



User Guide

INT10G12MSBP / INT10G12SSBP



10/2024

Release Version: 4.33.2

Copyright © 2024 Garland Technology, LLC. All rights reserved.

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

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

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

Notice

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

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

Table of Contents

1. Dashboard	6
Basic LED Indications.....	6
Dashboard Panel	6
LED Indications.....	6
Packet Broker	7
Dashboard Panel	7
LED Indications.....	7
Default Tap Mode.....	8
Dashboard Panel	8
LED Indications.....	8
Primary-Secondary Tap Mode.....	9
Dashboard Panel	9
LED Indications.....	9
Load Balance Tap Mode.....	10
Dashboard Panel	10
LED Indications.....	10
ATLB2 Chained Tap Mode	11
Dashboard Panel	11
LED Indications.....	11
2. System.....	12
System Info	13
General	13
Admin.....	13
Users	13
Groups	14
Authentication	14
Local Authentication Disable	15
Local Authentication Enable	15
TACACS Primary Authentication	15
TACACS Test	15
TACACS Ping Test	16
TACACS Secondary Authentication	16
TACACS Test	16
TACACS Ping Test	16
Network Settings	17
IPv4 / Disable	17
IPv4 Enable.....	17
IPv6 Enable.....	17
IPv6 Disable	18
Add SSL Certificate.....	18

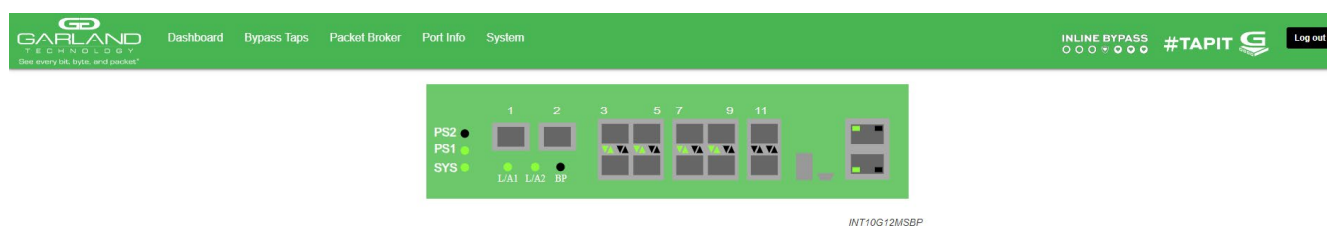
Disable Using Uploaded SSL Certificate	18
Date & Time	19
Timezone	19
UTC	19
Manually Set Date & Time	19
NTP No Authentication (Symmetric)	20
NTP Authentication (Symmetric)	20
Syslog	21
Syslog Test	21
SNMP	21
SNMP Test	22
Export Configuration	22
Import Configuration	22
Software Upgrade	23
Reboot	23
3. Bypass Taps	24
Default Tap Mode	25
Bypass Tap Name	25
Heartbeat Settings	26
Taps Settings	26
Primary-Secondary Tap Mode	30
Bypass Tap Name	31
Heartbeat Settings	31
Configure Primary-Secondary Tap Mode	31
Taps Settings	32
Switch To Primary	35
Load Balance Tap Mode	36
Bypass Tap Name	37
Heartbeat Settings	37
Configure Load Balance Tap Mode	37
ATLB2 Chained Tap Mode	41
Configure ATLB2 Chained Tap Mode	42
Remove Entity	42
Add Entity	44
Remove Entity Inline Appliance Member	44
Add Entity Inline Appliance Member	45
Taps Settings	45
ATLB2 Chained Tap Mode GUI Indications	48
Normal	48
Entity Member Abnormal	49
Entity Bypass	50
Entity Removed From Chain	51

ATLB2 Chained Tap Forced Bypass.....	52
ATLB2 Chained Tap Bypass.....	53
4 Packet Broker	54
Tunnels	55
Encapsulate l2GRE Packets (GRE-TX Only)	55
Decapsulate l2GRE Packets (GRE-RX Only).....	57
Filter Template.....	59
Load Balancing Group	60
Load Balancing Policy	60
Config Map	61
Ingress.....	62
Filters.....	62
Egress.....	63
Egress Filter.....	64
Config Map Save	65
Modify a Config Map	66
Delete Config Map	67
Config Map Priority.....	67
Method 1	68
Method 2	68
Enable/Disable Config Map	69
Disable Config Map.....	69
Enable Config Map.....	69
4. Port Info	70
Port Configuration.....	70
Port Description.....	70
Set Speed	71
Mode	71
Port Statistics	71
VLAN Tag	71
VLAN Strip	72

1. Dashboard

This section provides an overview of the basic dashboard architecture, default port assignments and LED indications. The port assignments and LED indications will change on the dashboard based on configuration changes. 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.

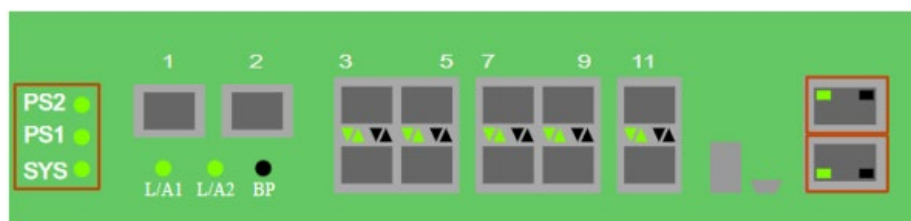
The dashboard provides access to the Packet Broker, Port Info and System configuration options by selecting the desired option in the top menu bar. These options are covered in detail per their specific sections.



Basic LED Indications

The basic LED indications are consistent regardless of configuration changes. The Ethernet and Serial interfaces always indicate (GREEN). However, on the faceplate, the Ethernet Interface has LEDs to indicate link and activity while there are no Serial Interface LEDs.

Dashboard Panel



LED Indications

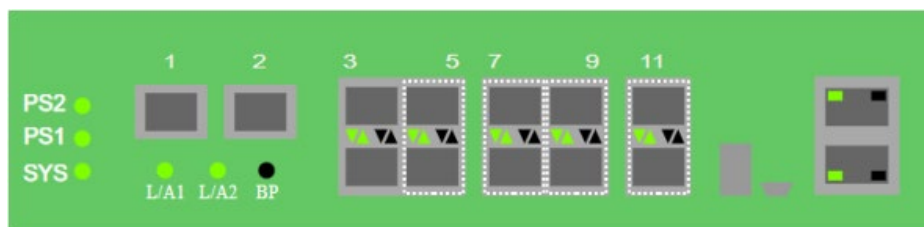
PS2	Power Supply 2 LED
PS1	Power Supply 1 LED
SYS	System LED
Ethernet Interface	Upper Left LED (always illuminated)
Serial Interface	Lower Left LED (always illuminated)

Packet Broker

The packet broker section typically consists of ports 5 through 12. However, the available packet broker ports is determined by the following conditions:

- The tap mode selected, Default, Load Balance, Primary-Secondary or ATLB2 Chained.
- If tap monitor ports are applied

Dashboard Panel



LED Indications

Port 3 Left Up Arrow	Link LED
Port 4 Left Down Arrow	Link LED
Port 5 Left Up Arrow	Link LED
Port 6 Left Down Arrow	Link LED
Port 7 Left Up Arrow	Link LED
Port 8 Left Down Arrow	Link LED
Port 9 Left Up Arrow	Link LED
Port 10 Left Down Arrow	Link LED
Port 11 Left Up Arrow	Link LED
Port 12 Left Down Arrow	Link LED

* The right up/down arrows for ports 3 through 12 are activity LEDs. These LEDs are N/A in the GUI.

Default Tap Mode

In this mode, the network ports and inline appliance ports are defined by the system.

Dashboard Panel



LED Indications

L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	Tap 1 Bypass LED
Port 3 Left Up Arrow	Tap 1 Inline Appliance Link LED
Port 4 Left Down Arrow	Tap 1 Inline Appliance Link LED

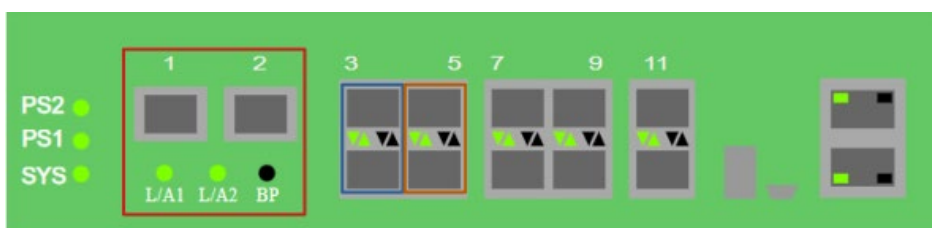
* The right up/down arrows for ports 5 through 12 are activity LEDs. These LEDs are N/A in the GUI.

* The L/A1 and L/A2 LEDs only indicate link in the GUI.

Primary-Secondary Tap Mode

In this mode, the network ports and the primary inline appliance ports are defined by the system for the tap. The secondary inline appliance ports will be automatically configured by the system in the order assigned to the tap. The secondary inline appliance ports availability are considered in vertical pairs, 5/6, 7/8, etc.

Dashboard Panel



LED Indications

L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	Tap 1 Bypass LED
Port 3 Left Up Arrow	Tap 1 Primary Inline Appliance Link LED
Port 4 Left Down Arrow	Tap 1 Primary Inline Appliance Link LED
Port X Left Up Arrow	Tap 1 Secondary Inline Appliance Link LED
Port X Left Down Arrow	Tap 1 Secondary Inline Appliance Link LED

* The right up/down arrows for the primary inline appliance ports 3 and 4 as well as the secondary inline appliance ports X are activity LEDs. These LEDs are N/A in the GUI.

* The L/A1 and L/A2 LEDs only indicate link in the GUI.

Load Balance Tap Mode

In this mode, the network ports and initial inline appliance ports are defined by the system for the tap. The tap may have up to three additional inline appliance ports applied, total 4. The ports will be automatically configured by the system in the order assigned to the tap. The ports availability are considered in vertical pairs, 5/6, 7/8, etc.

Dashboard Panel



LED Indications

L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	N/A
Port 9 Left Up Arrow	Tap 1 Inline Appliance Link LED
Port 10 Left Down Arrow	Tap 1 Inline Appliance Link LED
Port X Even Left Up Arrow	Tap 1 Additional Inline Appliance 2 through 4 Link LED
Port X Odd Left Down Arrow	Tap 1 Additional Inline Appliance 2 through 4 Link LED

* The right up/down arrows for the inline appliance ports 3 and 4 as well as the additional inline appliance ports X are activity LEDs. These LEDs are N/A in the GUI.

* The L/A1 and L/A2 LEDs only indicate link in the GUI.

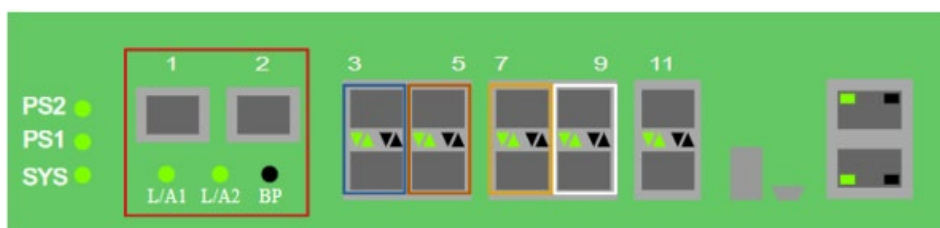
ATLB2 Chained Tap Mode

When this mode is applied, the system automatically configures the following default configuration.

Ports 1	Tap 1 Network Port
Ports 2	Tap 1 Network Port
Ports 3-4	Entity A Inline Appliance Ports
Ports 5-6	Entity B Inline Appliance Ports
Ports 7-8	Entity C Inline Appliance Ports
Ports 9-10	Entity D Inline Appliance Ports

Any previous configured database associated with ports 1 through 10 will be deleted when this mode is applied. Network ports 1 and 2 are paired. The network traffic is chained through entities A, B, C and D.

