GARLAND TECHNOLOGY

See every bit, byte, and packet®

User Guide

INT10G12MSBP / INT10G12SSBP

12/2022

Release Version: 4.22.1

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 (click topic to go directly to the page)

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.

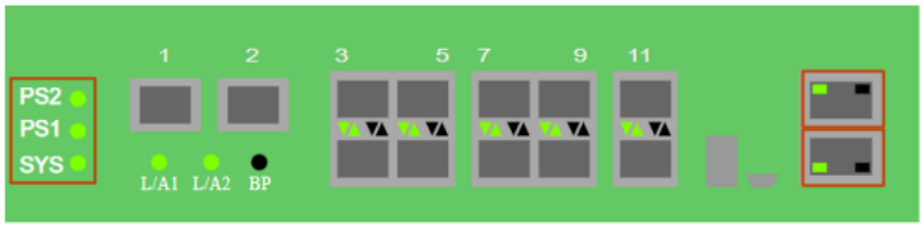
The dashboard provides access to the Packet Broker, Port Info and System configuration options by selecting the desired option in the top menu bar. These options are covered in detail per their specific sections.

INT10G12MSBP

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

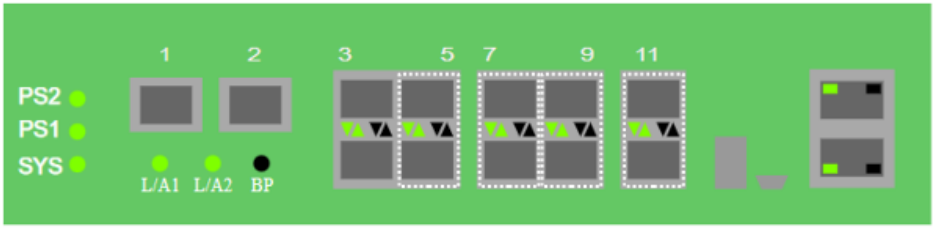
PS2	Power Supply 2 LED
PS1	Power Supply 1 LED
SYS	System LED
Ethernet Interface	Upper Left LED (always illuminated)
Serial Interface	Lower Left LED (always illuminated)

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

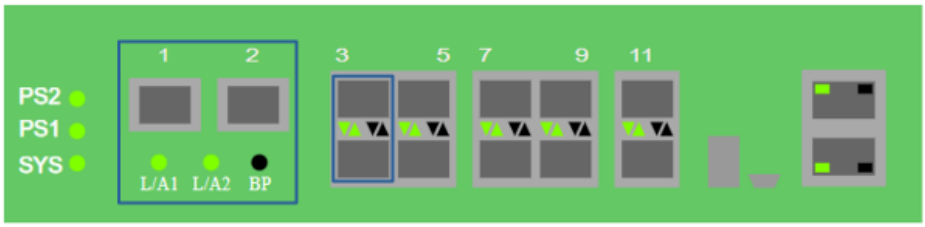
Port 3 Left Up Arrow	Link LED
Port 4 Left Down Arrow	Link LED
Port 5 Left Up Arrow	Link LED
Port 6 Left Down Arrow	Link LED
Port 7 Left Up Arrow	Link LED
Port 8 Left Down Arrow	Link LED
Port 9 Left Up Arrow	Link LED
Port 10 Left Down Arrow	Link LED
Port 11 Left Up Arrow	Link LED
Port 12 Left Down Arrow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

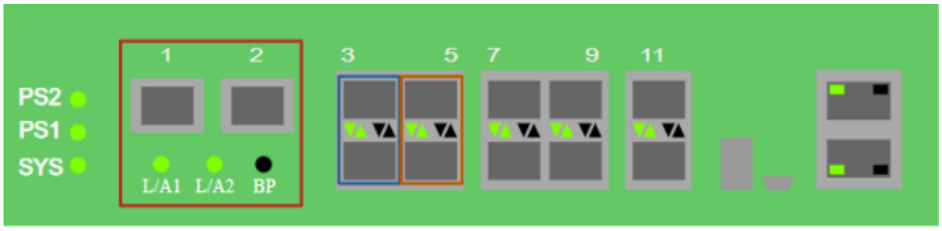
L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	Tap 1 Bypass LED
Port 3 Left Up Arrow	Tap 1 Inline Appliance Link LED
Port 4 Left Down Arrow	Tap 1 Inline Appliance Link LED

** 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

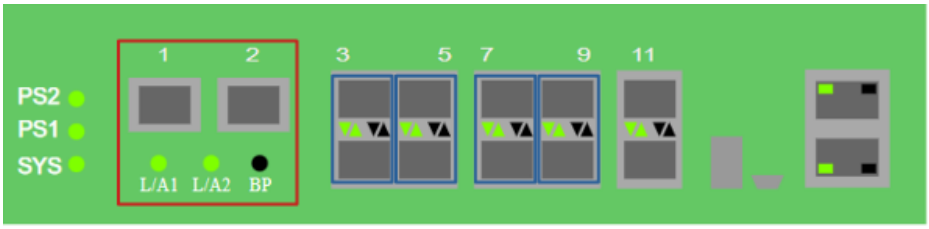
L/A1	Tap 1 Network Port 1 Link/Activity LED
L/A2	Tap 1 Network Port 2 Link/Activity LED
BP	Tap 1 Bypass LED
Port 3 Left Up Arrow	Tap 1 Primary Inline Appliance Link LED
Port 4 Left Down Arrow	Tap 1 Primary Inline Appliance Link LED
Port X Left Up Arrow	Tap 1 Secondary Inline Appliance Link LED
Port X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

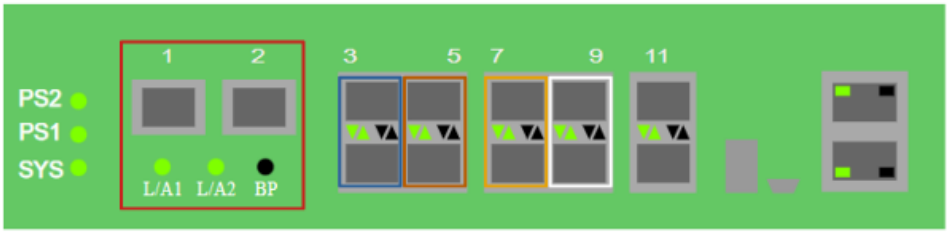
ATLB2 Chained Tap Mode

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

INT10G12MSBP

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 displayed.

