GARLAND
TECHNOLOGY
See every bit, byte, and packet®

User Guide

INT40G2SR44 / INT40G2LR44

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.

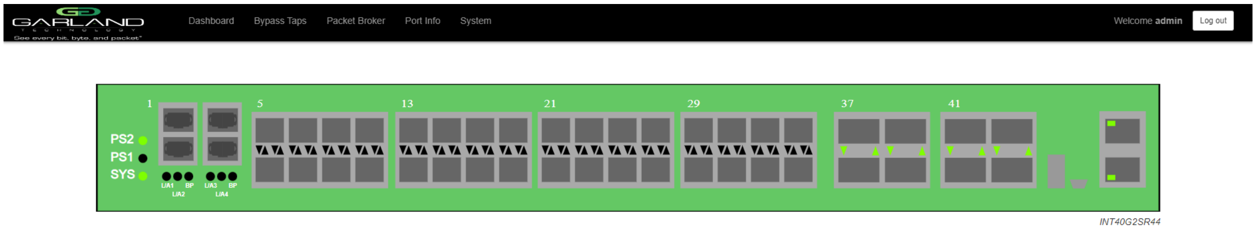
The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Table of Contents

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.

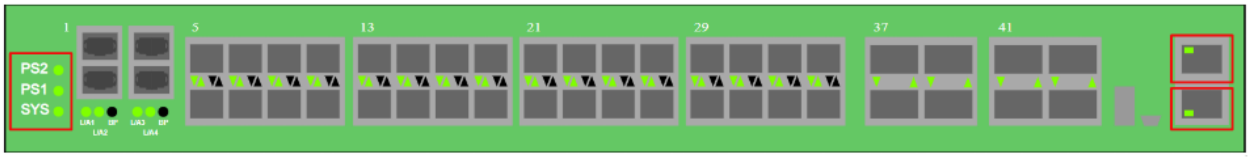
The dashboard provides access to the Bypass Taps, Packet Broker, Port Info and System configuration options by selecting the desired option in the top menu bar. These options are covered in detail per their specific sections.



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

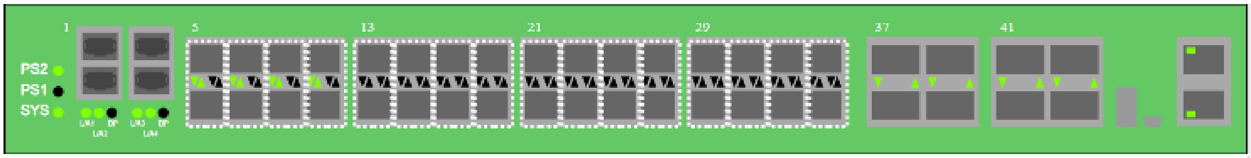
PS2	Power Supply 2 LED
PS1	Power Supply 1 LED
SYS	System LED

Ethernet Interface	Upper Left LED (always illuminated)
Serial Interface	Lower Left LED (always illuminated)

Packet Broker

The Packet Broker of the Dashboard consists of the following.

Dashboard Panel



LED Indications

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
Port 13 Left Up Arrow	Link LED
Port 14 Left Down Arrow	Link LED
Port 15 Left Up Arrow	Link LED
Port 16 Left Down Arrow	Link LED
Port 17 Left Up Arrow	Link LED
Port 18 Left Down Arrow	Link LED
Port 19 Left Up Arrow	Link LED
Port 20 Left Down Arrow	Link LED
Port 21 Left Up Arrow	Link LED
Port 22 Left Down Arrow	Link LED
Port 23 Left Up Arrow	Link LED
Port 24 Left Down Arrow	Link LED
Port 25 Left Up Arrow	Link LED
Port 26 Left Down Arrow	Link LED
Port 27 Left Up Arrow	Link LED
Port 28 Left Down Arrow	Link LED
Port 29 Left Up Arrow	Link LED
Port 30 Left Down Arrow	Link LED
Port 31 Left Up Arrow	Link LED
Port 32 Left Down Arrow	Link LED