Dashboard Panel



LED Indications

L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	Tap 1 Bypass LED
Port 3 Left Up Arrow	Entity A Inline Appliance Link LED
Port 4 Left Down Arrow	Entity A Inline Appliance Link LED
Port 5 Left Up Arrow	Entity B Inline Appliance Link LED
Port 6 Left Down Arrow	Entity B Inline Appliance Link LED
Port 7 Left Up Arrow	Entity C Inline Appliance Link LED
Port 8 Left Down Arrow	Entity C Inline Appliance Link LED
Port 9 Left Up Arrow	Entity D Inline Appliance Link LED
Port 10 Left Down Arrow	Entity D Inline Appliance Link LED

* The right up/down arrows for the entity inline appliance ports 3 through 10 are activity LEDs. These LEDs are N/A in the GUI.

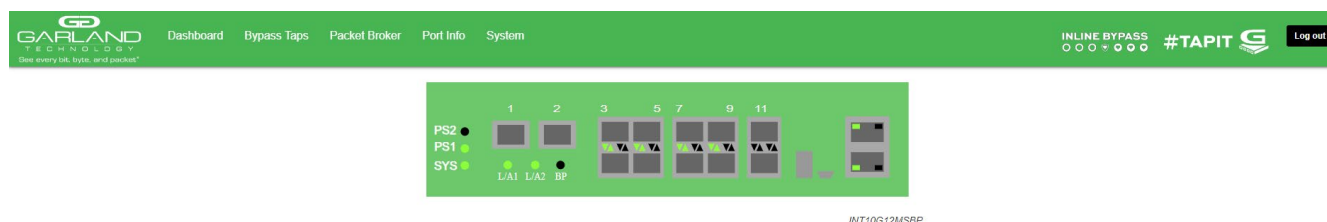
* The L/A1 and L/A2 LEDs only indicate link in the GUI.

2. System

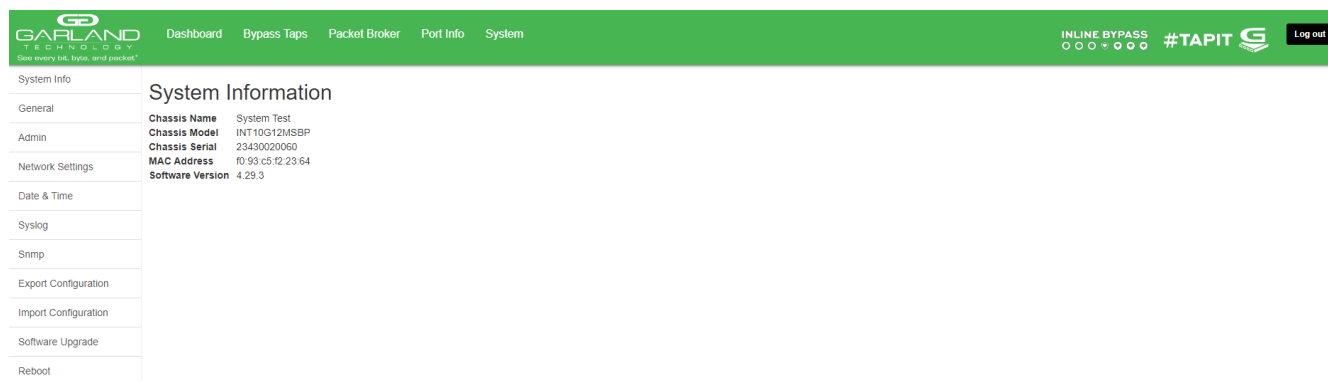
The following configuration options may be displayed, modified, enabled, or disabled under the System panel.

System Info
General
Admin
Network Settings
Date & Time
Syslog

SNMP
Export Configuration
Import Configuration
Software Upgrade
Reboot



1. Select System on the Dashboard Menu bar.



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

System Info

The System Information panel displays the following.

Chassis Name	Chassis Model	Chassis Serial Number
MAC Address	Software Version	

1. Select System Info.

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 display.

Users

The default user is “admin”. Changes to the default user “admin” are allowed. However, the “admin” user may not 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 48 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 48 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 default 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. Enter the Timeout value, (5-60 sec).
5. Select Save to save updates.
6. 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. Enter the Timeout value, (5-60 sec).
5. Select Save to save updates.
6. 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, (www.xxx.yyy.zzz/xx).
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 Taps

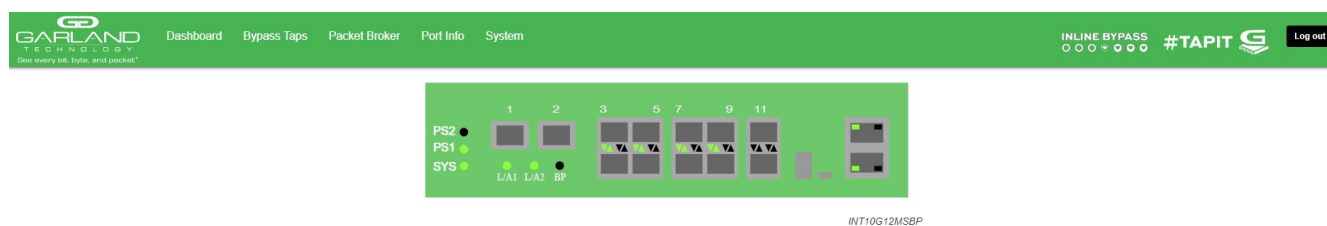
The following mode options may be displayed, modified, enabled, or disabled under the Bypass Taps panel.

Default Tap Mode

Primary-Secondary Tap Mode

Load Balance Tap Mode

ATLB2 Chained Tap Mode



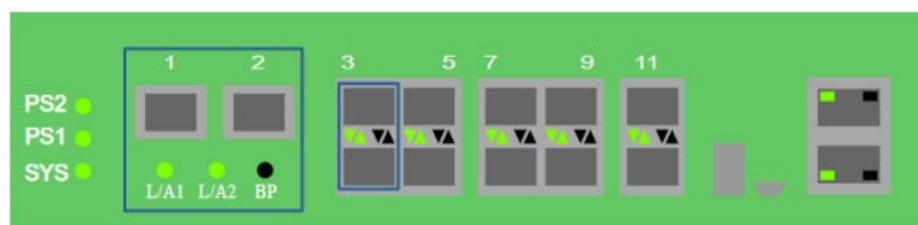
1. Select Bypass Taps on the Dashboard Menu bar.



The Bypass Taps panel will be displayed.

Default Tap Mode

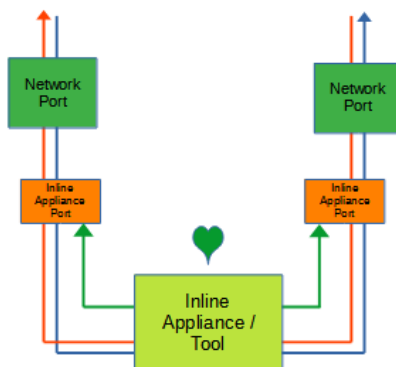
In this mode, the network ports and inline appliance ports are defined by the system. Ports 5 through 12 may be configured as packet broker ports or tap monitor ports. The network ports are typically connected to network devices such as a server or router. The inline appliance ports are typically connected 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.



Tap 1

- Port 1 (Network)
- Port 2 (Network)
- Port 3 (Inline Appliance)
- Port 4 (Inline Appliance)

Figure 1 Default Tap Mode



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 any 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 Default Tap Mode (Inline)

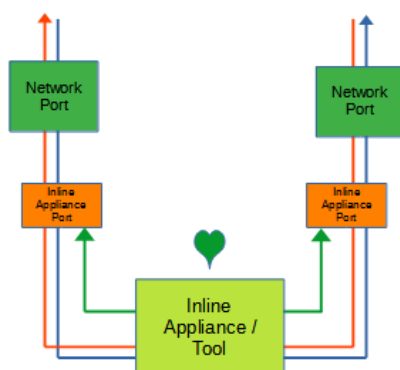
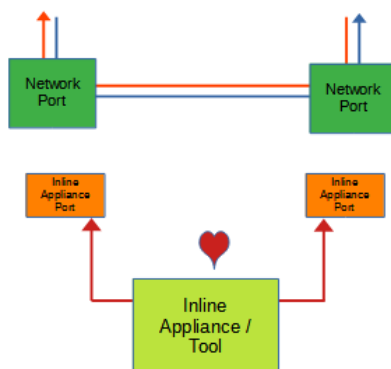
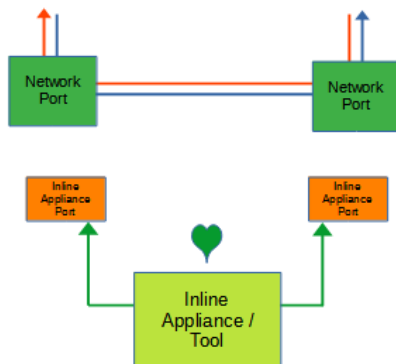


Figure 3 Default Tap Mode (Bypass)



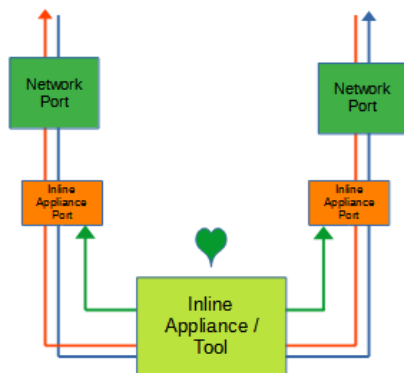
Force Bypass If selected, the tap will switch the traffic between the network ports with no regard for the inline appliance port(s), link, or heartbeats. Typically used during maintenance activities.

Figure 4 Default Tap 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 Default Tap Mode (Force Inline)



4. 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.

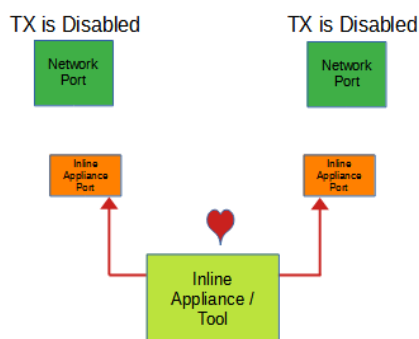
5. LFP If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 6 Default Tap 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 Default Tap Mode (Reverse Bypass)



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

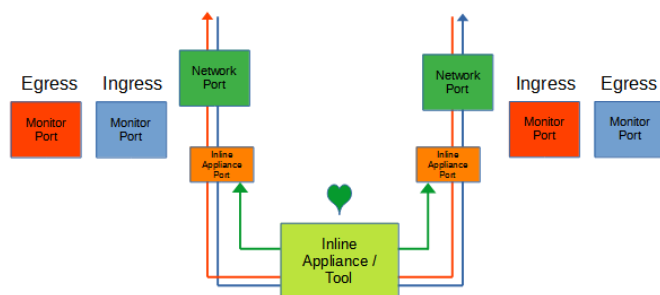
8. Select Cancel to return the Bypass Taps panel.

Monitor Ports

Monitor ports may be added to any tap. Each tap may have up to two monitor ports per network port, total of four monitor ports per tap. The monitor ports may be added to monitor the ingress traffic or egress traffic. The monitor ports will continue to pass traffic to the connected device when the tap is placed in the Forced Bypass mode.