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.
3. Enter the Password.
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. Select Save to save updates.

5. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

   The TACACS Test panel will appear.

2. Select Primary.

3. Enter the Username.

4. Enter the Password.

5. Select Test.

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

TACACS Ping Test

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

1. Select TACACS 1 Ping.

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

TACACS Secondary Authentication

1. Select Enable Secondary.

   The TACACS Secondary panel will be displayed.

2. Enter the IP Address, IPv4 or IPv6.

3. Enter the Secret Word, (optional).

4. Select Save to save updates.

5. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

   The TACACS Test panel will appear.

2. Select Secondary.

3. Enter the Username.

4. Enter the Password.

5. Select Test.

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

TACACS Ping Test

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

1. Select TACACS 2 Ping.

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

Network Settings

Upon the initial turn up via the serial interface the IPv4 address, IPv4 gateway, IPv6 address and IPv6 gateway may have been already established. The IPv4 and IPv6 management interfaces may be enabled or disabled independently as well as both enabled or disabled simultaneously. If the IPv4 and IPv6 management interfaces are disabled simultaneously, access is only allowed via the serial interface. Any modifications made to any setting option will cause GUI disruption for about 60 seconds.

Also note that modifying the management interfaces may cause network disruption if prior consideration and planning have not been performed.

The default system network configurations are as follows:

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

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

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

1. Select Network Settings.

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

IPv4 / Disable

1. Deselect Enable IPv4.

2. Select Save.

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

3. Select OK.

IPv4 Enable

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

IPv6 Enable

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

IPv6 Disable

1. Deselect Enable IPv6.
2. Select Save.

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

3. Select OK.

Add SSL Certificate

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

1. Select Add SSL Certificate.

The Select Certificate and Select Key File panel will appear.

2. Select Choose File for Select Certificate.
3. Select the desired cert.pem file.
4. Select Open.

5. Select the Choose File for Select Key File.

6. Select the desired key.pem file.

7. Select Open.

8. Select Upload.

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

9. Verify SSL Certificate Loaded "true".

10. Verify Using Uploaded SSL Certificate "true".

Disable Using Uploaded SSL Certificate

1. Select Edit Settings.

2. Deselect Using Uploaded SSL Certificate.

3. Select Save.

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

4. Refresh Browser.

5. Verify SSL Certificate Loaded "true".

6. Verify Using Uploaded SSL Certificate "false".

Date & Time

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

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

1. Select Date & Time.

The Date & Time Settings panel will be displayed.

Timezone

1. Select Edit Settings.

2. Select the desired Timezone using the pull down panel.

3. Select Save.

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

UTC

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

Manually Set Date & Time

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

NTP No Authentication (Symmetric)

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

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

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

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

NTP Authentication (Symmetric)

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

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

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

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

Syslog

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

1. Select Syslog.

   The Syslog Configuration panel will be displayed.

2. Select Edit Settings.

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

Syslog Test

1. Select Syslog Test.

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

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

SNMP

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

The following SNMP configuration options are supported:

V2 Read/Write
V2 Read Only
V3 Auth Type MD5 / SHA
V3 Priv ProtocolDES / 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.

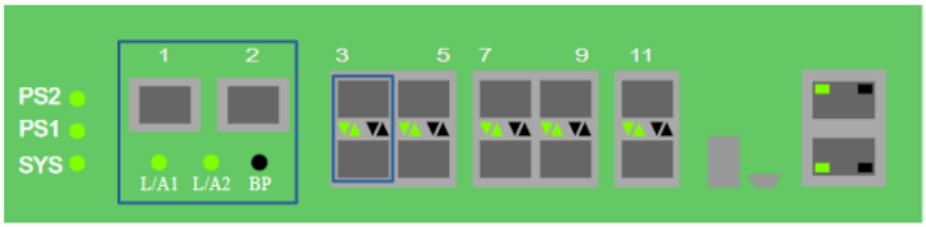
Default Tap Mode
Primary-Secondary Tap Mode
Load Balance Tap Mode
ATLB2 Chained Tap Mode

1. Select Bypass Taps on the Dashboard Menu bar.

The Bypass Taps panel will be displayed.

Default Tap Mode

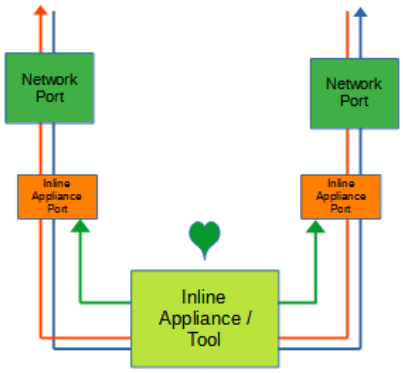
In this mode, the network ports and inline appliance ports are defined by the system. Ports 5 through 12 may be configured as packet broker ports or tap monitor ports. The network ports are typically connected to network devices such as a server or router. The inline appliance ports are typically connected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