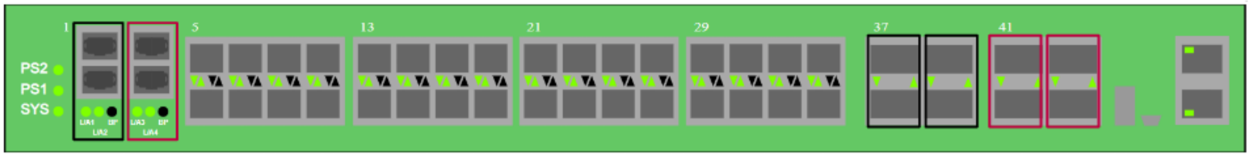
Port 33 Left Up Arrow	Link LED
Port 34 Left Down Arrow	Link LED
Port 35 Left Up Arrow	Link LED
Port 36 Left Down Arrow	Link LED

** The right up/down arrows for ports 5 through 36 are activity LEDs. These LEDs are N/A in the GUI.*

Bypass Taps

The Bypass Taps of the Dashboard consists of the following.

Dashboard Panel



LED Indications

Tap 1

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 37 Right Up Arrow	Tap 1 Primary Inline Appliance Link LED
Port 38 Left Down Arrow	Tap 1 Primary Inline Appliance Link LED
Port 39 Right Up Arrow	Tap 1 Secondary Inline Appliance Link LED
Port 40 Left Down Arrow	Tap 1 Secondary Inline Appliance Link LED

Tap 2

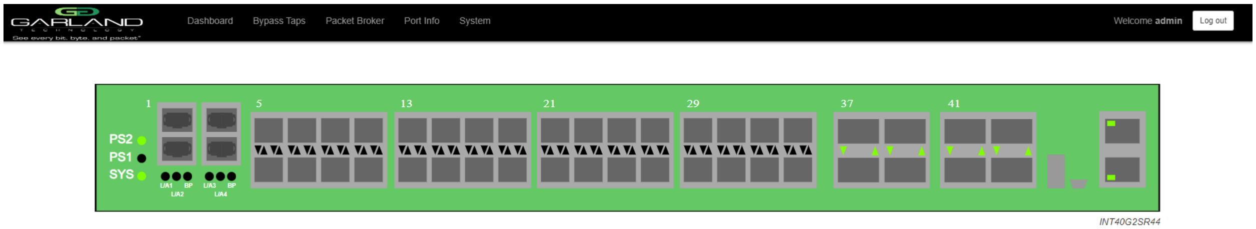
L/A3	Tap 2 Network Port 3 Link/Activity LED
L/A4	Tap 2 Network Port 4 Link/Activity LED
BP	Tap 2 Bypass LED
Port 41 Right Up Arrow	Tap 2 Primary Inline Appliance Link LED
Port 42 Left Down Arrow	Tap 2 Primary Inline Appliance Link LED
Port 43 Right Up Arrow	Tap 2 Secondary Inline Appliance Link LED
Port 44 Left Down Arrow	Tap 2 Secondary Inline Appliance Link LED

** The L/A1 through L/A4 LEDs only indicate link in the GUI.*
** The up/down arrows for ports 37 through 44 only indicate link in the GUI.*

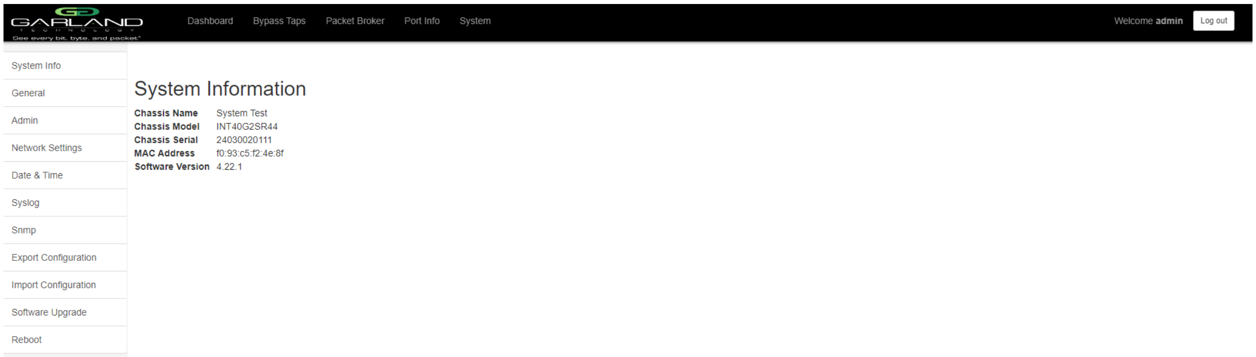
2. System

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.



