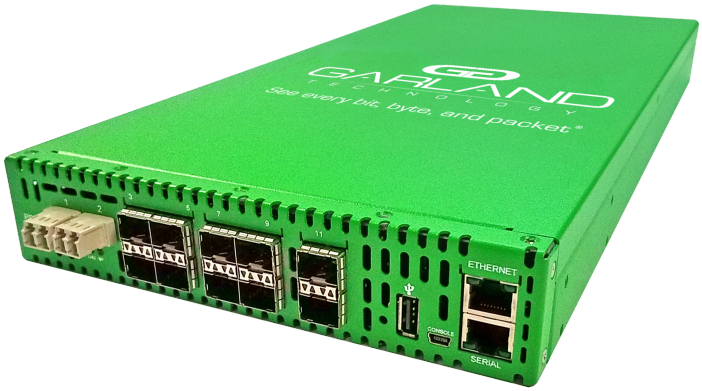
EdgeLens® Focus

Inline Security Packet Broker

User Guide By Garland Technology

INT10G12MSBP / INT10G12SSBP / INT10G12ESBP



Garland Technology: Integrated Bypass System
Firmware Rev Level: 1.15.1

Office: 716-242-8500
garlandtechnology.com/support
garlandtechnology.com

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.

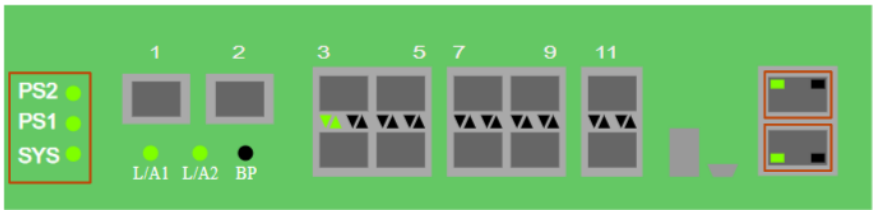
Table of contents

1. INT10G12xxBP Dashboard

The Dashboard of the INT10G12xxBP is divided into 3 sections.

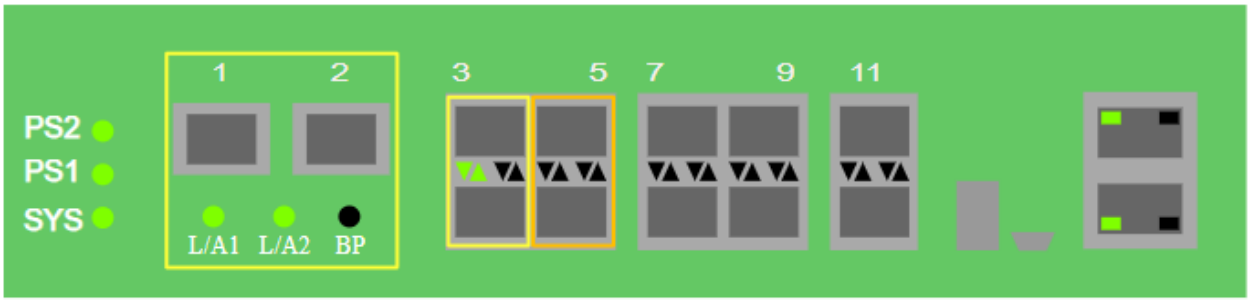
1. System 2. Bypass Taps 3. Packet Broker

1. System
The System Section of the Dashboard consists of the following.



PS2	Power Supply 2 LED Green indicates normal Off indicates power not applied
PS1	Power Supply 1 LED Green indicates normal Off indicates power not applied
SYS	System LED Green indicates normal
Ethernet Interface	Upper Right LED GUI always indicates Green
Serial Interface	Lower Right LED GUI always indicates Green

2. Bypass Taps
The Bypass Taps Section of the Dashboard consists of the following.



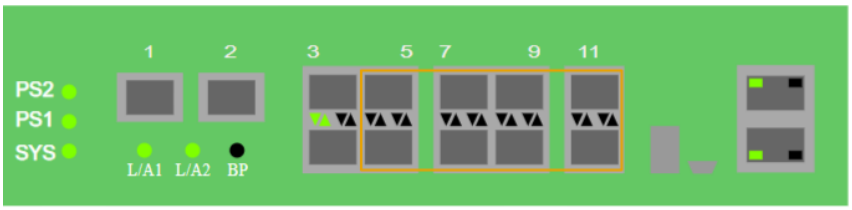
Tap 1

Port 1 - L/A1	Link/Activity LED Network Port Activity LED N/A GUI
Port 2 - L/A2	Link/Activity LED Network Port Activity LED N/A GUI
BP	Green indicates Tap in Bypass Off indicates Tap Inline
Port 3 - Up Arrows	Link/Activity LED Primary Inline Appliance Port Activity LED N/A GUI
Port 4 - Down Arrows	Link/Activity LED Primary Inline Appliance Port Activity LED N/A GUI
Port 5 - Up Arrows	Link/Activity LED Secondary Inline Appliance Port Activity LED N/A GUI (optional)
Port 6 - Down Arrows	Link/Activity LED Secondary Inline Appliance Port Activity LED N/A GUI (optional)

3. Packet Broker

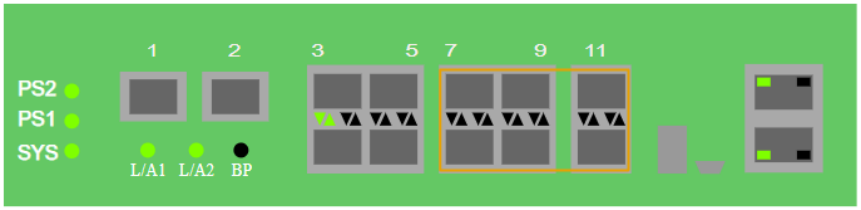
The Packet Broker Section of the Dashboard consists of the following.

Ports 5 thru 12 if the Secondary Inline Appliance is not applied to the Bypass Tap.



Port 5 thru 11 (odd) Up Arrows	Link/Activity LED Activity LED N/A GUI
Port 6 thru 12 (even) Down Arrows	Link/Activity LED Activity LED N/A GUI

Ports 7 thru 12 if the Secondary Inline Appliance is applied to the Bypass Tap.