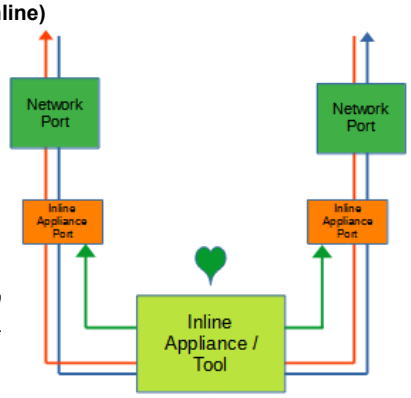
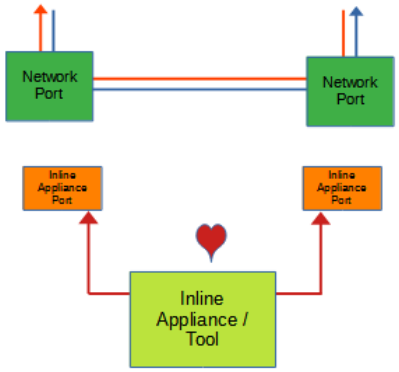
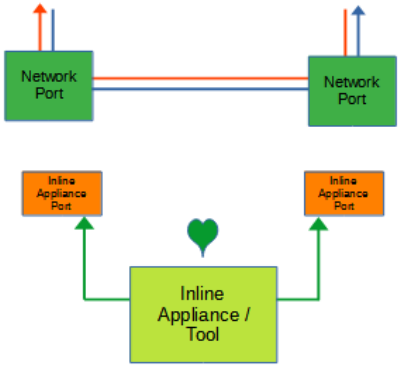


Figure 3 Default Tap Mode (Bypass)



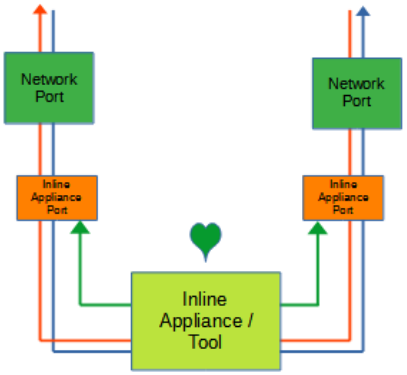
Force Bypass If selected, the tap will switch the traffic between the network ports with no regard for the inline appliance port(s), link or heartbeats. Typically used during maintenance activities.

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)

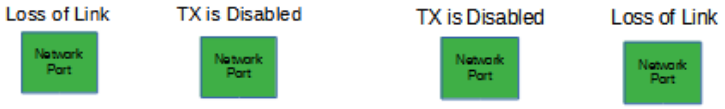


4. Select the Fail Mode.

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.

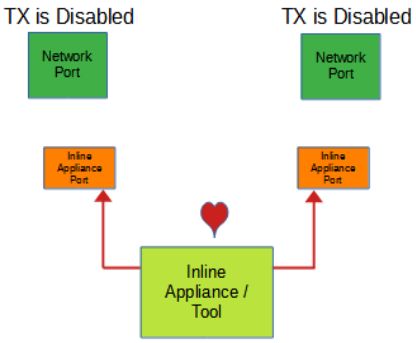
5. LFP — If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

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 of the 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.

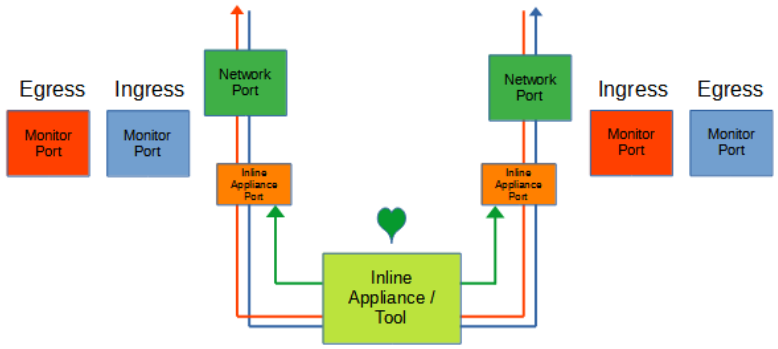
8. Select Cancel to return the Bypass Taps panel.

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 monotor ports may be added to monitor the ingress traffic or egress traffic.

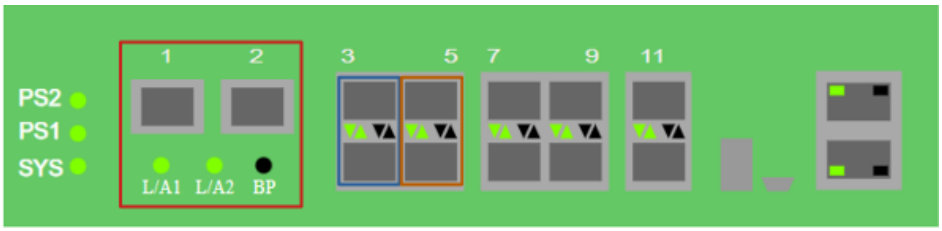
1. Create a monitor port by placing the curser on the desired port, shaded gray above the tap. Press the left mouse button and hold to select the port. Drag the port to the desired network port. The default of any monitor port is ingress. Change the monitor port traffic by placing the curser on the ingress 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

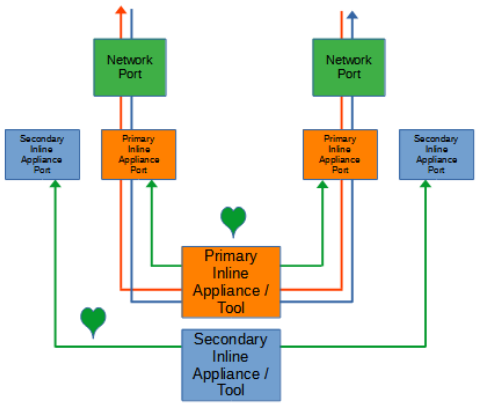
In this mode, the network, primary inline appliance and secondary inline appliance ports are defined by the system. The network ports are typically connected to network devices such as a server or router. The primary inline appliance ports are typically connected to a primary inline appliance or tool 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 with 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
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 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)

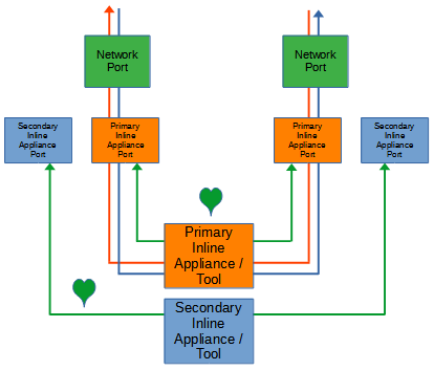


Figure 11 Primary-Secondary Tap Mode (Secondary Inline)