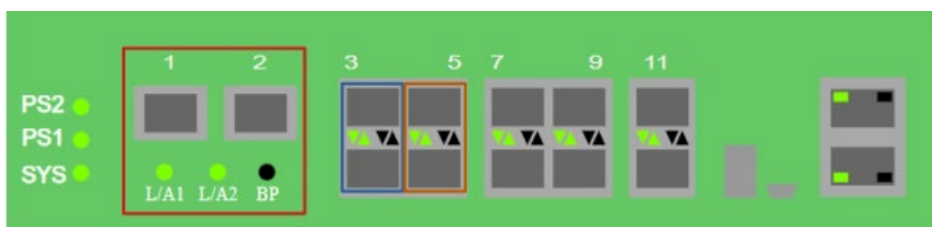
1. Create a monitor port by placing the cursor on the desired port, shaded gray above the tap. Press the left mouse button and hold to select the port. Drag the port to the desired network port. The default of any monitor port is ingress. Change the monitor port traffic by placing the cursor on the ingress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

Figure 8 Default Tap Mode (Monitor Port)



Primary-Secondary Tap Mode

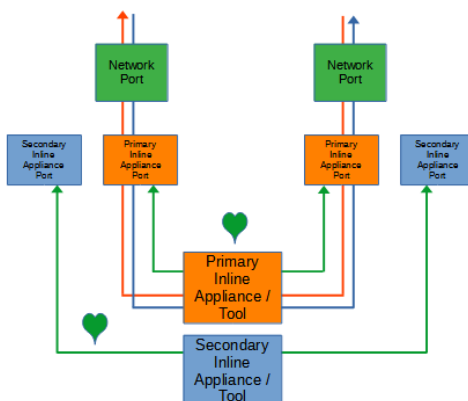
In this mode, the network, primary inline appliance, and secondary inline appliance ports are defined by the system. The network ports are typically connected to network devices such as a server or router. The primary inline appliance ports are typically connected to a primary inline appliance or tool to monitor the network traffic. The secondary inline appliance ports are typically connected to a secondary inline appliance or tool to monitor the network traffic. The network traffic is sent to the primary inline appliance or the secondary inline appliance. Heartbeat packets are transmitted bidirectionally from the primary inline appliance ports on the tap through the primary inline appliance or tool to monitor the health of the device. Likewise, heartbeat packets are transmitted bidirectionally from the secondary inline appliance ports on the tap through the secondary inline appliance or tool to monitor the health of the device.



Tap 1

- Port 1 (Network)
- Port 2 (Network)
- Port 3 (Primary)
- Port 4 (Primary)
- Port 5 (Secondary)
- Port 6 (Secondary)

Figure 9 Primary-Secondary Tap Mode



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 any inline appliance port before any tap will switch from the primary inline appliance to the secondary inline appliance to bypass.

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

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

4. Select Save to save updates.
5. Select Cancel to return the Bypass Taps panel.

Configure Primary-Secondary Tap Mode

1. Edit the tap mode by placing the cursor on any tap and double-press the left mouse button.

The Tap panel will be displayed.

2. Place the cursor on the Primary-Secondary Mode Select option. Select with the left mouse button. Drag the Primary-Secondary option to the blue box and release.
3. Select the red X to remove.
4. Place the cursor on the Inline Appliance option. Select the left mouse button. Drag the Inline Appliance option to the blue box and release.
5. Select the red X to remove.

6. Select Save to save updates.

The Bypass Taps panel will be displayed. Inline (Primary) will be displayed.

7. Place the cursor on the tap and double-press the left mouse button.

The Tap panel will be displayed. Green indicates Active, Yellow indicates Standby.

8. Select Cancel to return the Bypass Taps panel.

Taps Settings

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

Tap Modes	LFP
Fail Mode	Reverse Bypass

1. Edit the Tap Settings, by placing the cursor on any 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 primary inline appliance port(s) and secondary inline appliance port(s), loss of link or heartbeats. The default switching action from inline to bypass is defined by the system as, from the primary inline appliance, to the secondary inline appliance, to bypass. The default switching action from bypass to inline is defined by the system as, from bypass to the secondary inline appliance. Switching from the secondary inline appliance to the primary inline appliance may be accomplished via two methods. Select the Switch to Primary option or enable Revertive. If revertive is enabled, then the system will switch from bypass to the primary inline appliance if it is recovered first.

Figure 10 Primary-Secondary Tap Mode (Primary Inline)

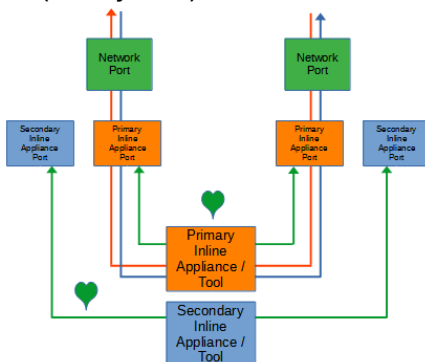


Figure 11 Primary-Secondary Tap Mode (Secondary Inline)

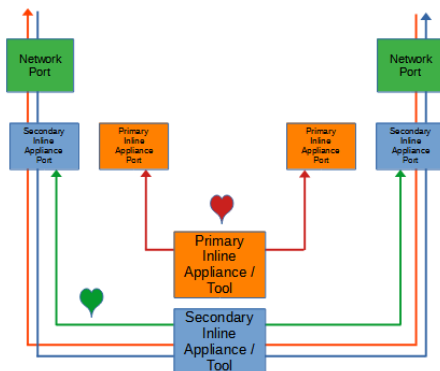
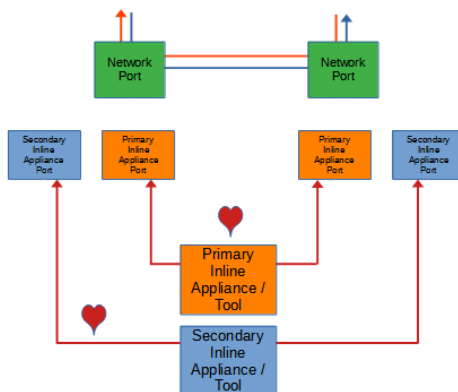
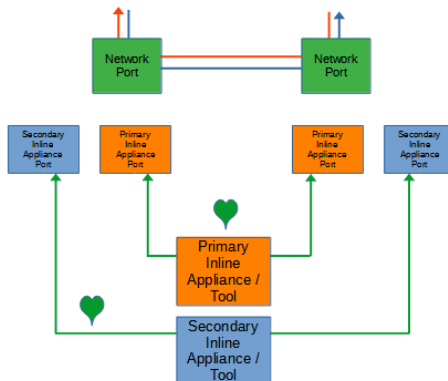


Figure 12 Primary-Secondary Tap Mode (Bypass)



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

Figure 13 Primary-Secondary Tap Mode (Force Bypass)



4. 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. |

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.

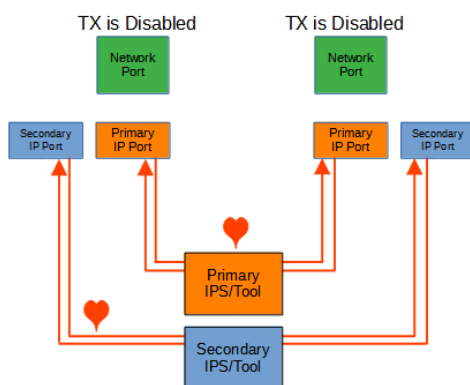
Figure 14 Primary-Secondary Tap Mode (LFP)



6. Reverse Bypass

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

Figure 15 Primary-Secondary Tap Mode (Reverse Bypass)



7. Revertive

If enabled and the primary inline appliance port(s) fail, loss of link or heartbeats, the system will switch to the secondary inline appliance. When the issue with the primary inline appliance is resolved, has link and heartbeats. The traffic will automatically revert to the primary inline appliance. This option also affects the switching from bypass to inline. If disabled, the system is designed to switch from bypass to the secondary inline appliance. If the primary inline appliance restores first, has link and heartbeats, a manual switch to the primary inline appliance is required. If enabled and the primary inline appliance restores first, the system will switch from bypass to the primary inline appliance.

8. Select Accept to save updates. Save must additionally be selected on the Bypass Taps panel.
9. Select Cancel to return the Bypass Taps panel.

Switch To Primary

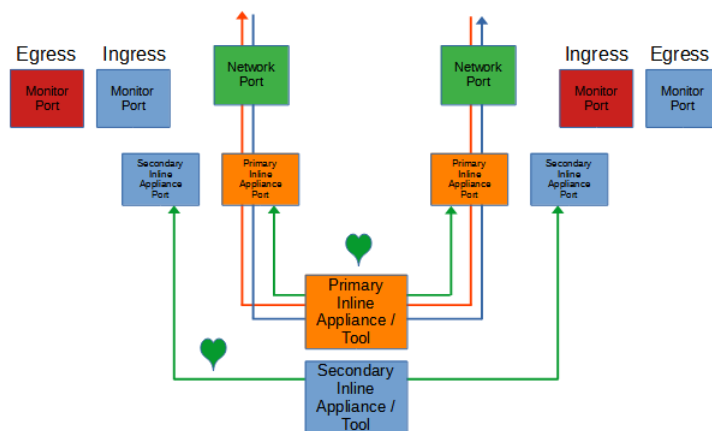
1. Select to manually switch the traffic from the secondary inline appliance to the primary inline appliance.

Monitor Ports

Monitor ports may be added to any tap. Each tap may have up to two monitor ports per network port, total of four monitor ports per tap. The monitor ports may be added to monitor the ingress traffic or egress traffic. The monitor ports will continue to pass traffic to the connected device when the tap is placed in the Forced Bypass mode.

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. Select Save to save updates.
3. Select Cancel to return the Bypass Taps panel.

Figure 16 Primary-Secondary Tap Mode (Monitor Port)



Load Balance Tap Mode

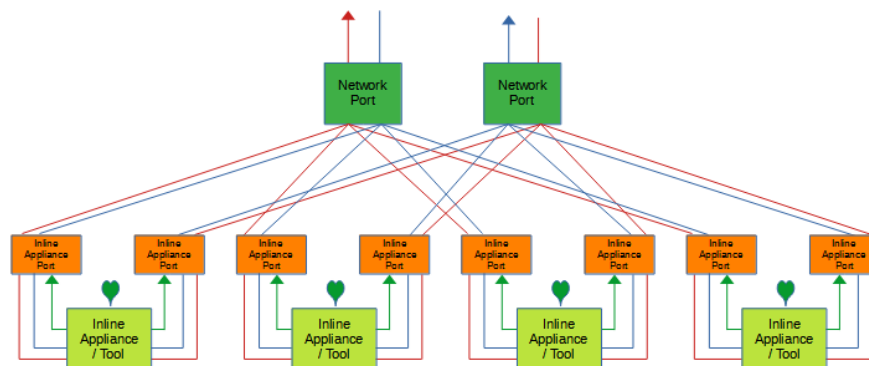
In this mode, the network and inline appliance ports are defined by the system. The tap may have up to three additional inline appliance ports applied, total 4. Any port that is not assigned as an inline appliance port may be configured as packet broker port. The network ports are typically connected to network devices such as a server or router. The inline appliance ports are typically connected to IPSs or tools to monitor the network traffic. The network traffic is load balanced to the inline appliance ports. However, heartbeat packets are transmitted bidirectionally from inline appliance ports on the tap through the IPSs or tools to monitor the health of the devices.



Tap 1

- Port 1 (Network)
- Port 2 (Network)
- Port 3 (Inline Appliance)
- Port 4 (Inline Appliance)
- Port 5 (Inline Appliance)
- Port 6 (Inline Appliance)
- Port 7 (Inline Appliance)
- Port 8 (Inline Appliance)
- Port 9 (Inline Appliance)
- Port 10 (Inline Appliance)

Figure 17 Load Balance Tap Mode



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 an inline appliance port before any tap will remove the inline appliance from the load balance group.

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.

Configure Load Balance Tap Mode

1. Edit the tap mode by placing the cursor on any tap and double-press the left mouse button.

The Tap panel will be displayed.

2. Place the cursor on the Load Balance Mode Select option. Select with the left mouse button. Drag the Load Balance option to the blue box and release.

3. Select the red X to remove.

4. Place the cursor on the Inline Appliance option. Select the left mouse button. Drag the Inline Appliance option to the blue box and release. The next available vertical port pair will be added. Repeat this step to apply up to four inline appliance ports per tap.

5. Select the red X to remove.

6. Select Save to save updates.

The Bypass Taps panel will be displayed. Inline will be displayed.

7. Place the cursor on the tap and double-press the left mouse button.

The Tap panel will be displayed. Green indicates Active.