System Information

Chassis Name	System Test
Chassis Model	INT40G2SR44
Chassis Serial	24030020111
MAC Address	f0:93:c5:f2:4e:8f
Software Version	4.22.1

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

The System Information panel will be displayed.

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.

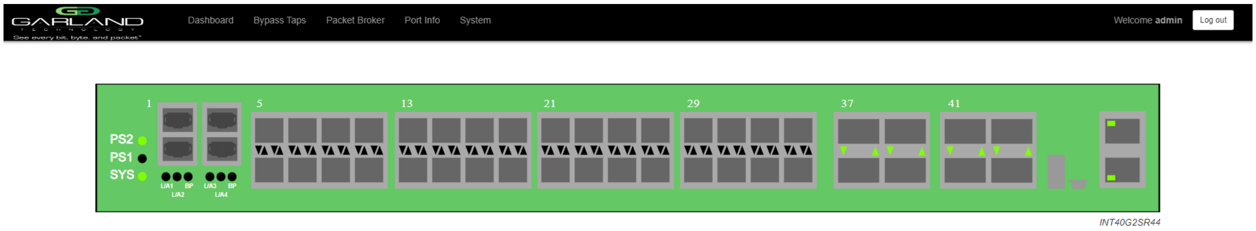
4. Select Go.

    The Login panel will be displayed.

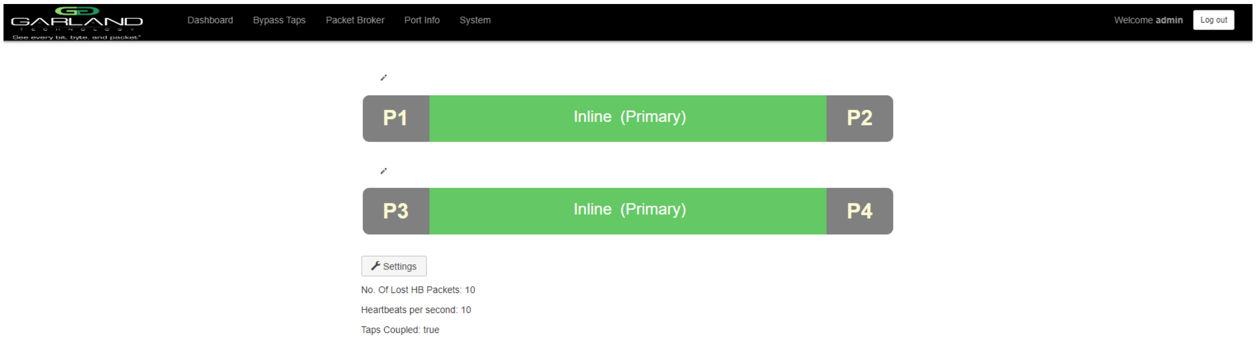
3. Bypass Taps

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

Tap Settings
Bypass Tap Name|
Heartbeat Settings



1. Select Bypass Taps on the Dashboard Menu bar.

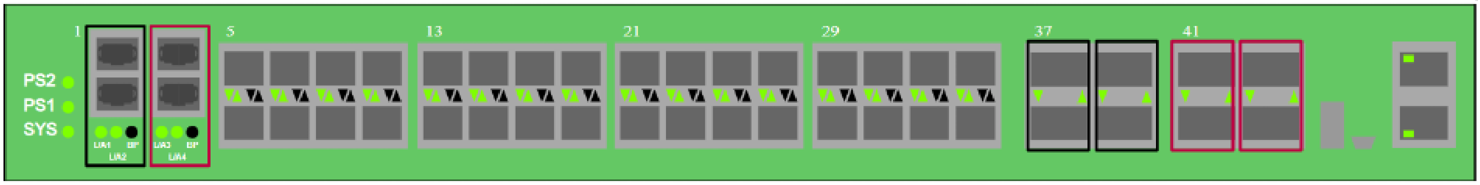


No. Of Lost HB Packets: 10
Heartbeats per second: 10
Taps Coupled: true

The Bypass Taps panel will be displayed. The taps may be configured individually.