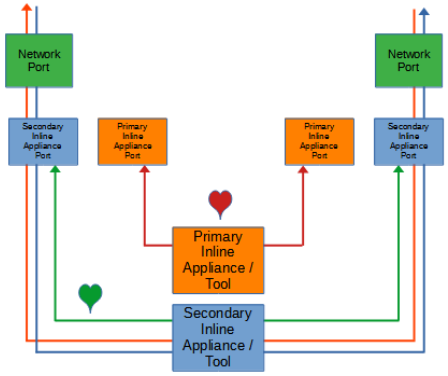
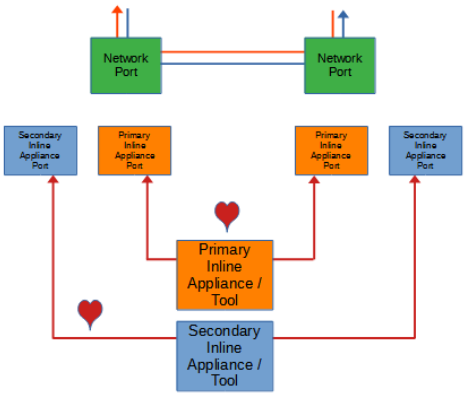
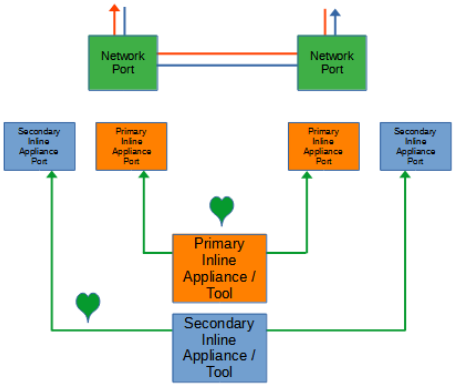


Figure 12 Primary-Secondary Tap Mode (Bypass)



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)

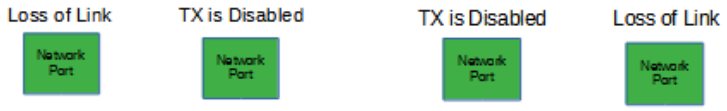


4. Select the Fail Mode.

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.

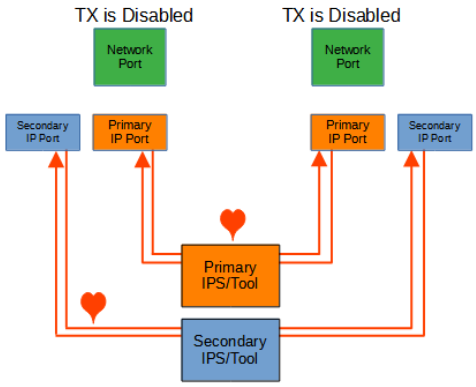
5. LFP — If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

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 back 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

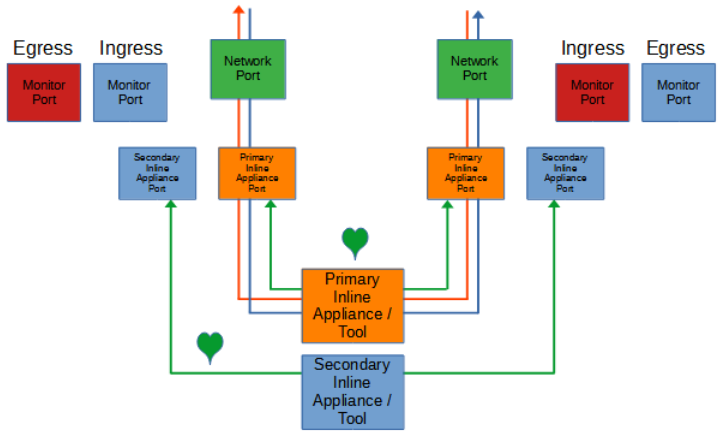
Monitor ports may be added to any tap. Each tap may have up to two monitor ports per network port, total of four monitor ports per tap. The monotor ports may be added to monitor the ingress traffic or egress traffic.

1. Create a monitor port by placing the curser 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 curser 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.

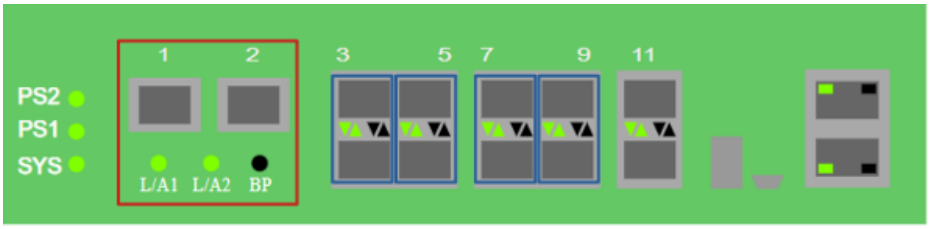
3. Select Cancel to return the Bypass Taps panel.