8. Select Cancel to return the Bypass Taps panel.

Taps Settings

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

Tap Modes	Reverse Bypass
Fail Mode	Bypass Threshold
LFP	

1. Edit the Tap Settings, by placing the cursor on any 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, defined by the bypass threshold value, 1-4. When the issue with the inline appliance port(s) is resolved, have link and heartbeats, the tap will automatically switch back to inline.
--------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 18 Load Balance Tap Mode (Inline)

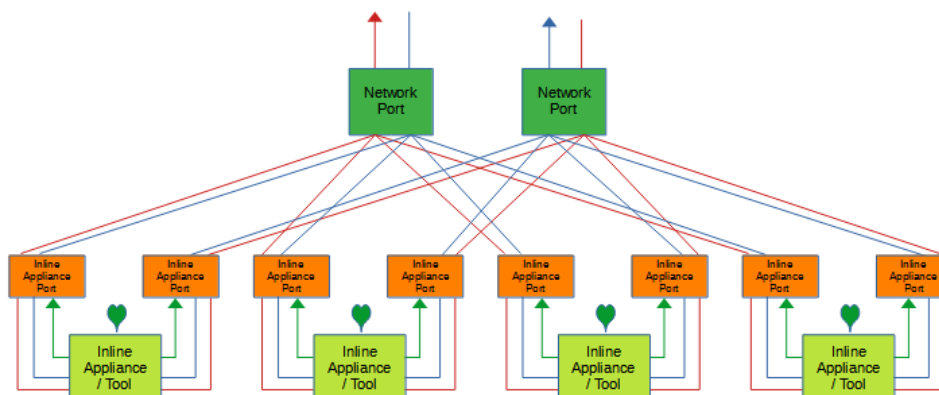
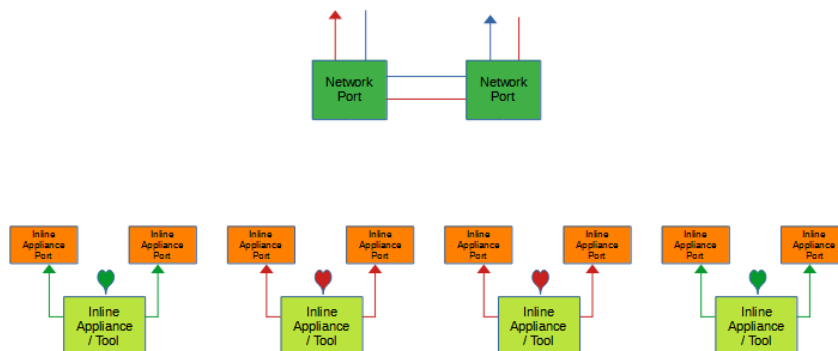
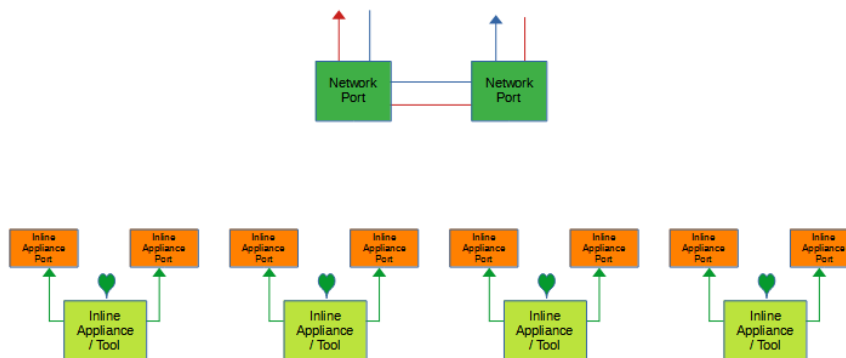


Figure 19 Load Balance Tap Mode (Bypass, Bypass Threshold=2)



Force Bypass If selected, the tap will switch the traffic between the network ports with no regard for the inline appliance ports, link, or heartbeats. Typically used during maintenance activities.

Figure 20 Load Balance Tap Mode (Force Bypass)



4. 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.

5. LFP

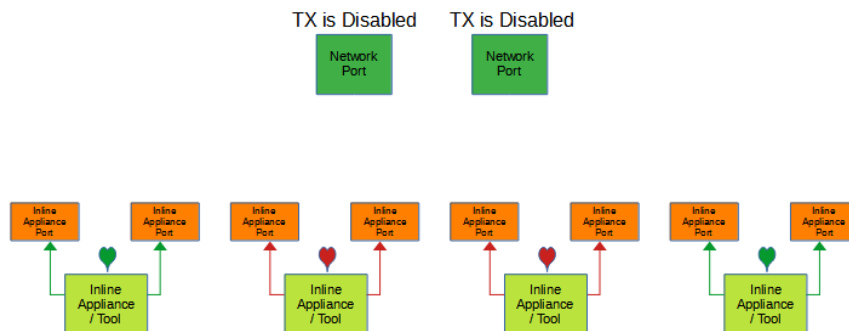
If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 21 Load Balance Tap Mode (LFP)



6. Reverse Bypass If enabled and the inline appliance port(s) fail, loss of link or heartbeats, defined by the bypass threshold value, 1-4. The TX will be disabled on both of the network ports. The RX for both network ports remain on.

Figure 22 Load Balance Tap Mode (Reverse Bypass, Bypass Threshold=2)



7. Bypass Threshold The bypass threshold determines how many inline appliances port(s) may fail, loss of link or heartbeats, before the tap switches to bypass.
8. Select Accept to save updates. Save must additionally be selected on the Bypass Taps panel.
9. Select Cancel to return the Bypass Taps panel.

ATLB2 Chained Tap Mode

When the tap is placed in this mode the system automatically defines:

- Ports 1-2 Network Ports
- Ports 3-4 Entity A inline appliance ports
- Ports 5-6 Entity B inline appliance ports
- Ports 7-8 Entity C inline appliance ports
- Ports 9-10 Entity D inline appliance ports

Any previous configured database associated with ports 1 through 12 will be deleted when this mode is applied. Entity inline appliance ports or entities may be removed. Any entity inline appliance ports that are removed may be used as packet broker ports. The network ports are typically connected to network devices such as a server or router. The network traffic is chained through entities A, B, C and D and load balanced to each entity inline appliance ports. Heartbeat packets are transmitted bidirectionally from the entity inline appliance ports on the tap through the IPSs or tools to monitor the health of the devices.



Tap 1

Port 1 (Network)
Port 2 (Network)

Entity A

Port 3 (Inline Appliance)
Port 4 (Inline Appliance)

Entity B

Port 5 (Inline Appliance)
Port 6 (Inline Appliance)

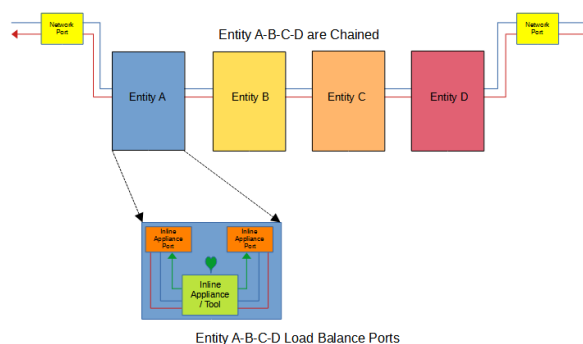
Entity C

Port 7 (Inline Appliance)
Port 8 (Inline Appliance)

Entity D

Port 9 (Inline Appliance)
Port 10 (Inline Appliance)

Figure 23 ATLB2 Chained Tap Mode



Configure ATLB2 Chained Tap Mode

1. Select the Settings option on the Bypass Taps panel.

The Configure Tap Settings panel will be displayed.

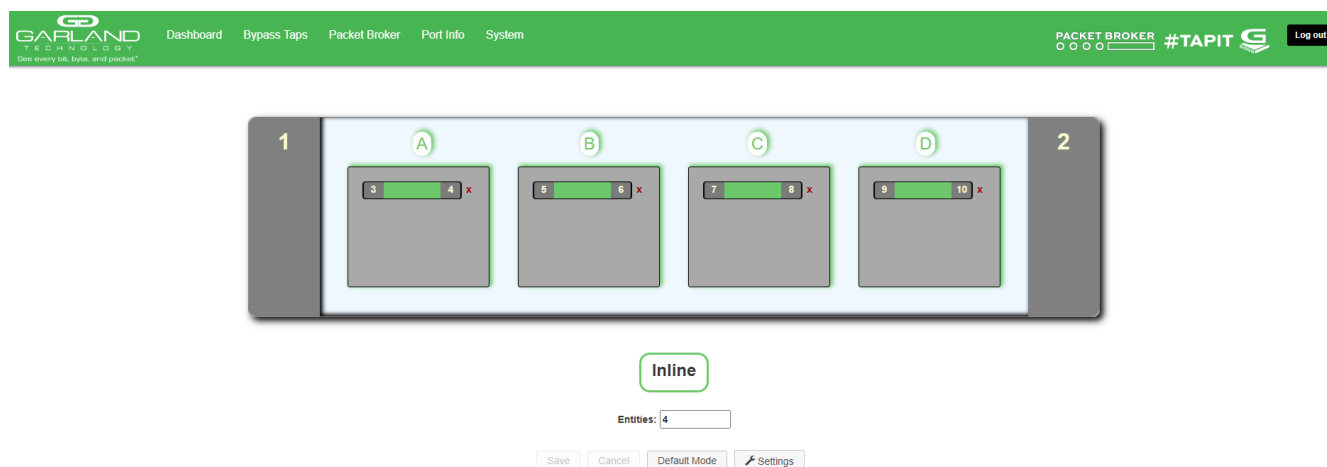
2. Select the ATLB2 Chained Mode option.

3. Select the Save option.

A "Packetbroker data will be cleared. Go to ATLB2 Mode?" message will be displayed.

4. Select OK.

The ATLB2 Chained tap mode will be displayed.



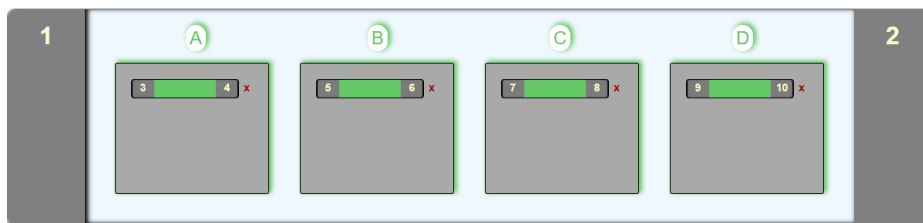
The default configuration will be displayed.

Remove Entity

An entity is removed from the chain by removing all the inline appliance port members. Entity inline appliance port members are removed as member pairs. If the entity inline appliance port members are removed, the ports may be configured as packet broker ports.

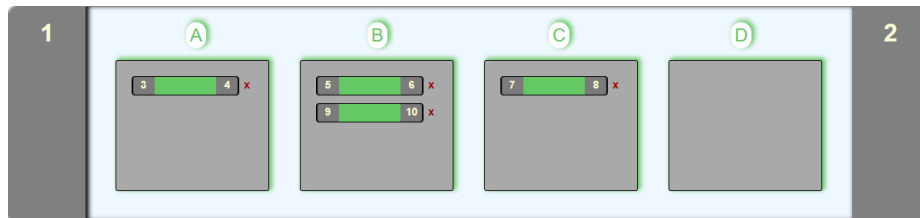
1. Select the down arrow in the Entities panel, 4, 3, 2, 1.