Port 7 thru 11 (odd) Up Arrows	Link/Activity LED Activity LED N/A GUI
Port 8 thru 12 (even) Down Arrows	Link/Activity LED Activity LED N/A GUI

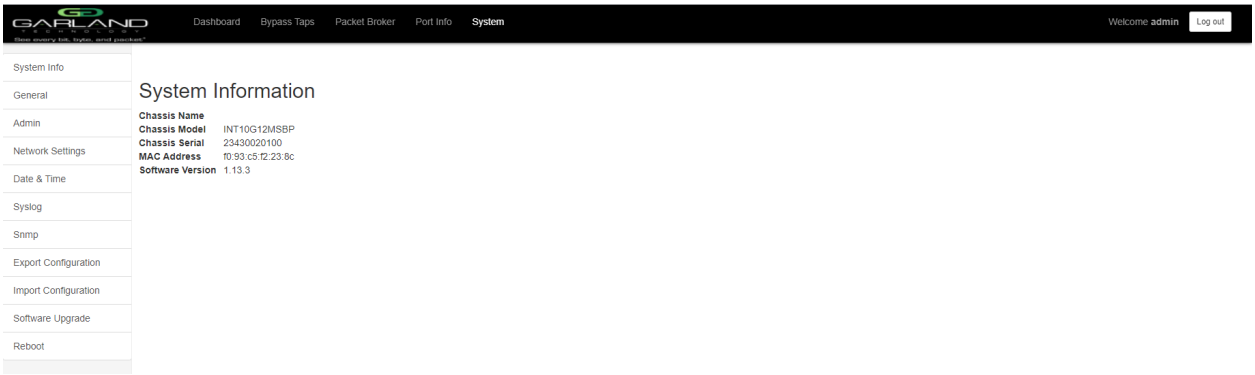
2. INT10G12xxBP System

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

1. System Info
2. General
3. Admin
4. Network Settings
5. Date & Time
6. Syslog
7. SNMP
8. Export Configuration
9. Import Configuration
10. Software Upgrade
11. Reboot

INT10G12MSBP

Access the System panel by selecting 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 System panel.

1 System Info

The System Information is displayed by default. The System Information panel displays the following.

Chassis Name
Chassis Model
Chassis Serial Number
MAC Address
Software Version

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

Chassis Name
Key Press Timeout (secs)

1. Select General on the System panel.

   The General System Settings panel will be displayed with the current configuration.

2. Select Edit Configuration.

3. Enter the desired Chassis Name.

4. Enter the desired Key Press Timeout (secs), (60-3600). The default is 60.

5. Select Save to save updates.

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

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

Groups
Users
Local Authentication
TACACS Authentication

1. Select Admin on the System panel.

   The Admin Settings panel will be displayed with 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.

3.1 Groups
The group defines the privileges for a user or group of users. A group may be used for local authorization 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.

   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.

3.2 Users

If a user is created it is for local authorization. Users defined for use with TACACS are defined on the TACACS server.

1. Select Users + to create a new local user.

   The Create New User panel will be displayed.

2. Enter the Username. (5-32 char, No spaces or special characters)

3. Enter the Password. (5-32 char, No spaces or special characters)

4. Select the group the local user will be assigned to.

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.

3.3 Local Authentication

Local authentication is only used by a local user. Local authentication may be enabled or disabled independently of TACACS authentication.

1. Select Authentication / Authentication Settings.

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

2. Disable local authentication by deselecting Local Authentication. The local authentication may not be disabled if TACACS authentication is not enabled.

3. Select Save to save updates.

4. Select Cancel to return the Admin Settings panel.

3.4 TACACS Authentication

TACACS authentication is only used by a TACACS Server. TACACS authentication may be enabled or disabled independently of Local authentication.

1. Select Authentication / Authentication Settings.

   The Authentication Settings panel will be displayed. TACACS authentication is disabled by default.

2. Select TACACS Authentication to enable.

3. Enter the TACACS Server IP Address.

4. Enter the TACACS Server Secret Word, (3-20 characters)

5. Select Save to save updates.

6. Select Cancel to return the Admin Settings panel.

3.4.1 TACACS Test

The TACACS Test option may be used to verify the authentication and authorization of a TACACS user and password. The TACACS Test option will be active only if TACACS authentication has been enabled and the TACACS server and secret word have been defined.

1. Select TACACS Test.

   The TACACS Test panel will appear.

2. Enter the username to test on the TACACS server.

3. Enter the password to test on the TACACS sever.

4. Select Test.

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

3.4.2 TACACS Ping

The TACACS Ping 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 and the TACACS server and secret word has been defined.

1. Select TACACS Ping.

   The GUI will display the results of the ping sent to the TACACS server defined on the TACACS authentication panel.

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

Network Settings	DHCP IP Address Mask Gateway DNS 1 DNS 2
Add SSL Certificate	

4.1 Network Settings
Any change made to any network setting option could cause network connectivity disruption for about 60 seconds.

1. Select Network Settings on the System panel.

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

2. Select Edit Settings.

   The Edit Network Settings panel will appear.

3. Enable DHCP. Select to enable. Default is disabled.

4. Enter the unit Management IP Address. This is usually performed at turn up. Use caution if changing as the unit may become unreachable.

5. Enter the Mask. This is usually performed at turn up. Use caution if changing as the unit may become unreachable.

6. Enter the Gateway. This is usually performed at turn up. Use caution if changing as the unit may become unreachable.

7. Enter the desired DNS 1 address.

8. Enter the desired DNS 2 address.

9. Using Uploaded SSL Certificate. Default is disabled. Enabled if a SSL certificate and key have been uploaded to the unit using the Add SSL Certificate option on the Network Settings panel. Disable to use of the unit-generated SSL certificate.

10. Select Save to save updates.

11. Select Cancel to return the Network Settings panel.

4.2 Add SSL Certificate

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

1. Select Network Settings on the System panel.

   The Network Settings panel will be displayed.

2. Select Add SSL Certificate.

   The Select Certificate and Select Key File panel will appear.

3. Select Choose File for Select Certificate.

4. Select the desired file.

5. Select Open.

6. Select the Choose File for Select Key File.

7. Select the desired file.

8. Select Open.

9. Select Upload.

10. Select Restart Import to select a different certificate or key file.

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

12. Login to the unit via the GUI.

13. Select Network Settings on the System panel.

14. Verify the SSL Certificate Loaded displays true.

15. Verify the Using Uploaded SSL Certificate displays true.

5 Date & Time

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

Timezone	Time
UTC	Date
NTP	

1. Select Date & Time on the System panel.

   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. Select the desired Timezone.

4. Select the desired UTC. The UTC option is defined based on the Timezone selected.

5. NTP Timing may be enabled as desired.

6. If NTP Timing is not desired, local timing preferred enter the Hour: Minute.

7. If NTP Timing is not desired, local timing preferred enter the Month/Day/Year

8. Use Pool may be selected for NTP Timing. If Use Pool is selected, then no IP Address is required.

9. An IP Address may be entered for the NTP Timing source if Use Pool was not selected. If Use Pool is selected and an IP Address is entered, the unit will follow the Use Pool option.