Figure 16 Primary-Secondary Tap Mode (Monitor Port)



Load Balance Tap Mode

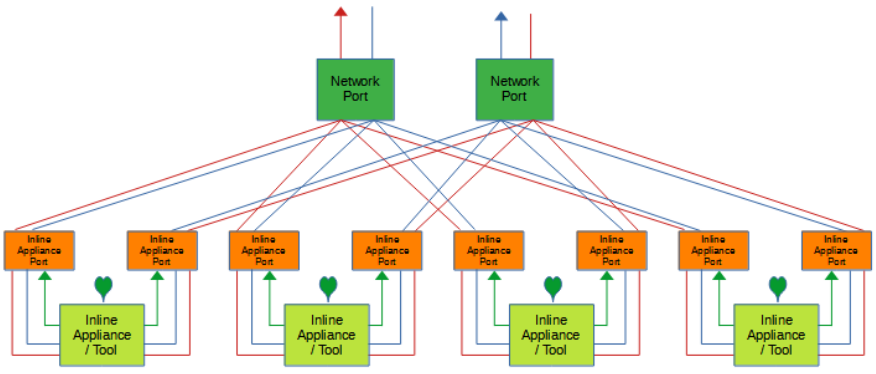
In this mode, the network and inline appliance ports are defined by the system. The tap may have up to three additional inline appliance ports applied, total 4. Any port that is not assigned as an inline appliance port may be configured as packet broker port. The network ports are typically connected 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 with 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
Fail Mode
LFP
Reverse Bypass
Bypass Threshold

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)

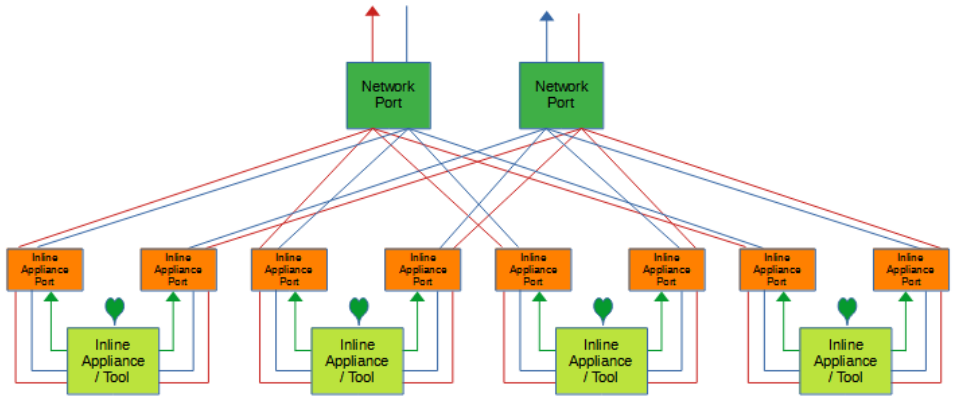
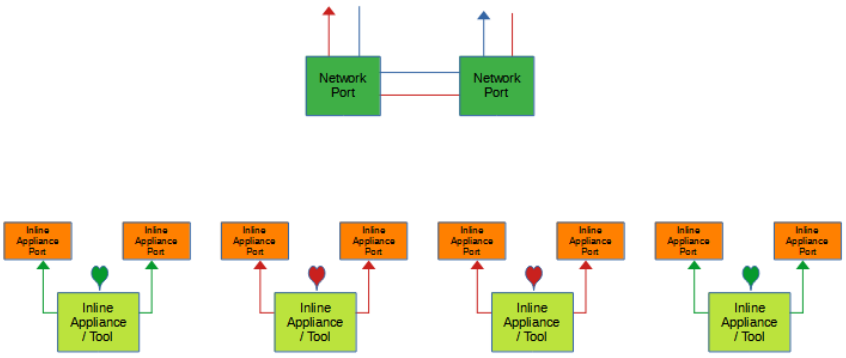
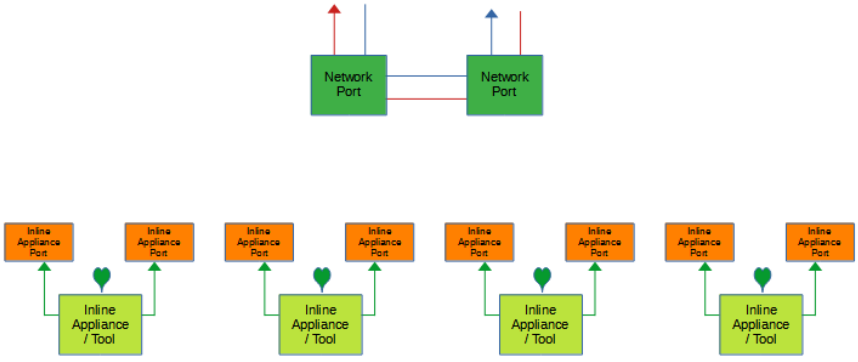


Figure 19 Load Balance Tap Mode (Bypass, Bypass Threshold=2)



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)



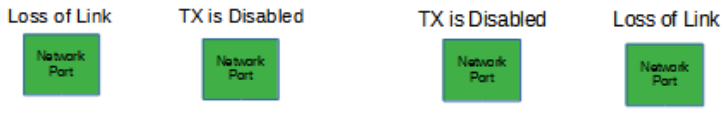
4. Select the Fail Mode.

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.

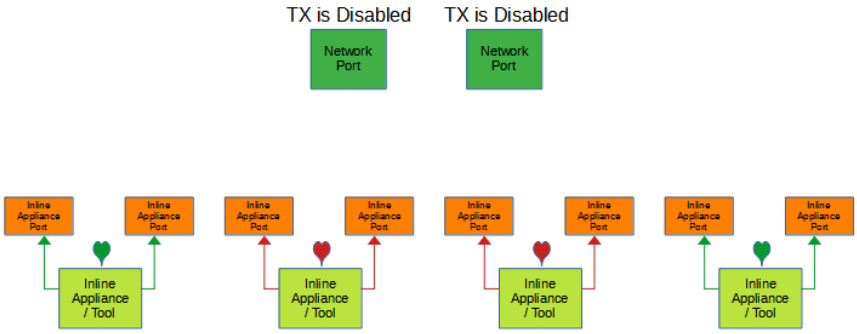
5. LFP — If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

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 appliance 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.