Basic 4 Entity Configuration



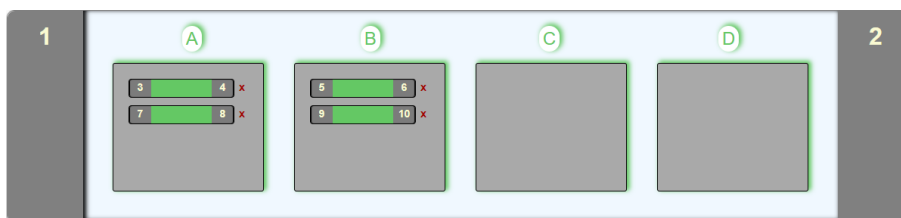
- Ports 1-2 Network Ports
- Ports 3-4 Entity A Inline Appliance Ports
- Ports 5-6 Entity B Inline Appliance Ports
- Ports 7-8 Entity C Inline Appliance Ports
- Ports 9-10 Entity D Inline Appliance Ports

Basic 3 Entity Configuration



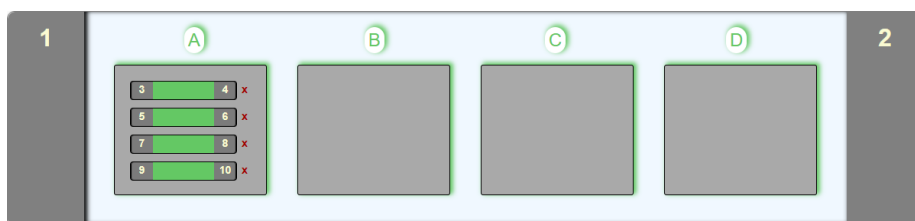
- Ports 1-2 Network Ports
- Ports 3-4 Entity A Inline Appliance Ports
- Ports 5-6 / 9-10 Entity B Inline Appliance Ports
- Ports 7-8 Entity C Inline Appliance Ports

Basic 2 Entity Configuration



- Ports 1-2
- Ports 3-4 / 7-8
- Ports 5-6 / 9-10
- Network Ports
- Entity A Inline Appliance Ports
- Entity B Inline Appliance Ports

Basic 1 Entity Configuration



- Ports 1-2
- Ports 3-4 / 5-6 / 7-8 / 9-10
- Network Ports
- Entity A Inline Appliance Ports

2. Select the Save option.

Add Entity

An entity must have at least one inline appliance port member to be considered part of the chain. Entity inline appliance port members are added as member pairs. If the ports for an entity inline appliance member are configured as packet broker ports they may not be added back to the entity until they are deleted as packet broker ports.

1. Select the up arrow in the Entities panel, 1, 2, 3, 4.
2. Select the Save option.

Remove Entity Inline Appliance Member

Entity inline appliance port members are removed as member pairs. If an entity inline appliance port member is removed, the ports may be configured as packet broker ports.

1. Entity inline appliance members may be removed by selecting the red X for the desired inline appliance port member(s).
2. Select the Save option.

Add Entity Inline Appliance Member

Entity inline appliance port members are added as member pairs. If the ports for an entity inline appliance port member are configured as packet broker ports they may not be added back to the entity until they are deleted as packet broker ports.

1. Select the up arrow in the Entities panel. The entity inline appliance members will appear.
2. Select the Save option.

Taps Settings

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

No. Of Lost HB Packets	LFP
Heartbeats per Second	Reverse Bypass
Tap Modes	Bypass Threshold
Fail Mode	

1. Select Settings.

The Configure Tap Settings panel will be displayed.

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

This is the number of heartbeats that must be lost on any inline appliance port member before any entity will remove the inline appliance from the load balance group.

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

This is the number of heartbeats per second sent on the inline appliance ports for all entities.

4. Select the Tap Mode.

Active	Allows the tap to automatically switch from inline to bypass if an issue occurs with all entities A, B, C and D inline appliance port(s), loss of link or heartbeats based on the bypass threshold value for each entity. Each entity A, B, C and D are in bypass. The network port pairs 1-2 will be connected. When the issue with any entity A, B, C or D inline appliance port(s) is resolved, have link and heartbeats, the tap will automatically switch back to inline.
--------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Figure 24 ATLB2 Chained Tap Mode (Inline)

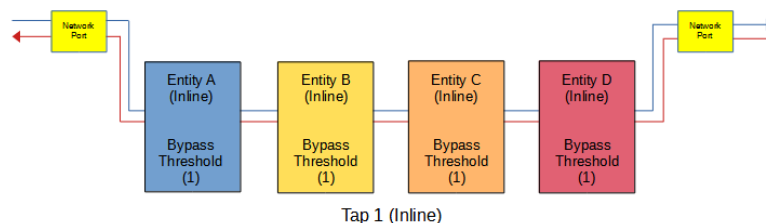
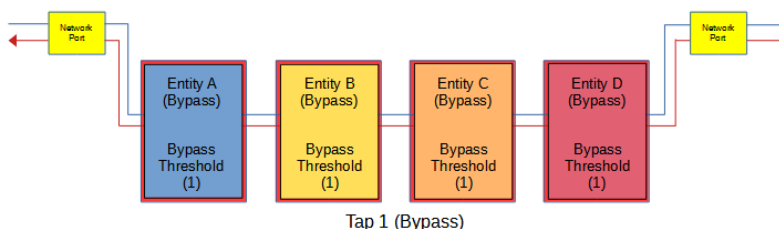
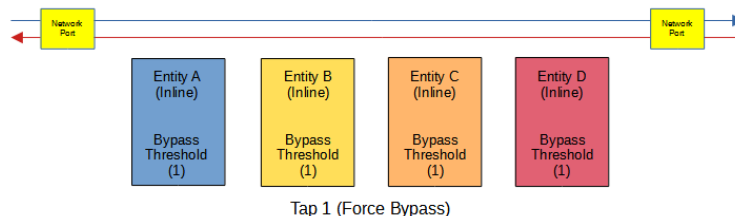


Figure 25 ATLB2 Chained Tap Mode (Bypass)



Force Bypass If selected, the tap will switch the traffic between the network port pairs 1-2 with no regard for the entity inline appliance port(s), link or heartbeats. Typically used during maintenance activities.

Figure 26 ATLB2 Chained Tap Mode (Force Bypass)



5. Select the Fail Mode.

Open If selected and power is lost to the unit. The traffic will switch between the network ports 1-2.

Closed If selected and power is lost to the unit. The traffic will go down.

6. LFP

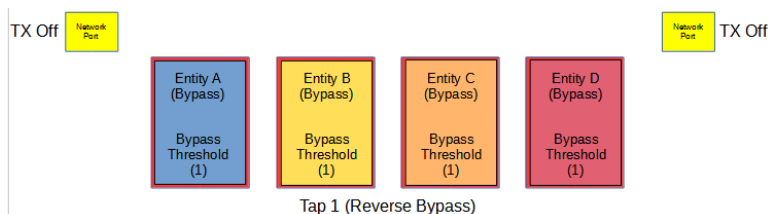
If enabled and link is lost on one of the network ports 1-2. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 27 ATLB2 Chained Tap Mode (LFP)



7. Reverse Bypass If enabled and all entities A, B, C and D are in bypass, inline appliance port(s) fail, loss of link or heartbeats based on the bypass threshold value for each entity. The TX will be disabled on all network ports 1-2. The RX on all network ports 1-2 remain on.

Figure 28 ATLB2 Chained Tap Mode (Reverse Bypass)



8. Bypass Threshold A The bypass threshold determines how many inline appliances port members may fail, loss of link or loss of heartbeats, before entity A switches to bypass.
9. Bypass Threshold B The bypass threshold determines how many inline appliances port members may fail, loss of link or loss of heartbeats, before entity B switches to bypass.
10. Bypass Threshold C The bypass threshold determines how many inline appliances port members may fail, loss of link or loss of heartbeats, before entity C switches to bypass.
11. Bypass Threshold D The bypass threshold determines how many inline appliances port members may fail, loss of link or loss of heartbeats, before entity D switches to bypass.
12. Select Accept to save updates. Save must additionally be selected on the Bypass Taps panel.
13. Select Cancel to return the Bypass Taps panel.
14. Select Add All to restore all entity inline appliance port members.
15. Select Remove Add to remove all entity inline appliance port members.
16. Select Default Mode to exit the ATLB2 Chained mode and restore the system to the Default mode.

A "Go back to default mode?" message will be displayed.

17. Select OK.

ATLB2 Chained Tap Mode GUI Indications

When the taps are placed in this mode the GUI will display various messages and colors to reflect the current conditions.

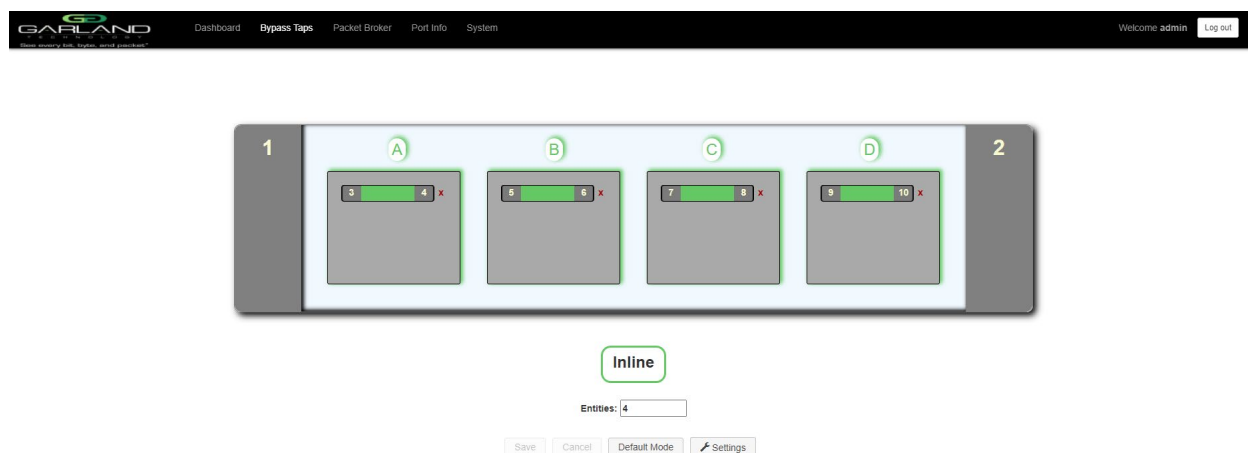
Normal

In this example the following may be determined:

1. The ATLB2 chained tap is inline.
2. Entity A's inline appliance members are normal, have links and heartbeats.
3. Entity B's inline appliance members are normal, have links and heartbeats.
4. Entity C's inline appliance members are normal, have links and heartbeats.
5. Entity D's inline appliance members are normal, have links and heartbeats.
6. The traffic per this display indicates:

Port 1 – Entity A – Entity B – Entity C – Entity D – Port 2

Port 2 – Entity D – Entity C – Entity B – Entity A – Port 1

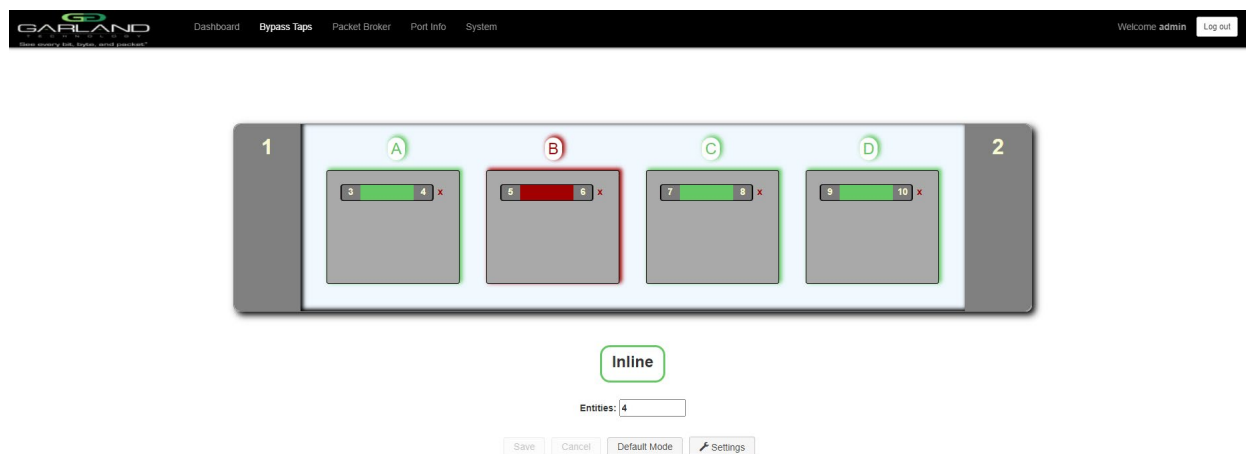


Entity Member Abnormal

In this example the following may be determined:

1. The ATLB2 chained tap is inline.
2. Entity A's inline appliance members are normal, have links and heartbeats.
3. Entity B's inline appliance members are abnormal, loss of links or heartbeats.
4. Entity C's inline appliance members are normal, have links and heartbeats.
5. Entity D's inline appliance members are normal, have links and heartbeats.
6. The traffic per this display indicates:

Port 1 – Entity A – Entity C – Entity D – Port 2
Port 2 – Entity D – Entity C – Entity A – Port 1



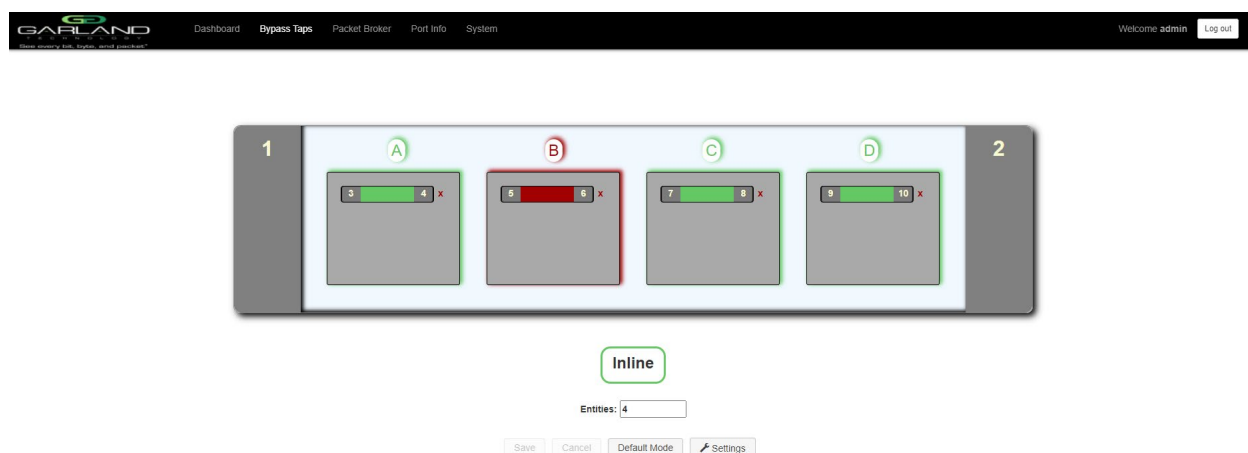
Entity Bypass

In this example the following may be determined:

1. The ATLB2 chained tap is inline.
2. Entity A's inline appliance members are normal, have links and heartbeats.
3. Entity B's inline appliance members are abnormal, loss of links or heartbeats. Entity B is bypassed.
4. Entity C's inline appliance members are normal, have links and heartbeats.
5. Entity D's inline appliance members are normal, have links and heartbeats.
6. The traffic per this display indicates:

Port 1 – Entity A – Entity C – Entity D – Port 2

Port 2 – Entity D – Entity C – Entity A – Port 1



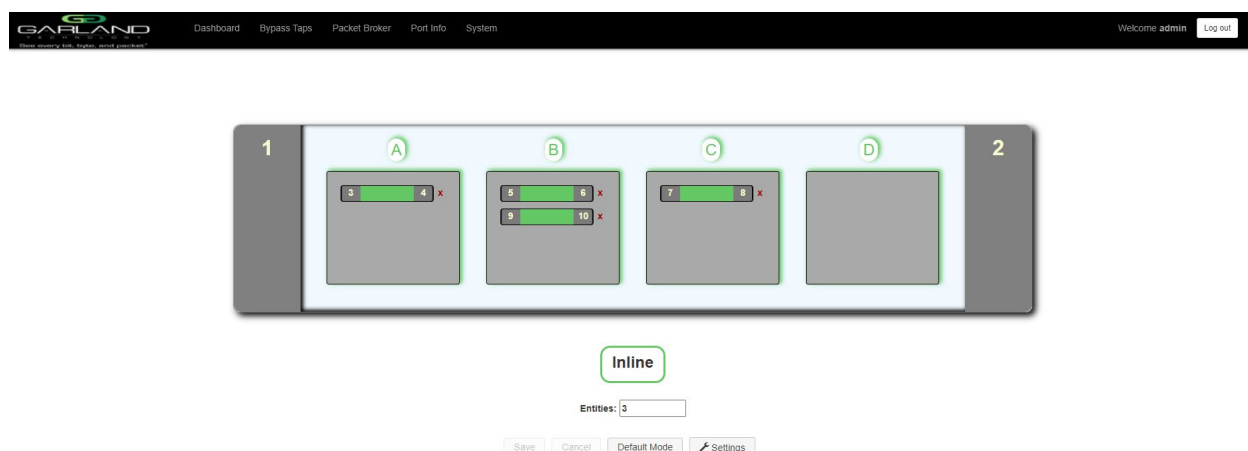
Entity Removed From Chain

In this example the following may be determined:

1. The ATLB2 chained tap is inline.
2. Entity A's inline appliance members are normal, have links and heartbeats.
3. Entity B's inline appliance members are normal, have links and heartbeats. The traffic is load balanced across both members.
4. Entity C's inline appliance members are normal, have links and heartbeats.
5. Entity D has been removed from the chain.
6. The traffic per this display indicates:

Port 1 – Entity A – Entity B – Entity C – Port 2

Port 2 – Entity C – Entity B – Entity A – Port 1

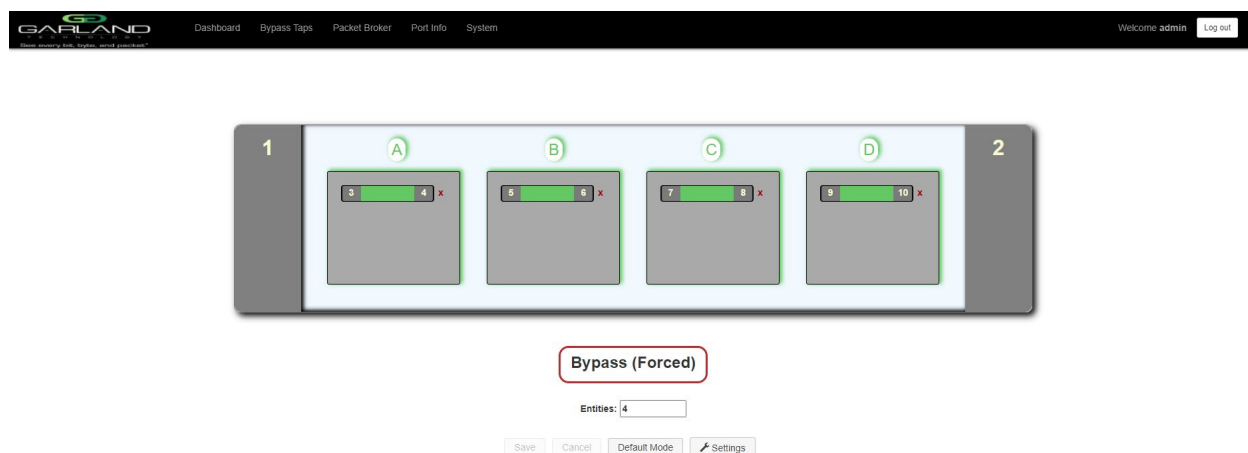


ATLB2 Chained Tap Forced Bypass

In this example the following may be determined:

1. The ATLB2 chained tap is Forced Bypass.
2. Entity A's inline appliance members are normal, have links and heartbeats.
3. Entity B's inline appliance members are normal, have links and heartbeats.
4. Entity C's inline appliance members are normal, have links and heartbeats.
5. Entity D's inline appliance members are normal, have links and heartbeats.
6. The traffic per this display indicates:

Port 1 – Port 2
Port 2 – Port 1



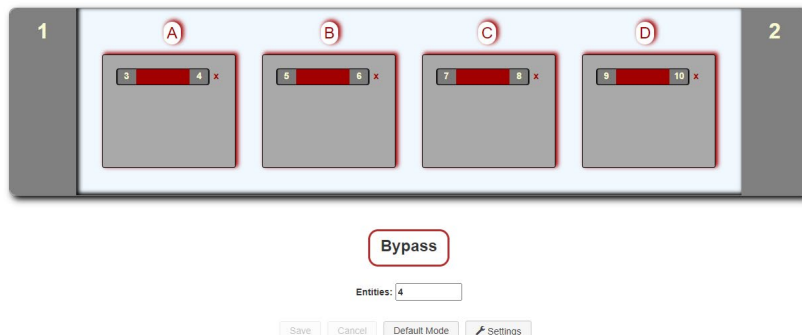
ATLB2 Chained Tap Bypass

In this example the following may be determined:

1. The ATLB2 chained tap is bypass.
2. Entity A's inline appliance members are abnormal, loss of links or loss of heartbeats.
Entity A is bypassed. Entity A's bypass threshold is 1.
3. Entity B's inline appliance members are abnormal, loss of links or loss of heartbeats.
Entity B is bypassed. Entity B's bypass threshold is 1.
4. Entity C's inline appliance members are abnormal, loss of links or loss of heartbeats.
Entity C is bypassed. Entity C's bypass threshold is 1.
5. Entity D's inline appliance members are abnormal, loss of links or loss of heartbeats.
Entity D is bypassed. Entity D's bypass threshold is 1.
6. The traffic per this display indicates:

Port 1 – Port 2

Port 2 – Port 1



4 Packet Broker

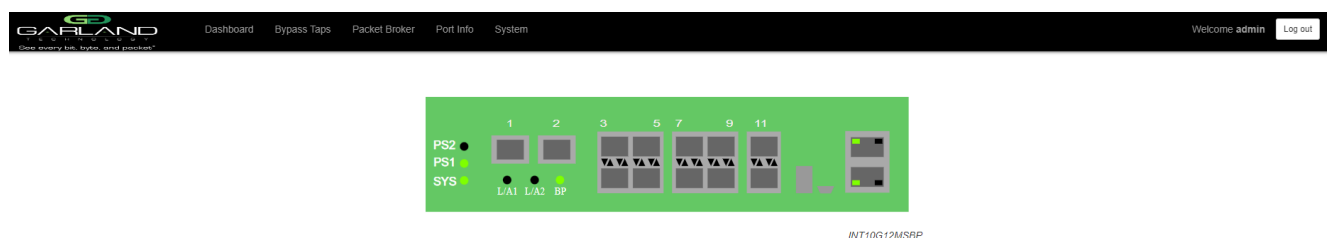
The packet broker section typically consists of ports 5 through 12. However, the available packet broker ports is determined by the following conditions:

- The tap mode selected, Default, Load Balance, Primary-Secondary or ATLB2 Chained
- If tap monitor ports are applied

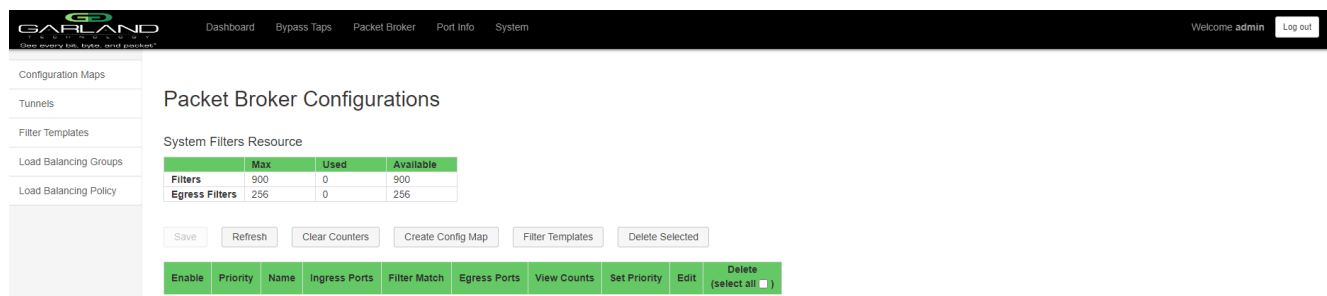
The following configuration options may be displayed, modified, enabled, or disabled under the Packet Broker panel.