6 Syslog

1. Select Syslog on the System panel.

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

2. Select Edit Settings.

3. Enable Syslog Config.

4. If desired enable the Unit ID. The Unit ID will be sent as part of any Syslog message from the unit.

5. Enter the desired Unit ID, (0-999).

6. Select the desired Protocol. Default is UDP, (UDP-TCP).

7. Enter the IP Address of the Syslog server.

8. Enter the Syslog Port Number. Default is 514, (0-65535).

9. Select Save to save updates.

10. Select Cancel to return the Syslog Configuration panel.

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

7 SNMP

1. Select SNMP on the System panel.

    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.

7.1 SNMPv2

1. Enter the Access Port number. Default is 161.
2. Enter the Trap Port number. Default is 162.
3. Enter the Trap IP Address.
4. Select the Protocol, (V2 Read/Write, V2 Read Only).
5. Enter the V2 Community Password. Default is abc, (1-20 characters)
6. Select Save to save updates.
7. Select Cancel to return the Syslog Configuration panel.
8. SNMP Test may be selected to send a test message to the SNMP server.

7.2 SNMPv3 MD5/DES

1. Enter the Access Port number. Default is 161.
2. Enter the Trap Port number. Default is 162.
3. Enter the Trap IP Address.
4. Select the Protocol, V3.
5. Enter the V3 User.
6. Select the V3 Auth Type, MD5.
7. Enter the V3 Auth Password, (8-20 characters).
8. Enter the V3 Priv Password, (8-20 characters).
9. Select the V3 Priv Protocol, DES.
10. Select Save to save updates.
11. Select Cancel to return the Syslog Configuration panel.
12. SNMP Test may be selected to send a Test Message to the SNMP Server.

7.3 SNMPv3 SHA/AES

1. Enter the Access Port number. Default is 161.
2. Enter the Trap Port number. Default is 162.
3. Enter the Trap IP Address.
4. Select the Protocol, V3.

5. Enter the V3 User.
6. Select the V3 Auth Type, SHA.
7. Enter the V3 Auth Password, (8-20 characters).
8. Enter the V3 Priv Password, (8-20 characters).
9. Select the V3 Priv Protocol, AES.
10. Select Save to save updates.
11. Select Cancel to return the Syslog Configuration panel.
12. SNMP Test may be selected to send a test message to the SNMP server.

8 Export Configuration

1. Select Export Configuration on the System panel.

   The Export Configuration panel will be displayed.

2. Select Export.

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

9 Import Configuration

1. Select Import Configuration on the System panel.

   The Import Configuration panel will be displayed.

2. Select Choose File for the Select Config File option.
3. Browse to and select the desired Config File.
4. Select Open.
5. Select Upload.

The unit will verify if the selected file is a valid Config file.

6. Select Configure.

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

10 Software Upgrade

The existing unit configuration will not be affected during firmware upgrades. It may be required to refresh or restart the web browser after a firmware upgrade is complete.

1. Select Software Upgrade on the System panel.

   The Update Firmware panel will be displayed.

2. Select Choose File for the Select File option.

3. Browse to and select the 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.

11 Reboot

A reboot will affect traffic for about 25 seconds.

1. Select Reboot on the System panel.

   The Reboot Device panel will be displayed.

2. Select Reboot.

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

4. Select OK.

   A “rebooting” message will be displayed.

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

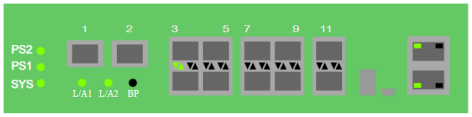
5. Select Go.

   The Login panel will be displayed.

3. INT10G12xxBP Port Info

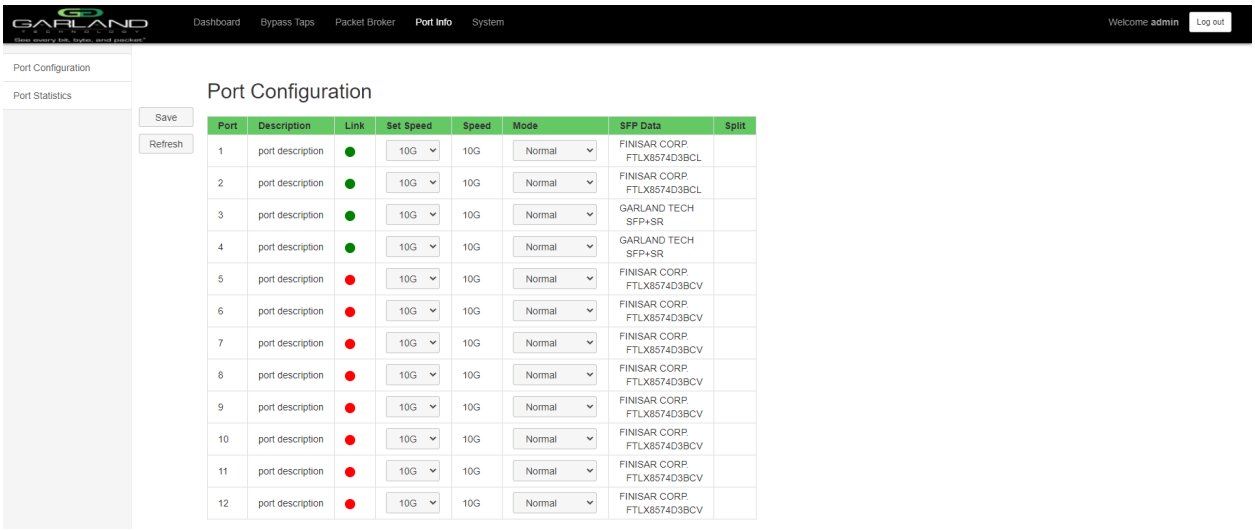
The following configuration options may be displayed, modified, cleared or refreshed under the Port Info panel.

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



INT10G12MSBP

Access the Port Configuration panel by selecting Port Info on the Dashboard menu bar.



The Port Configuration panel will be displayed.

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.

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.

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.

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.

2 Port Statistics

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

1. Port number
2. Receive Packets
3. Receive Discards
4. Receive Errors
5. Transmit Packets
6. Transmit Discards
7. Transmit Errors

1. Select Port Statistics on the Port Configuration panel.

   The Port Statistics panel will be displayed.

2. Update the statistics by selecting Refresh.

3. Clear and refresh the statistics by selecting Clear.

4. INT10G12xxBP Bypass Taps

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

1. Bypass Taps Panel
2. Bypass Tap Name
3. Heartbeat Settings
4. Tap Settings
5. Monitor Ports

Access the Bypass Taps panel by selecting Bypass Taps on the Dashboard Menu bar.