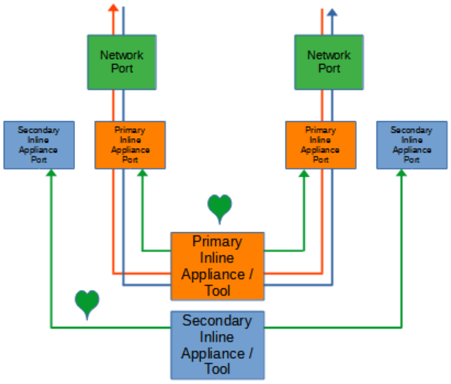
Primary-Secondary Tap Mode

The network, primary inline appliance and secondary inline appliance ports are defined by the system for each tap. 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. Ports 5 through 36 may be configured as packet broker ports.



Tap 1		Tap 2	
Port 1	Network Port	Port 3	Network Port
Port 2	Network Port	Port 4	Network Port
Port 37	Primary Inline Appliance	Port 41	Primary Inline Appliance
Port 38	Primary Inline Appliance	Port 42	Primary Inline Appliance
Port 39	Secondary Inline Appliance	Port 43	Secondary Inline Appliance
Port 40	Secondary Inline Appliance	Port 44	Secondary Inline Appliance

Figure 1 Primary-Secondary Tap


Network Port
Network Port
Secondary Inline Appliance Port
Primary Inline Appliance Port
Primary Inline Appliance Port
Secondary Inline Appliance Port
Primary Inline Appliance / Tool
Secondary Inline Appliance / Tool

Bypass Taps Panel

The Bypass Taps panel displays the following.

Tap 1 Name	Tap 2 Name
Tap 1 Current Status	Tap 2 Current Status
Tap 1 Current Active Inline Appliance	Tap 2 Current Active Inline Appliance

No. Of Lost HB Packets for Tap 1 and Tap 2
Heartbeats per Second for Tap 1 and Tap 2
Tap 1 and Tap 2 Current Coupled

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 Mode
Fail Mode
LFP
Reverse Bypass
Revertive
Coupled

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 2 Primary-Secondary Tap (Primary Inline)

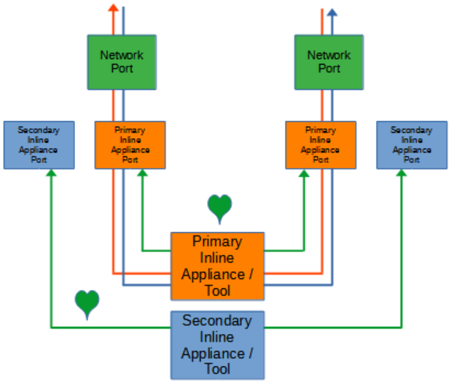

Network Port
Network Port
Secondary Inline Appliance Port
Primary Inline Appliance Port
Primary Inline Appliance Port
Secondary Inline Appliance Port
Primary Inline Appliance / Tool
Secondary Inline Appliance / Tool

Figure 3 Primary-Secondary Tap (Secondary Inline)

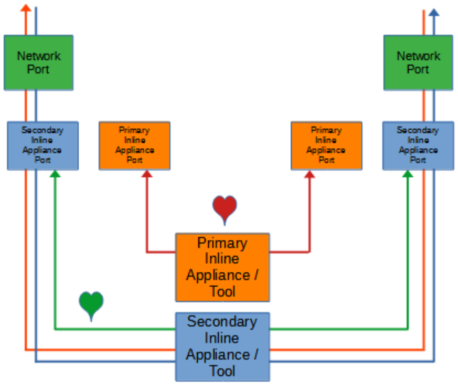
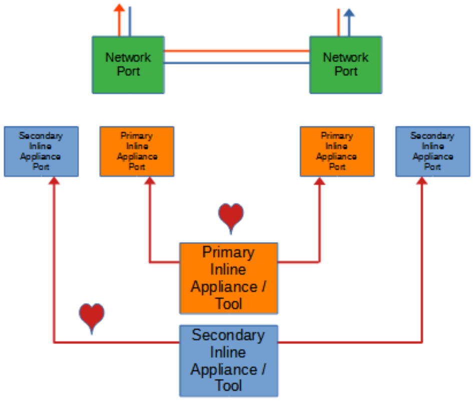
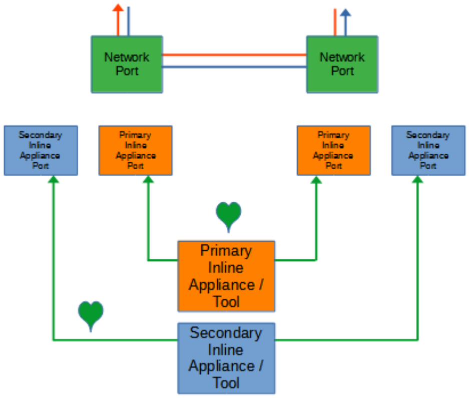