Configuration Maps
Tunnels
Filter Templates

Load Balance Groups
Load Balance Policy



1. Select Packet Broker on the Dashboard menu bar.



The Packet Broker Configurations panel will be displayed.

Tunnels

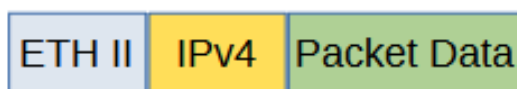
The system supports the ability to:

- Encapsulate I2GRE packets
- Decapsulate I2GRE packets

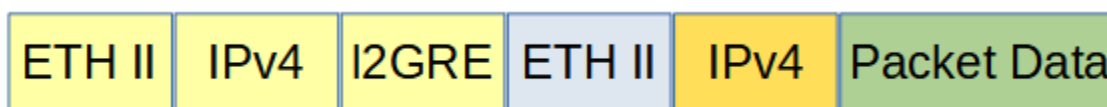
Encapsulate I2GRE Packets (GRE-TX Only)

When a packet is encapsulated with a I2GRE header the new I2GRE header segments are added to the original packet. The I2GRE header segments consists of Ethernet II, IPv4 and I2GRE as shown below.

Original Packet



I2GRE Encapsulated Packet



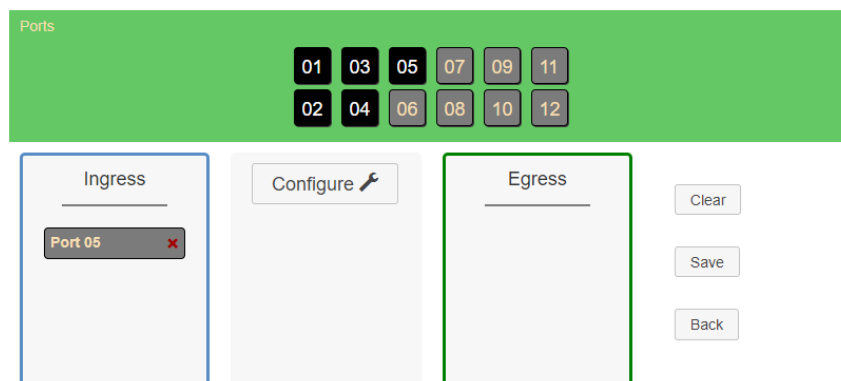
1. Select Tunnels.

The Tunnels panel will be displayed.

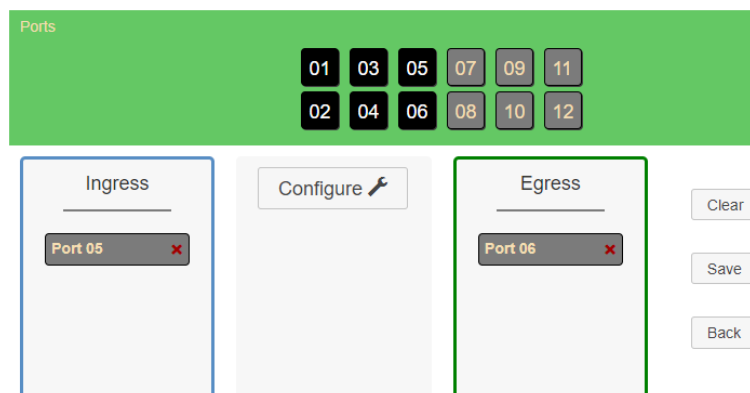
2. Select Create Tunnel.

The Create Tunnels panel will be displayed.

3. Add an ingress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Ingress panel and release.



4. 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.



5. Select Configure.

The Configure panel will be displayed.

6. Select GRE TX Only.
7. Enter the Tunnel IP Address, (I2GRE Header SIP).
8. Enter the Remote IP Address, (I2GRE Header DIP).
9. Enter the Remote MAC Address, (I2GRE Header DMAC).
10. Enter the Key, (1-16777215).

The default I2GRE Header SMAC is automatically defined by the system. There are five predefined SMACs.

11. Select Advanced to select an alternative SMAC or to manually enter the SMAC.
12. Select Advanced to add a VLAN ID, optional, (1-4095).
13. Select Set.
14. Select Cancel to disregard.
15. Select Save.

The gre-tx-only tunnel will be displayed on the Tunnels panel.

Create Tunnel

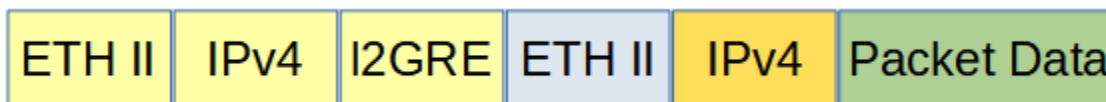
Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID
1	1234		gre-tx-only	10.10.10.10	f2:93:c5:e5:30:a7	10.10.10.25	f0:93:c5:a1:a1:a1		6	5	x

16. The tunnel may be deleted by selecting the red X.

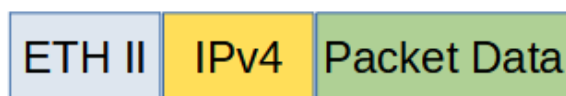
Decapsulate I2GRE Packets (GRE-RX Only)

When a I2GRE packet is decapsulated the I2GRE header segments are removed from the packet.

I2GRE Encapsulated Packet



I2GRE Decapsulated Packet



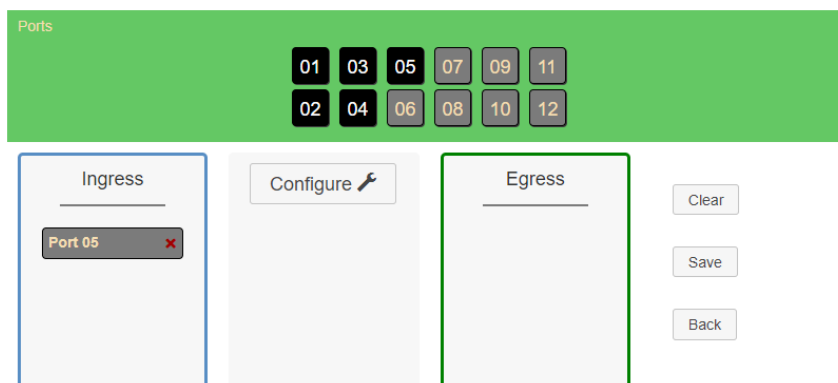
1. Select Tunnels.

The Tunnels panel will be displayed.

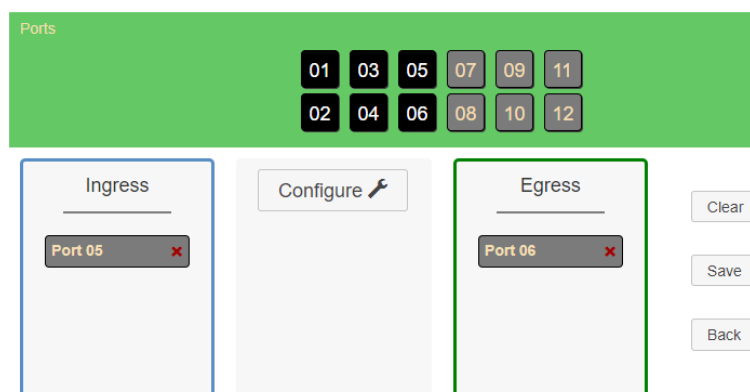
2. Select Create Tunnel.

The Create Tunnels panel will be displayed.

3. Add an ingress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Ingress panel and release.



4. 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.



5. Select Configure.

The Configure panel will be displayed.

6. Select GRE RX Only.
7. Enter the Tunnel IP Address, (I2GRE Header DIP).
8. Enter the Remote IP Address, (I2GRE Header SIP).
9. Enter the Key, (1-16777215).

The default I2GRE Header SMAC is automatically defined by the system. There are five predefined SMACs.

10. Select Advanced to select an alternative DMAC or to manually enter the DMAC, (I2GRE Header DMAC).
11. Select Advanced to add a VLAN ID, optional, (1-4095).
12. Select Set.
13. Select Cancel to disregard.
14. Select Save.

The gre-rx-only tunnel will be displayed on the Tunnels panel.

Create Tunnel

Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID	
1	2345		gre-rx-only	20.20.20.20	f2:93:c5:e5:30:a7	20.20.20.25			6	5		X

15. The tunnel may be deleted by selecting the red X.

Filter Template

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

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

The Filter Templates panel will be displayed.

2. Select Create Template.

The Create New Filter Template panel will be displayed.

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

4. Enter the description, optional.

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

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

Source MAC Address / Source MAC Mask	
Destination MAC Address / Destination MAC Mask	
Ether Type	
Source IPv4 Address / Source IP Mask	
Destination IPv4 Address / Destination IP Mask	
Source IPv6 Address / Source IP Mask	<i>IPv6 is not supported for this model</i>
Destination IPv6 Address / Destination IP Mask	<i>IPv6 is not supported for this model</i>
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.

Load Balancing Group

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

1. Select Load Balancing Groups.

The Load Balancing Groups panel will be displayed.

2. Select Create Group.

The Create New Load Balance Group panel will be displayed.

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

4. Enter the description, optional.

5. Add ports by placing the cursor on the desired port. Select 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.

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

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

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

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

Load Balancing Policy

The load balancing policy determines the hashing applied to all load balancing groups, taps in the load balance mode and the ATLB2 chained mode. The load balancing policy options are as follows:

IPv4 Source	L4 Source Port
IPv4 Destination	L4 Destination Port
IPv6 Source	MAC Source
IPv6 Destination	MAC Destination

1. Select Load Balancing Policy.

The Load Balancing Policy panel will be displayed.

2. Select or deselect the desired load balancing policy options.
3. Select Save to save updates.
4. Select Cancel to disregard changes.

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.

The screenshot displays the 'Create Config Map' panel in the Garland Technology Packet Broker interface. The panel includes a sidebar with navigation links: Configuration Maps, Tunnels, Filter Templates, Load Balancing Groups, and Load Balancing Policy. The main content area features a 'Back To Map List' button, input fields for 'Name' and 'Description', and status indicators for 'Available Filters: 900/900' and 'Available Egress Filters: 256/256'. A 'Ports' section shows a grid of 12 ports (01-12) with some shaded gray and others black. Below this are sections for 'Load Balancing Groups' and 'Filter Templates', each with a 'New' button. At the bottom, a diagram illustrates the flow from 'Ingress' to 'Filter' to 'Egress' components, with 'Clear Map', 'Save', and 'Reset' buttons to the right.

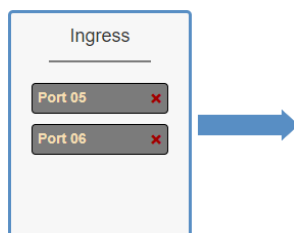
3. Select the Name pencil icon to apply a name, optional. If no name is entered the system will automatically apply a name to the config maps as follows, map, map(1), map(2) etc.
4. Place the cursor in the Name panel and enter the name.

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

Figure 1 Ingress



2. Remove a port by selecting the red X.

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 2 Filter

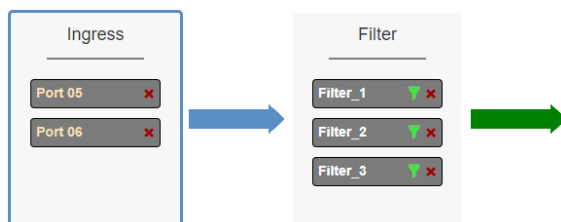
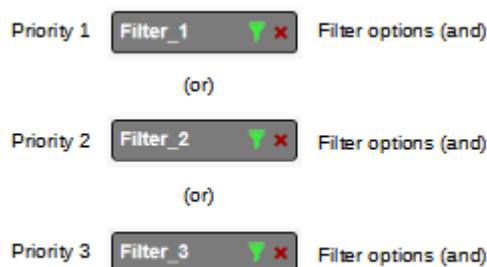


Figure 3 Filter System Considerations



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

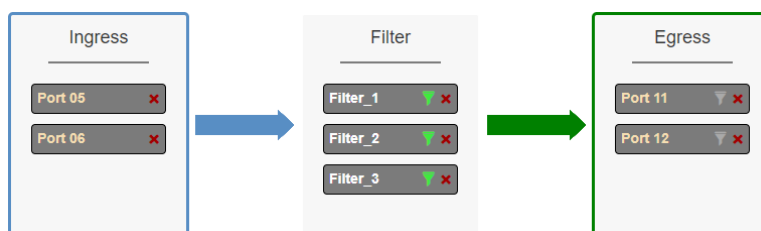
The Edit Filter panel will be displayed. Any option modification made will not change the original template. It is advisable to rename a filter if the original filter template options were modified.