The Bypass Taps panel will be displayed.

1 Bypass Taps Panel
The Bypass Taps panel displays the following.

Tap 1 Name
Tap 1 Current Status
Tap 1 Network Ports

No. Of Lost HB Packets for all taps
Heartbeats per Second for all taps

2 Bypass Tap Name
A name may be applied to the tap.

1. Select the pencil for the tap.

2. Enter the name. (1-15 characters)

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.

3 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, (10-100).

This is the number of heartbeats that must be lost before any tap will switch to Bypass.

3. Enter the Heartbeats per Second. Default is 10, (10-100).

This is the number of heartbeats per second sent by all taps.

4. Select Save to save updates.

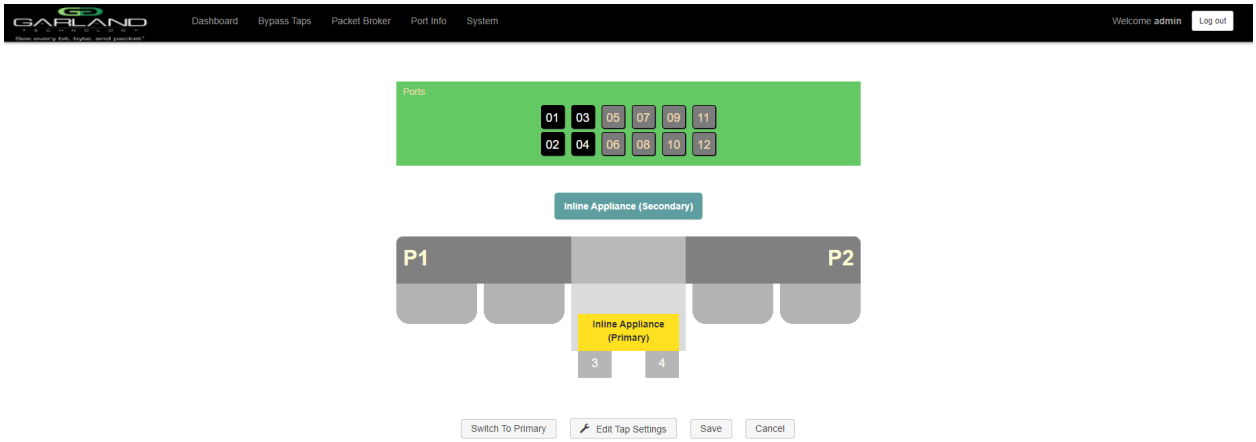
5. Select Cancel to return the Bypass Taps panel.

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

Primary/Secondary Inline Appliance	LFP
Tap Mode	Reverse Bypass
Fail Mode	Monitor Ports

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.



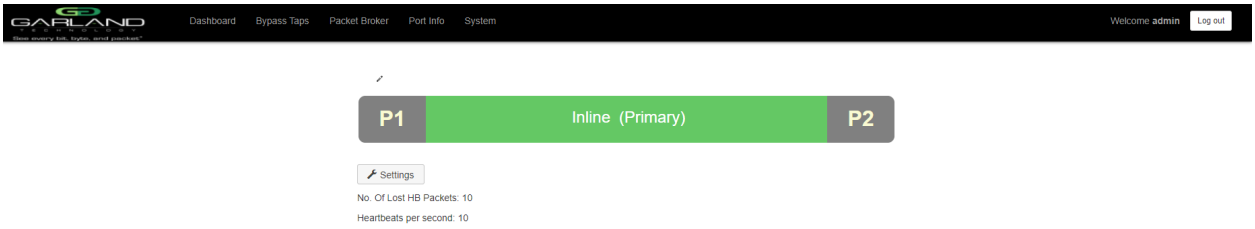
4.1 Primary/Secondary Inline Appliance

In the default tap configuration P1, P2 are network ports, P3, P4 are the primary inline appliance ports. A secondary inline appliance may be applied, P5, P6.

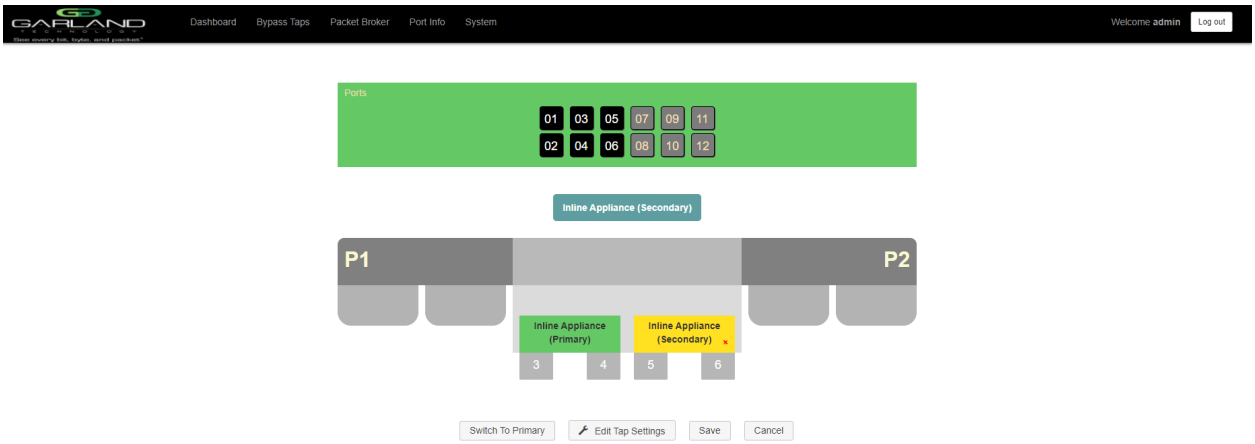
1. Add a secondary inline appliance by placing the cursor on the Inline Appliance (Secondary), above the tap. Press the left mouse button and hold to select. Drag the Inline Appliance (Secondary) on top of the Inline Appliance (Primary) and release the mouse button.

2. Select the Save to save updates.

The tap will display (Primary)



3. Place the cursor on the tap and double-press the left mouse button. The Tap panel will be displayed. The Primary Inline Appliance and Secondary Inline Appliance will be displayed. Green indicates active and yellow indicates standby.



4. Selecting the red X to remove the secondary inline appliance.

5. Select Edit Tap Settings to display, modify, enable or disable the Tap Mode, Fail Mode, LFP, Reverse Bypass and Revertive.

6. Select Switch To Primary to switch the tap traffic from the secondary inline appliance to the primary inline appliance.