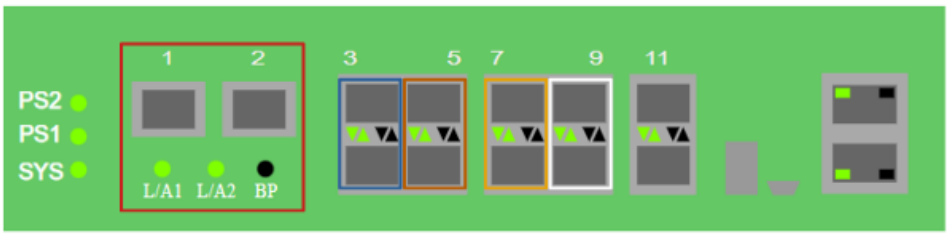
9. Select Cancel to return the Bypass Taps panel.

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.



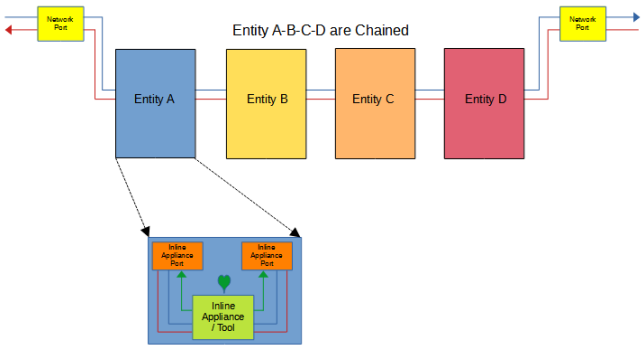
Tap 1

Port 1 (Network)
Port 2 (Network)

Entity A **Entity B** **Entity C** **Entity D**

Port 3 (Inline Appliance)	Port 5 (Inline Appliance)	Port 7 (Inline Appliance)	Port 9 (Inline Appliance)
Port 4 (Inline Appliance)	Port 6 (Inline Appliance)	Port 8 (Inline Appliance)	Port 10 (Inline Appliance)

Figure 23 ATLB2 Chained Tap Mode



Entity A-B-C-D Load Balance Ports

Configure ATLB2 Chained Tap Mode

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

   The Configure Tap Settings panel will be displayed.

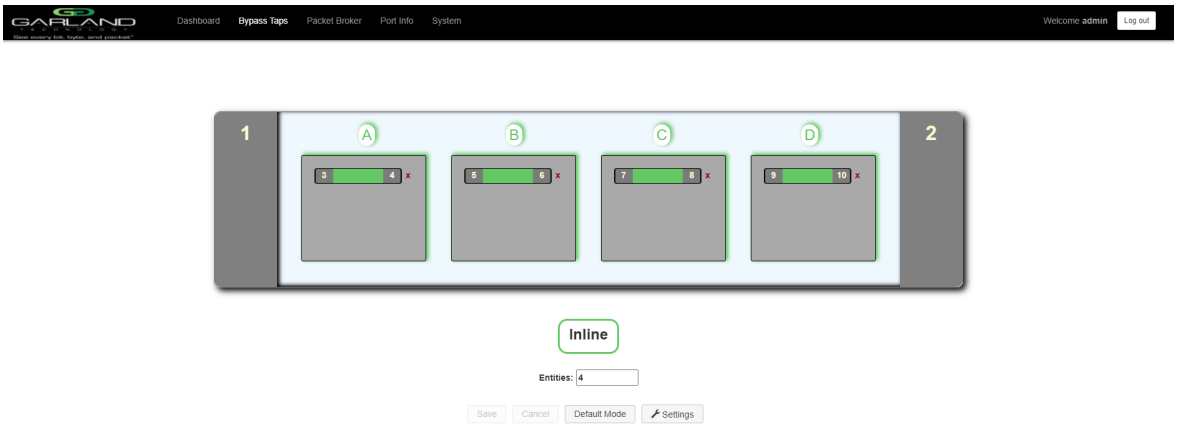
2. Select the ATLB2 Chained Mode option.

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 of 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

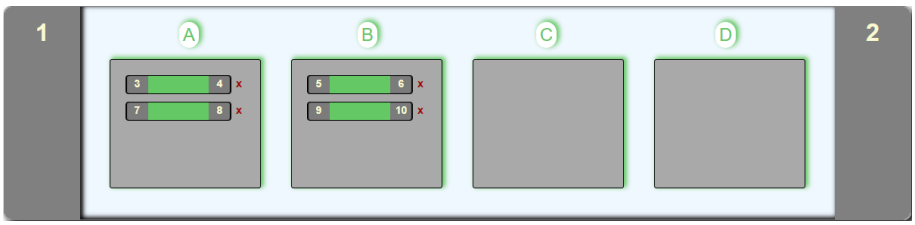
- Ports 1-2 Network Ports
- Ports 3-4 Entity A Inline Appliance Ports
- Ports 5-6 Entity B Inline Appliance Ports
- Ports 7-8 Entity C Inline Appliance Ports
- Ports 9-10 Entity D Inline Appliance Ports

Basic 3 Entity Configuration

- Ports 1-2 Network Ports

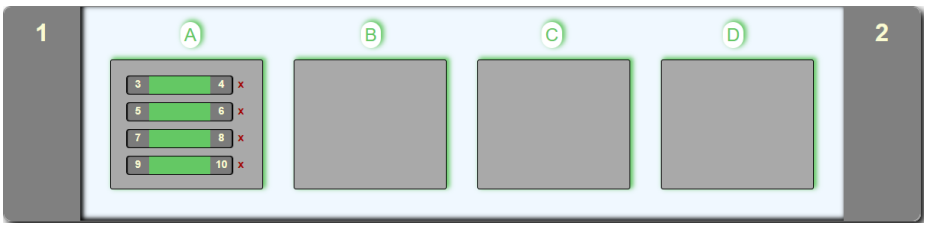
- Ports 3-4 Entity A Inline Appliance Ports
- Ports 5-6 / 9-10 Entity B Inline Appliance Ports
- Ports 7-8 Entity C Inline Appliance Ports

Basic 2 Entity Configuration



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

Basic 1 Entity Configuration



- Ports 1-2 Network Ports
- Ports 3-4 / 5-6 / 7-8 / 9-10 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 together. 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)

