh Counts to refresh the statistics.

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

6. Select Close to return to the Packet Broker Configurations panel.

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.

Config Map Priority

Usually 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. However, for the bypass filter mode the config maps can only be created from port 1 to port 3 or port 2 to port 4. Multiple egress ports is not allowed. 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. The Priority of a config map may be changed to a higher or lower value using two methods.

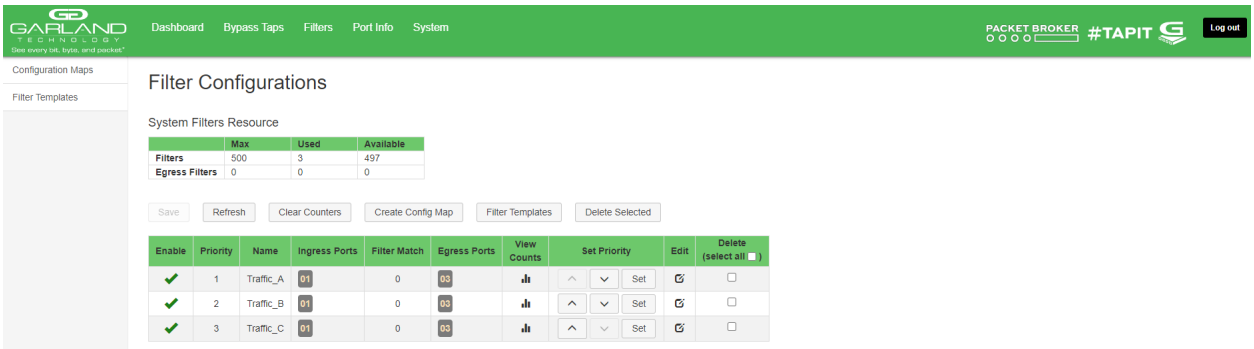


Figure 37 Config Map System Considerations

Method 1

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

2. Select Save to save updates.

Method 2

1. Select Set.

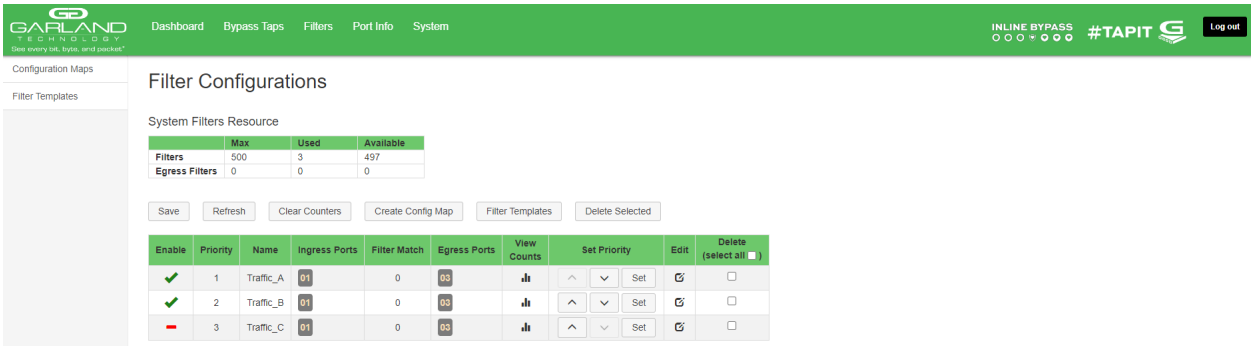
The Set Priority panel will be displayed.

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.



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.

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.

Enable Config Map

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

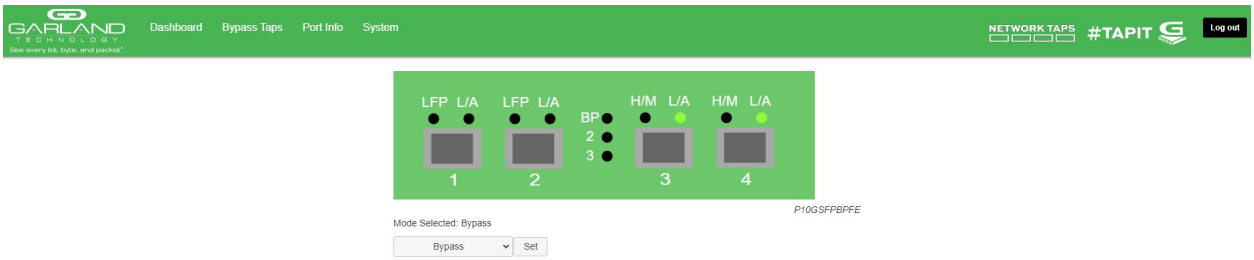
   The red dash will change to a green check.

2. Select Save.

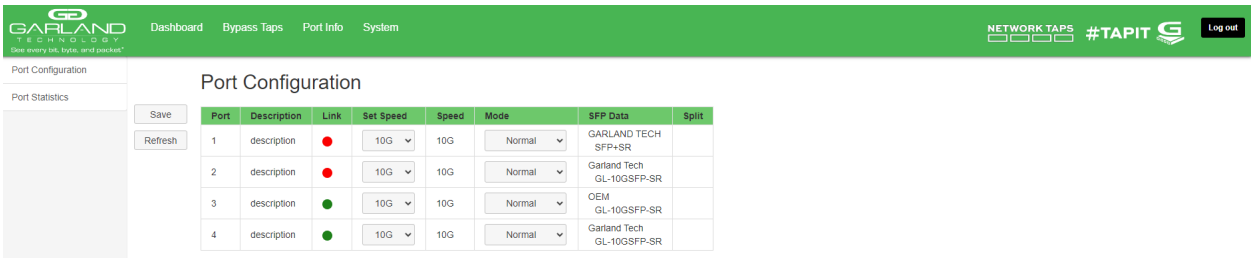
11. Port Info

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

Port Number	Speed
Port Description	Mode
Link	SFP Data
Set Speed	



1. Select Port Info on the Dashboard menu bar.



The Port Configuration panel will be displayed.

Port Configuration

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

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.

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.

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.

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.