7. Select Save to save updates.

8. Select Cancel to return the Bypass Taps panel.

4.2 Edit Tap Settings

1. Select Edit Tap Settings on the Bypass Tap panel.

   The Configure Inline Appliance panel will be displayed.

2. Select the Tap Mode.

Active	In normal conditions the tap will be inline. The traffic will flow bidirectional from one network port, through the primary inline appliance and back to the other network port. If an issue occurs with the primary inline appliance, loss of link or heartbeats, the tap will automatically switch to bypass, switching the traffic between the network ports. When the issue with the primary inline appliance is resolved, has link and heartbeats, the tap will automatically switch back to inline.
Force Bypass	If selected, the tap will switch the traffic between the network ports with no regard for the primary inline appliance link or heartbeats.

Force Inline	If selected, the tap will not be able to switch to bypass. The traffic will flow bidirectional from one network port, through the primary inline appliance and back to the other network port. If an issue occurs with the primary inline appliance, loss of link or heartbeats, the traffic will go down.

3. Select the Fail Mode.

Open	If selected and power is lost to the unit. The traffic will switch between the network ports.
Closed	If selected and power is lost to the unit. The traffic will go down.

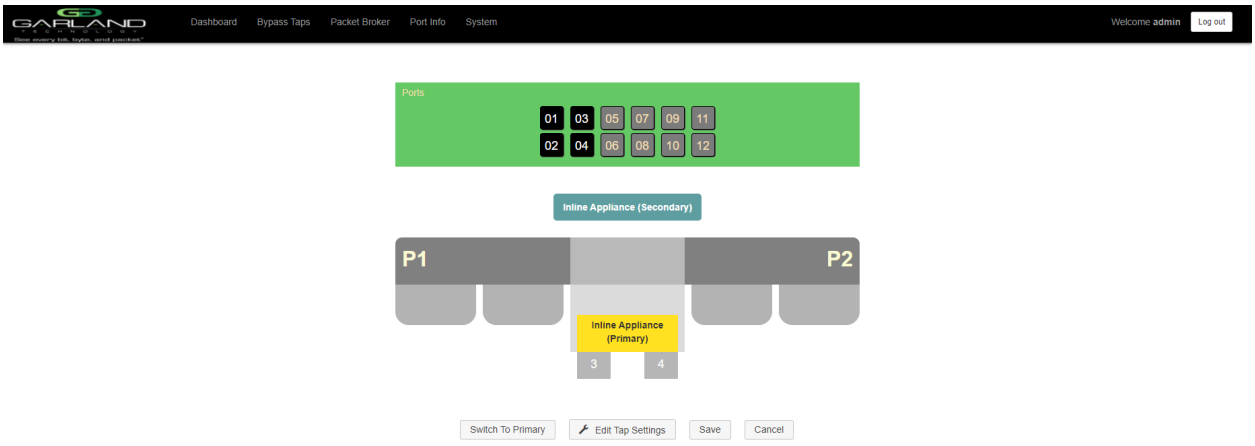
4. LFP	If enabled and the link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remains on.
5. Reverse Bypass	If enabled and the primary inline appliance fails, loss of link or heartbeats. The TX will be disabled on both of the network ports. The RX for both network ports remain on.
6. Revertive	If enabled and the traffic switches from the primary inline appliance, loss of link or heartbeats to the secondary inline appliance. The traffic will revert back to the primary inline appliance if in normal condition, has Link and heartbeats.

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

8. Select Cancel to return the Tap panel.

5 Monitor Ports

Monitor ports may be added to the tap if there is a primary inline appliance only or a primary and secondary inline appliance. The tap may have up to two monitor ports per network port, a total of four monitor ports per tap. The monitor ports may be added to monitor the ingress traffic or egress traffic.



1. Create a monitor port by placing the cursor on the desired port, shaded gray above the tap. Press the left mouse button and hold to select the port. Drag the port to the desired network port. The default of any monitor port is ingress. Change the monitor port traffic by placing the cursor on the ingress panel and press the left mouse button. Additional monitor ports may be added using the same procedure.

2. Remove a monitor port by selecting the red X.

3. Select Save to save updates.

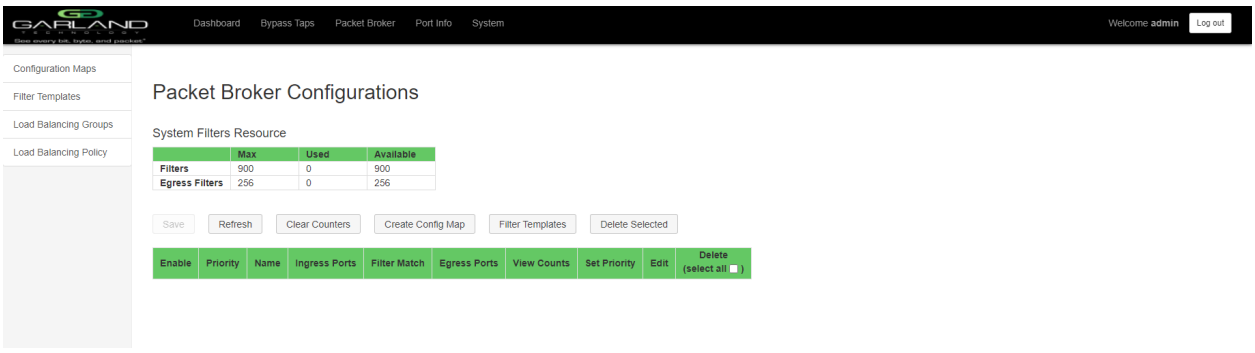
4. Select Cancel to return the Bypass Taps panel.

5. INT10G12xxBP Packet Broker

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

1. Filter Templates
2. Load Balance Policy
3. Load Balance Groups
4. Config Maps
5. Statistics
6. Ingress Filters Resources (900)
7. Egress Filter Resources (256)

Access the packet broker panel by selecting Packet Broker on the Dashboard menu bar.



The Packet Broker Configurations panel will be displayed.

1 Filter Templates
Filter templates may be applied to config maps as an ingress filter or egress filter. A filter template may be created as a Pass All, Pass By or Deny By. Filter templates will also appear on the Create Config Map panel. Modifications to the filter template being used as an ingress filter or egress filter are allowed. Changes made to the filter template applied to a config map will not change the original filter template. Once the config map is saved, the filter template becomes an ingress filter or egress filter, thus, filter templates may be deleted even if used on a config map. It is advisable to rename a filter template applied to a config map if the original filter template was modified when applied to a config map.

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 filter name, (0-16 characters).