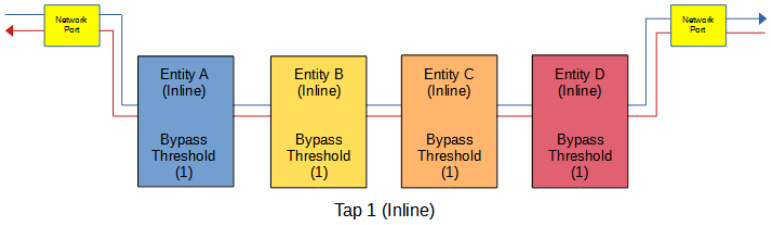
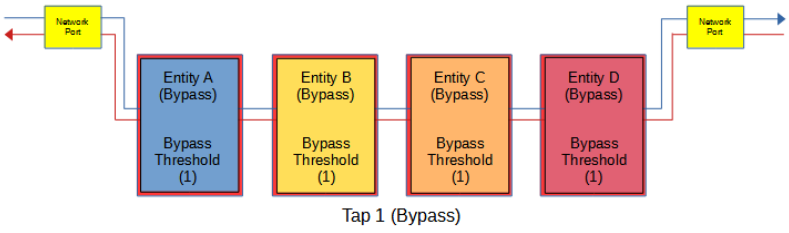
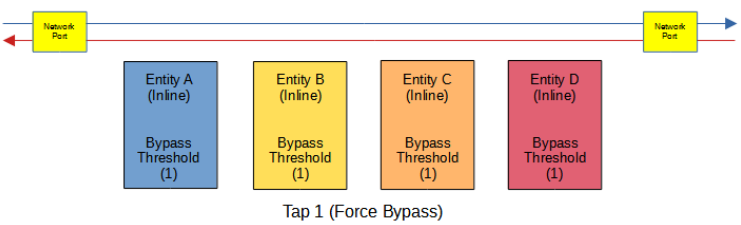


Figure 25 ATLB2 Chained Tap Mode (Bypass)



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.

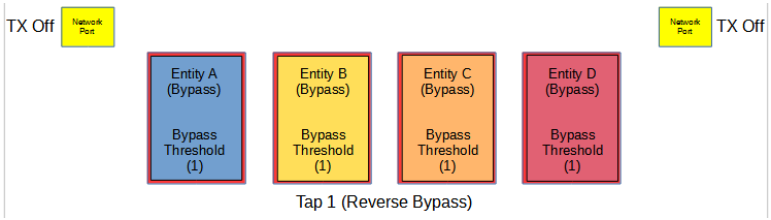
Open	If selected and power is lost to the unit. The traffic will switch between the network ports 1-2.
Closed	If selected and power is lost to the unit. The traffic will go down.

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 appliance 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 appliance 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 appliance 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 appliance 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 link and heartbeats.
3. Entity B's inline appliance members are normal, have link and heartbeats.
4. Entity C's inline appliance members are normal, have link and heartbeats.
5. Entity D's inline appliance members are normal, have link and heartbeats.
6. The traffic per this display indicates:

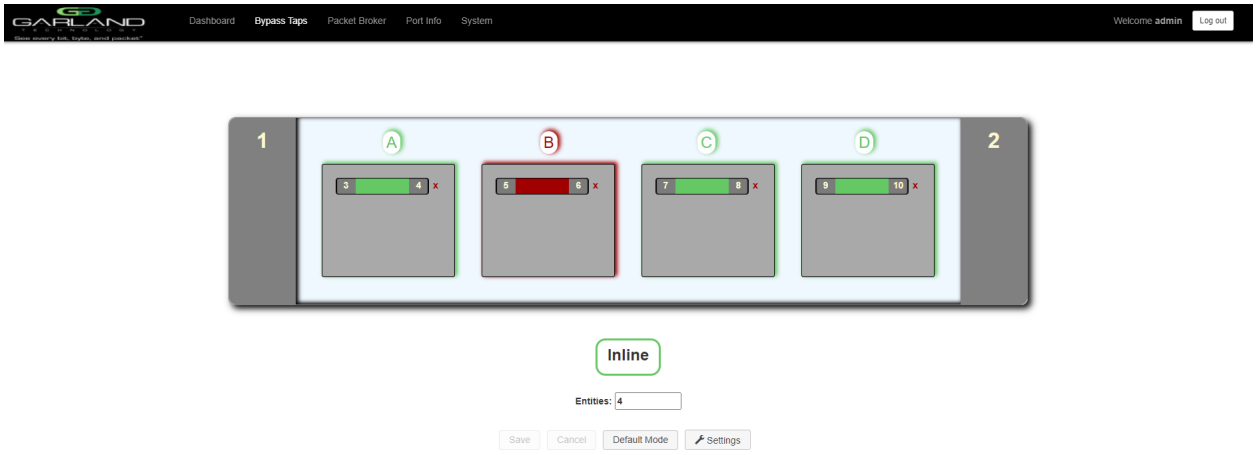
Port 1 – Entity A – Entity B – Entity C – Entity D – Port 2
Port 2 – Entity D – Entity C – Entity B – Entity A – Port 1

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, has link and heartbeats.
3. Entity B's inline appliance members are abnormal, loss of link or heartbeats.
4. Entity C's inline appliance members are normal, has link and heartbeats.
5. Entity D's inline appliance members are normal, has link 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