3. Enter the filter name, optional. If no name is entered the system will automatically apply a name to the filter as follows, iFilt, iFilt(2), iFilt(3) etc.
4. Select Accept once all desired options have been modified.
5. Remove a Filter Template by selecting the Red X.

Egress

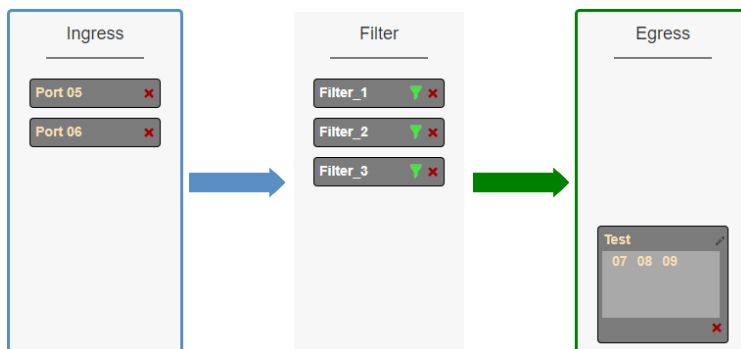
1. Add an egress port by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Egress panel and release. Repeat for all desired ports. If multiple ports are added, then 100% of the traffic will be sent to each port.

Figure 4 Egress Port(s)



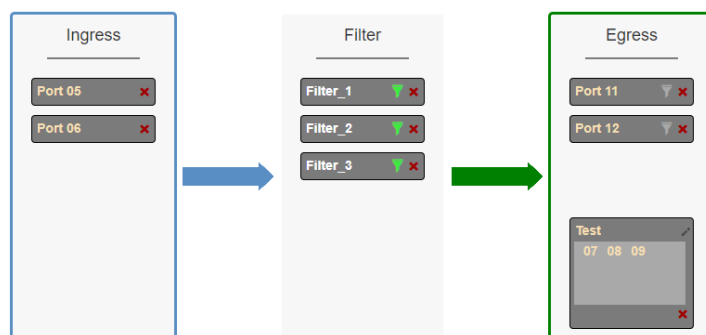
2. Add a load balancing group by placing the cursor on a previously created load balancing group or new load balancing group. Select the left mouse button. Drag the load balancing group to the Egress panel and release. Ports may be added or removed from any load balancing group. If ports are added or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

Figure 5 Egress Load Balancing Group



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

Figure 6 Egress Load Balancing Group and Port(s)

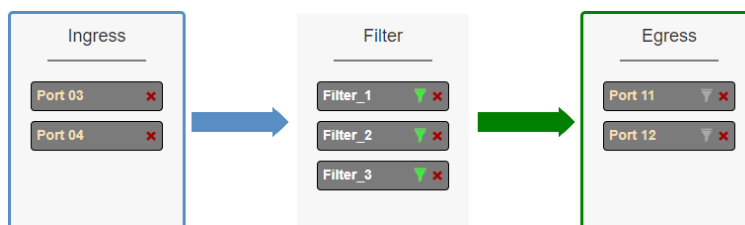


4. Remove a port or load balancing group by selecting the Red X.

Egress Filter

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

Figure 7 Egress Filter



The Port XX Egress Filters panel will be displayed.

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

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

Figure 8 Port XX Egress Filters

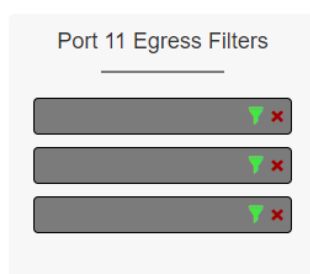
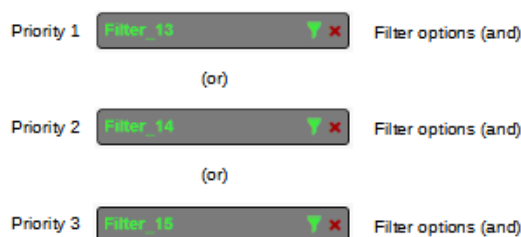


Figure 9 Egress Filter System Considerations



3. If new is selected, the Edit Filter panel will be displayed.
4. Enter the filter name, optional. If no name is entered the system will automatically apply a name to the egress filter as follows, eFitPXX, eFitPXX(2), eFitPXX(3) etc.
5. Select Accept.
6. Select Cancel to disregard.
7. Remove a filter template 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.

2. Select Cancel to disregard.

Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	900	1	899
Egress Filters	256	2	254

Buttons: Save, Refresh, Clear Counters, Create Config Map, Filter Templates, Delete Selected

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all)
<input checked="" type="checkbox"/>	1	map	05 06	NaN	11 12		^ v Set		<input type="checkbox"/>

Modify a Config Map

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

Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	900	1	899
Egress Filters	256	0	256

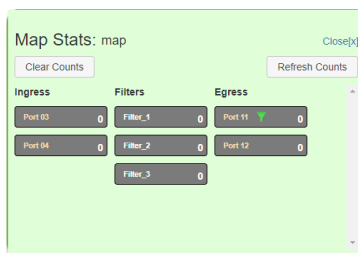
Buttons: Save, Refresh, Clear Counters, Create Config Map, Filter Templates, Delete Selected

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all)
<input checked="" type="checkbox"/>	1	map	05 06	0	11 12		^ v Set		<input type="checkbox"/>

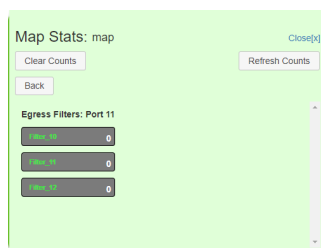
Config Map Statistics

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.

Delete Config Map

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

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all)
<input checked="" type="checkbox"/>	1	map	05 06	0	11 12		^ v Set		<input type="checkbox"/>

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 options, i.e., different port(s) or load balancing groups. In this case, the config map with the highest priority will be considered first. In the following example there are three

config maps with ingress port 5. 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 9 Config Map System Considerations

Priority 1	✓	1	Traffic_A	03	0	04	1	^ v Set	✎	<input type="checkbox"/>	Config Map options (and)
(or)											
Priority 2	✓	2	Traffic_B	03	0	05	1	^ v Set	✎	<input type="checkbox"/>	Config Map options (and)
(or)											
Priority 3	✓	3	Traffic_C	03	0	06	1	^ v Set	✎	<input type="checkbox"/>	Config Map options (and)

Method 1

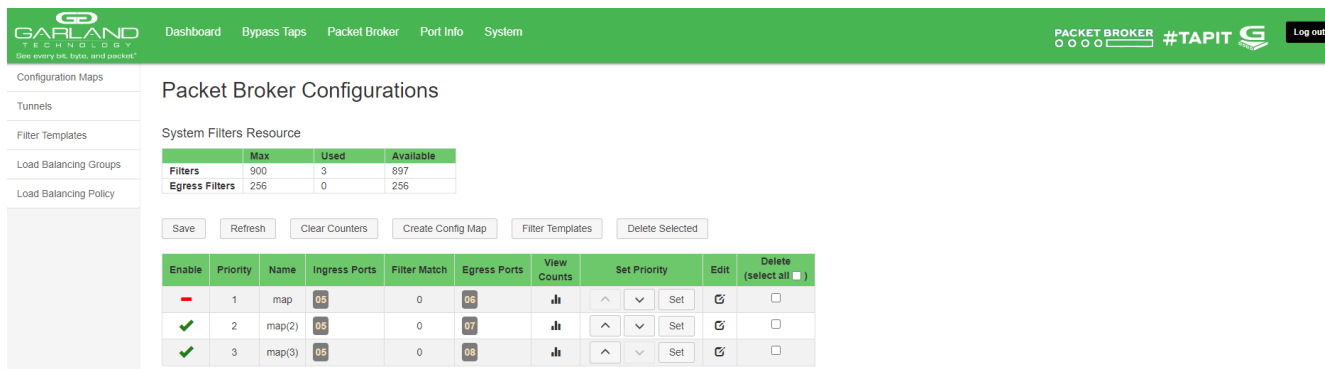
1. Select the up or down arrow for the config map.
2. Select Save to save updates.

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.



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	900	3	897
Egress Filters	256	0	256

Save Refresh Clear Counters Create Config Map Filter Templates Delete Selected

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all)
—	1	map	06	0	06	1	^ v Set	✎	<input type="checkbox"/>
✓	2	map(2)	06	0	07	1	^ v Set	✎	<input type="checkbox"/>
✓	3	map(3)	06	0	08	1	^ v Set	✎	<input type="checkbox"/>

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.

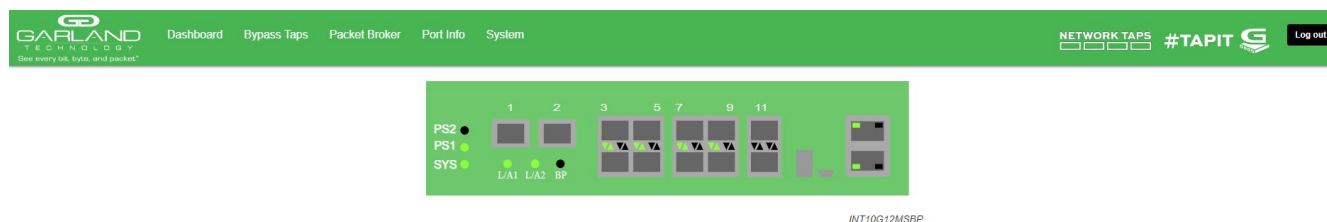
The red dash will change to a green check.

2. Select Save.

4. Port Info

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

Port Number	Mode
Port Description	SFP Data
Link	VLAN Tag
Set Speed	VLAN Strip
Speed	Port Statistics



1. Select Port Info on the Dashboard menu bar.

Port	Description	Link	Set Speed	Speed	Mode	SFP Data	VLAN Tag	VLAN Strip	Split
1	description	●	10G	10G	Normal	FINISAR CORP FTLX8574D38CV			
2	description	●	10G	10G	Normal	FINISAR CORP FTLX8574D38CV			
3	description	●	10G	10G	Normal	GARLAND TECH SFP+SR			
4	description	●	10G	10G	Normal	GARLAND TECH SFP+SR			
5	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	
6	description	●	10G	10G	Normal	OEM GL-10GSFP-SR	<input type="checkbox"/>	<input type="checkbox"/>	
7	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	
8	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	
9	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	
10	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	
11	description	●	10G	10G	Normal	OEM GL-10GSFP-SR	<input type="checkbox"/>	<input type="checkbox"/>	
12	description	●	10G	10G	Normal	GARLAND TECH SFP+SR	<input type="checkbox"/>	<input type="checkbox"/>	

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.

VLAN Tag

VLAN tag applies a VLAN ID to the packets when the port is configured as an ingress port on a config map. This option is only available for packet brokers ports. The packet broker section consists of ports 1 through 12.

1. Select the VLAN Tag enable option for the desired port.

2. Enter the desired VLAN ID, (1-4094).
3. Select Save.
4. Disable by deselecting the VLAN Tag option for the desired port.
5. Select Save.

VLAN Strip

VLAN strip removes the outer VLAN ID for packets when the port is configured as an egress port on a config map. This option is only available for packet brokers ports. The packet broker section consists of ports 1 through 12.

1. Select the VLAN Strip option for the desired port.
2. Select Save.
3. Disable by deselecting the VLAN Strip option for the desired port.
4. Select Save.