4. Enter the description, optional (0-64 characters).

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 filter options will be displayed as follows:

    Source MAC Address and Source MAC Mask, (optional)
    Destination MAC Address and Destination MAC Mask, (optional)
    Ether Type
    Source IP Address and Source IP Mask, (optional)
    Destination IP Address and Destination IP Mask, (optional)
    Inner VLAN ID (0-4094)
    Outer VLAN ID (0-4094)
    DSCP (0-63)
    IP Protocol (TCP, UDP or Other, (0-255))
    L4 Source Port (0-65535) or Range, (Minimum 0-65535 – Maximum 0-65535)
    L4 Destination Port (0-65535) or Range, (Minimum 0-65535 – Maximum 0-65535)

7. Select Save Template once all desired options have been enabled and defined.

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.

2. Load Balance Policy
The load balance policy determines the hashing applied to load balance groups. The load balance policy options are as follows and may be applied as L3 and/or L4 or L2.

    Ipv4 Source
    Ipv4 Destination
    L4 Source Port

L4 Destination Port
MAC Source
MAC Destination

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

   The Load Balance Policy panel will be displayed.

2. Select the desired load balance policy options.

3. Select Save to save updates.

4. Select Cancel to disregard changes.

3. Load Balance Groups

Load balance groups are used as the egress on config maps. The traffic applied to the ports assigned to a load balance group will follow the hashing per the load balance policy. Ports may be added or removed from load balance groups as desired. Load balance groups will also appear on the Create Config Map panel.

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

   The Load Balancing Groups panel will be displayed.

2. Select Create Group.

   The Create New Load Balance Group panel will be displayed.

3. Enter the name, (0-16 characters).

4. Enter the description, optional (1-64 characters).

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

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

7. Select Save to save updates.

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

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

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

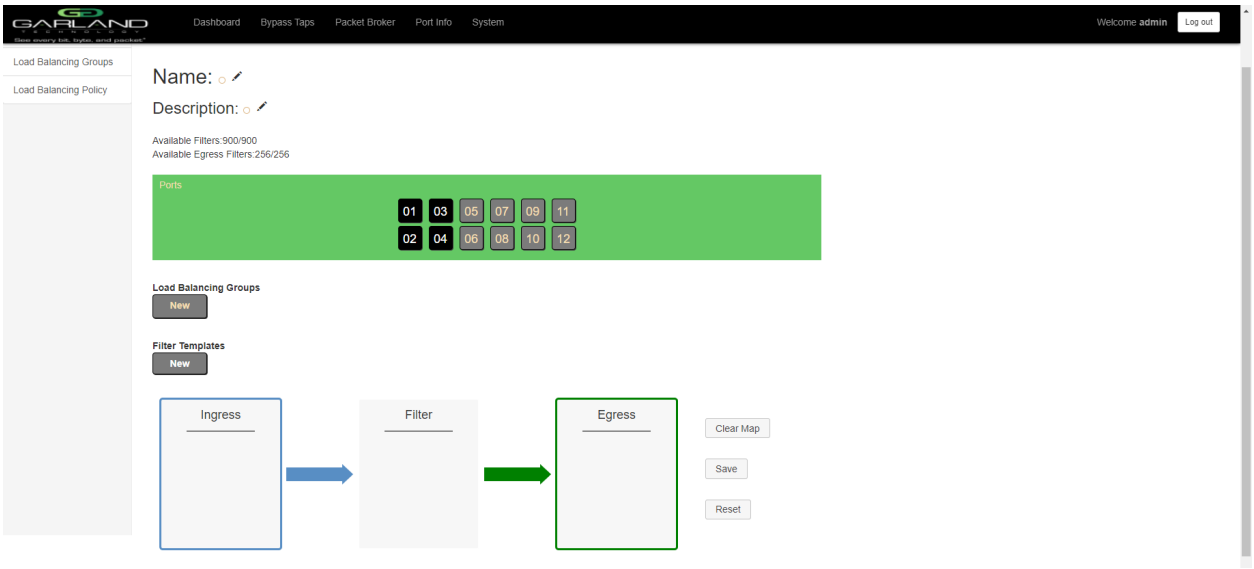
10. Deleted the load balance group by selecting the red X. Load balance groups may not be deleted if used to create a config map.

4. Config Maps

Config maps are unidirectional connections between ingress port(s) to egress port(s). Config maps may have one ingress filter or multiple ingress filters applied. Ingress filters may be modified as they are applied to a config map even if a filter template is used. Egress filters may be applied to egress ports and may be modified even if a filter template is selected.

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

   The Create Config Map panel will be displayed. Any previously created load balance groups or filter templates will be displayed. Any port shaded grey can be used for a config map with the exception that if the secondary inline appliance has been aplied to the tap, ports 5 and 6 are not available to be used on a config map.



2. Select the Name pencil to apply a name, optional.

3. Place the cursor in the Name panel and enter the name, (1-16 characters).

4. Select the Check to apply updates.

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

6. Place the cursor in the Description panel and enter the description, optional (1-64 characters).

7. Select the Check to apply updates.

4.1 Ingress Ports

1. Add ingress ports by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Ingress panel and release. Repeat for all desired ports.

> Ports may be added in any combination. If multiple ports are added, then the traffic from all ingress ports will be aggregated.

2. Remove a port by selecting the red X.

4.2 Ingress Filters

1. Add ingress filters by placing the cursor on the desired filter template. A previously created filter template or the New filter template may be selected. Select with the left mouse button. Drag the filter template to the Filter panel and release it. Repeat for all desired filter templates.

> Filter templates may be added in any combination. If multiple filter templates are added, then the top filter template is the highest priority. Filter templates may be selected and moved up or down depending on preference.

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

> The Edit Filter panel will be displayed.
>
> It is advisable to rename a previously created filter template if modifications are made when applied to a config map. Changes made to a previously created filter template will not change the original filter template.

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

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

4.3 Egress Ports

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

2. Add a load balance group by placing the cursor on the desired group. Select with the left mouse button. Drag the group to the Egress panel and release. If New is selected, ports may be applied by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the New panel and release.
Repeat for all desired ports.

> One load balance group may be applied to the egress. Additional separate ports may also be applied. The traffic applied to the ports assigned to the load balance group will follow the hashing per the load balance policy. If separate ports are added, then the traffic will be copied to the separate ports.

3. Remove a port or load balance group by selecting the red X.

4.4 Egress Filters

Egress filters may be applied to the ports assigned to the egress when creating a config map. Egress filters may not be applied to a load balance group. An egress filter may be created as a Pass By or Deny By.

1. Select the grey filter icon on the port.

   The Port XX Egress Filters panel will be displayed.