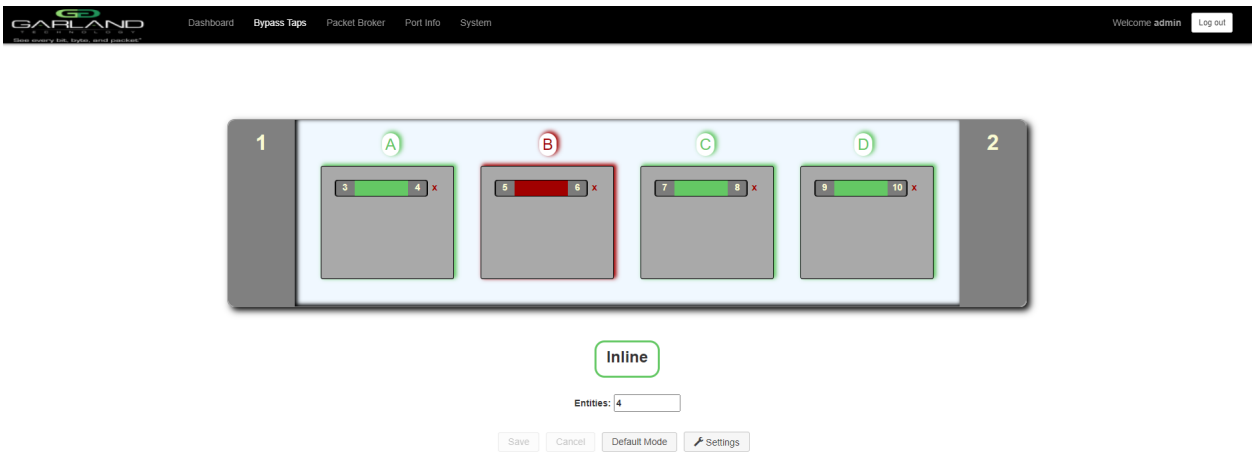


Entity Bypass

In this example the following may be determined:

1. The ATLB2 chained tap is inline.
2. Entity A's inline appliance members are normal, has link and heartbeats.
3. Entity B's inline appliance members are abnormal, loss of link or heartbeats. Entity B is bypassed.
4. Entity C's inline appliance members are normal, has link and heartbeats.
5. Entity D's inline appliance members are normal, has link 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

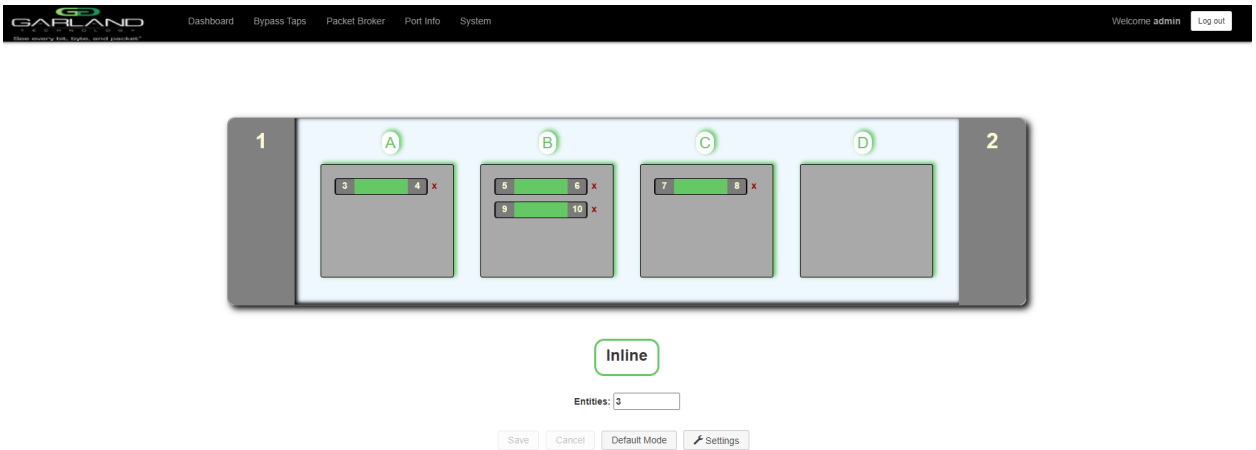


Entity Removed From Chain

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 link and heartbeats.
3. Entity B's inline appliance members are normal, have link and heartbeats. The traffic is load balanced across both members.
4. Entity C's inline appliance members are normal, have link 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

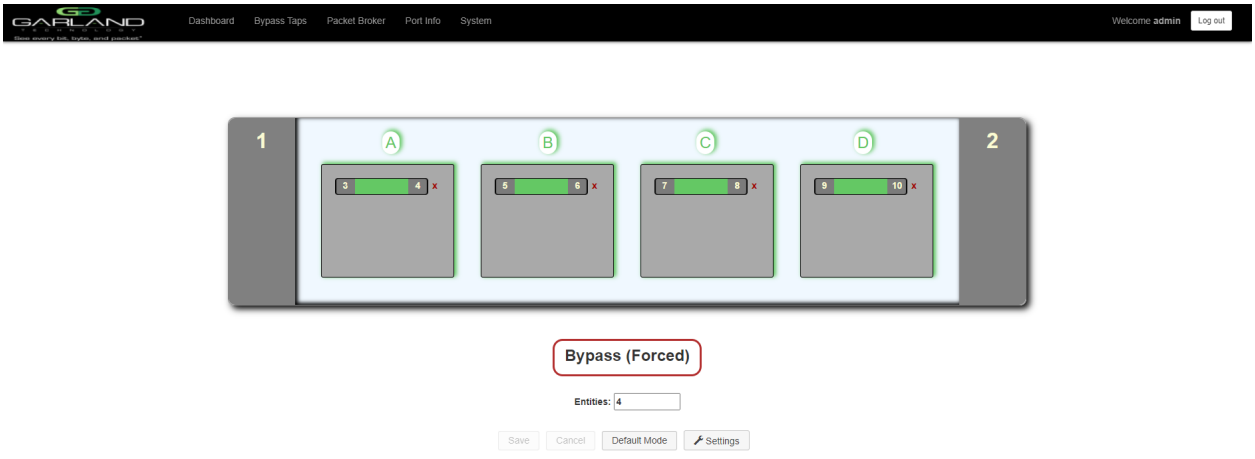


ATLB2 Chained Tap Forced Bypass

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 link and heartbeats.
3. Entity B's inline appliance members are normal, have link and heartbeats.
4. Entity C's inline appliance members are normal, have link and heartbeats.
5. Entity D's inline appliance members are normal, have link 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 link 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 link 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 link 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 link 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