2. Add egress filters by placing the cursor on the desired filter template. A previously created filter template or the New filter template may be selected. Select with the left mouse button. Drag the filter template below the Port XX Egress Filters and release. Repeat for all desired filter templates.

   Filter templates may be added in any combination. If multiple filter templates are added, then the top filter template is the highest priority. Filter templates may be selected and moved up or down depending on preference.

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

   The Edit Filter panel will be displayed.

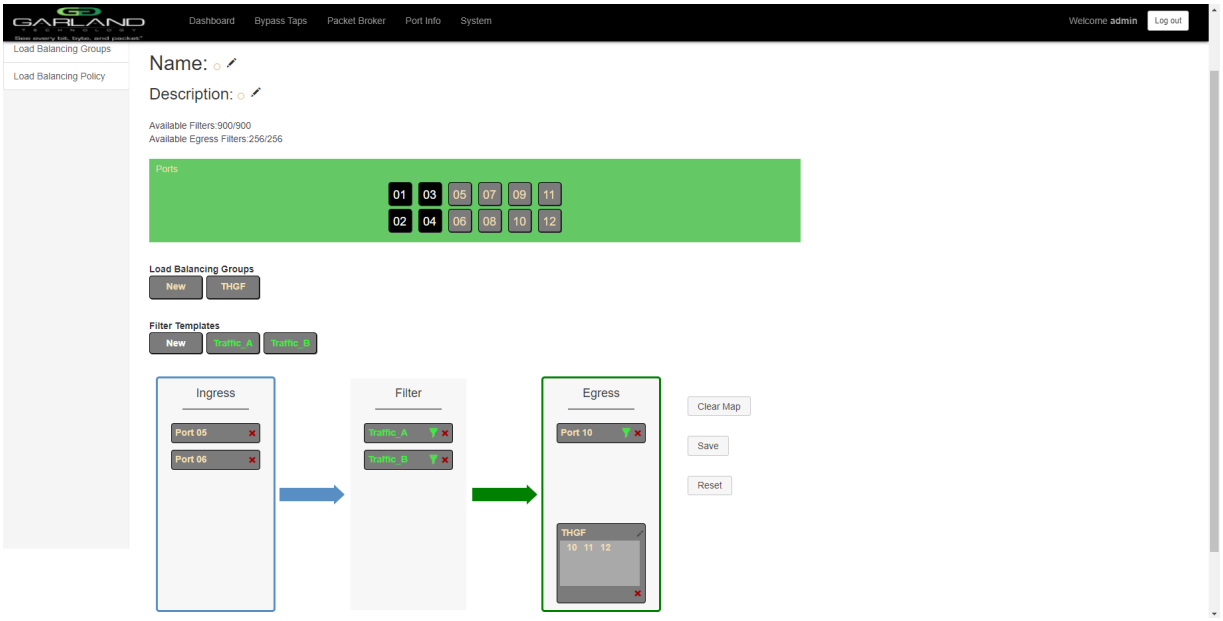
   It is advisable to rename a previously created filter template if modifications are made when applied to a config map. Changes made to a previously created filter template will not change the original filter template.

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

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

6. Select Back when all egress filters have been applied.

   The egress port filter icon changes to green.



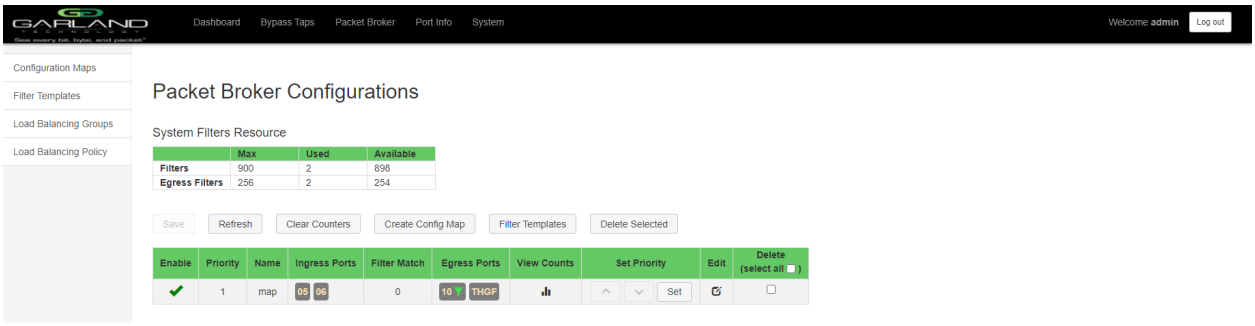
4.5 Config Map Save

1. Select Save to save the current configuration.

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

2. Select Yes to save the Config Map.

3. Select Cancel to disregard.



4.6 Modify a Config Map

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

   Name
   Description
   Add/Remove Ingress Ports
   Add/Remove/Modify/Reprioritize Ingress Filters
   Add/Remove Egress Ports
   Add/Remove/Modify/Reprioritize Egress Filters

4.6.1 Save

1. Select Save to save the current configuration.

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

2. Select Yes to save the config map.

3. Select Cancel to disregard.

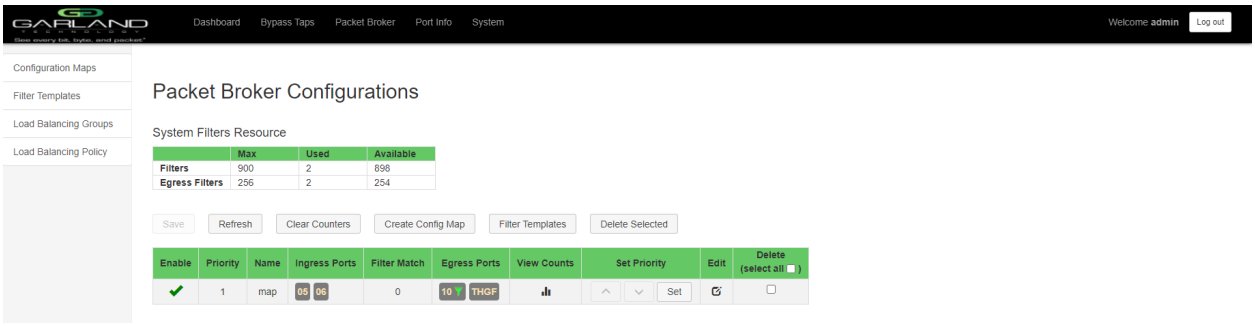
4.6.2 Reset

1. Select reset to reset the current configuration.

   The “Reset all changes?” panel will be displayed.

2. Select Yes to reset the Config Map.

3. Select Cancel to disregard.



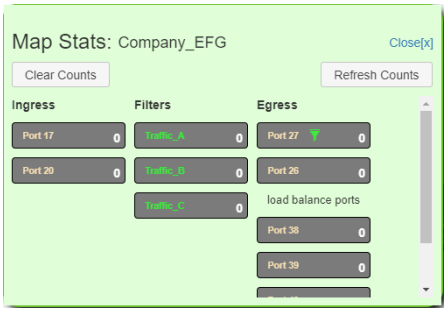
4.7 Config Map Statistics

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

1. Select Refresh to refresh the config map statistics.

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

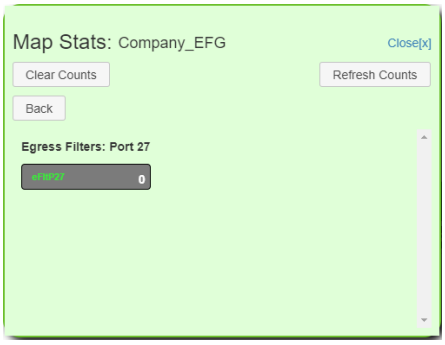
3. Select the View Counts icon to display individual statistics.



4. Select Refresh Counts to refresh the statistics.

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

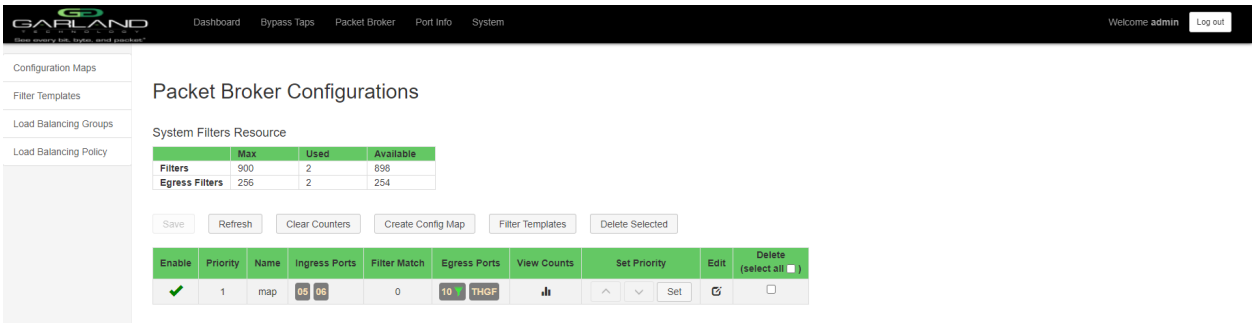
6. Select the Egress Filter icon to display the statistics.



7. Select Refresh Counts to refresh the statistics.

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

9. Select Back to return to the individual statistics.

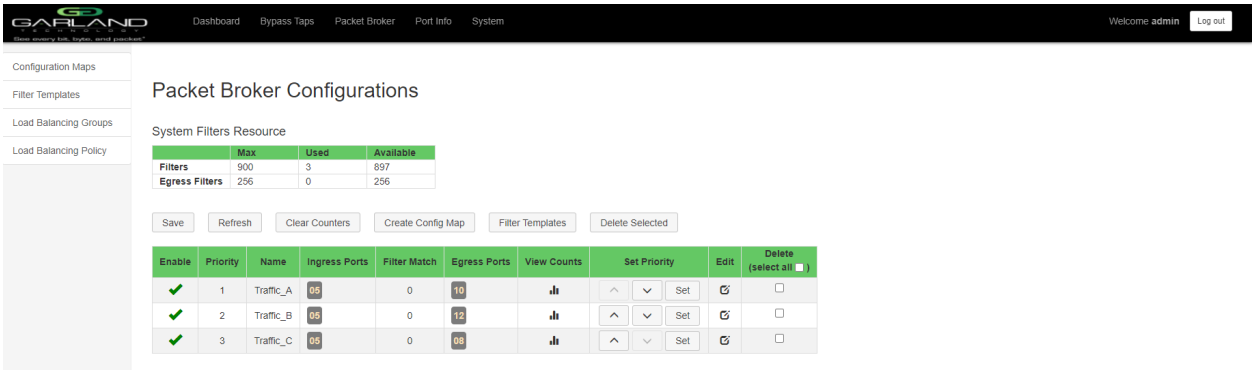


4.8 Delete Config Map

1. Select the Delete in the Delete column for the desired config map.

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

3. Select Delete Selected.



4.9 Config Map Priority

The config map priority needs to be considered when the same ingress port is used in multiple config maps to multiple egress destinations or the same egress destination. In this case, the config map with the highest priority will be considered first. In the above example, there are three config maps with ingress port 5. The Traffic_A config map is the highest priority, 1. The Traffic_B is the next priority, 2. The Traffic_C is the next priority, 3. Consequently, a config map with priority 21 has a higher priority than a config map with priority 34.

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

Method 1

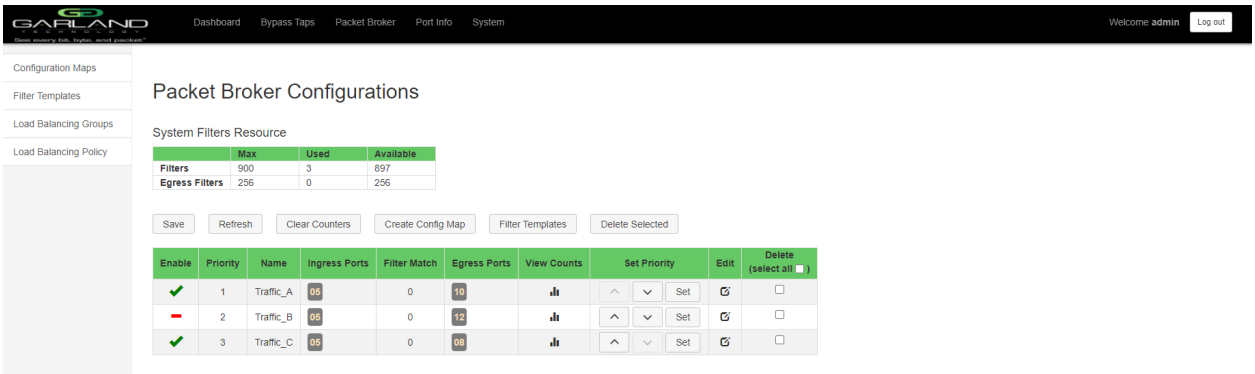
1. Select the up or down arrow for the config map.
2. Select Save to save updates.

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.



4.10 Enable/Disable Config Map

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

4.10.1 Disable Config Map

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

   The green check will change to a red dash.

2. Select Save.

4.10.2 Enable Config Map

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

   The red dash will change to a green check.

2. Select Save.