Network Port
Network Port
Secondary Inline Appliance Port
Primary Inline Appliance Port
Primary Inline Appliance Port
Secondary Inline Appliance Port
Primary Inline Appliance / Tool
Secondary Inline Appliance / Tool

Figure 4 Primary-Secondary Tap (Bypass)


Network Port
Network Port
Secondary Inline Appliance Port
Primary Inline Appliance Port
Primary Inline Appliance Port
Secondary Inline Appliance Port
Primary Inline Appliance / Tool
Secondary Inline Appliance / Tool

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 5 Primary-Secondary Tap (Force Bypass)


Network Port
Network Port
Secondary Inline Appliance Port
Primary Inline Appliance Port
Primary Inline Appliance Port
Secondary Inline Appliance Port
Primary Inline Appliance / Tool
Secondary Inline Appliance / Tool

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.

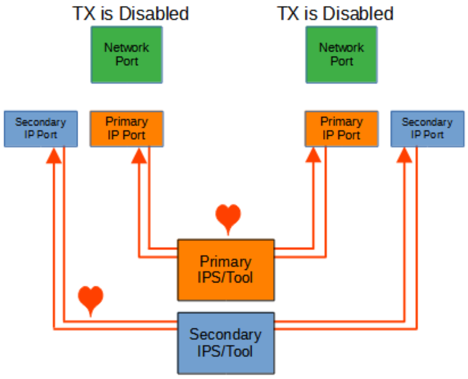
5. LFP — If enabled and link is lost on one of the network ports. The TX will be disabled on the other network port. The RX for both network ports remain on.

Figure 6 Primary-Secondary Tap (LFP)

Loss of Link
Network Port
TX is Disabled
Network Port
TX is Disabled
Network Port
Loss of Link
Network Port

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 7 Primary-Secondary Tap (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. Taps Coupled If enabled all switching functionality supported by Tap 1 and Tap 2 are coupled together. Taps coupled will couple the revertive option for both Taps. If taps coupled is enabled or disabled the other tap options can not be selected until the accept and save are selected. Then the other tap options will become active.

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

10. Select Cancel to return the Tap panel.

11. Select Back to Primary to manually switch the traffic from the secondary inline appliance to the primary inline appliance. This function is independent for each tap unless they are coupled. Then selecting Back to Primary on either tap, will cause both taps to switch.

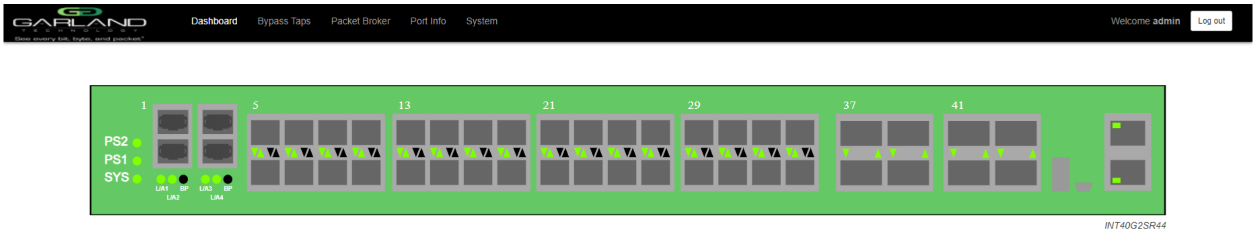
12. Select Save to save updates.

13. Select Cancel to return the Bypass Taps panel.

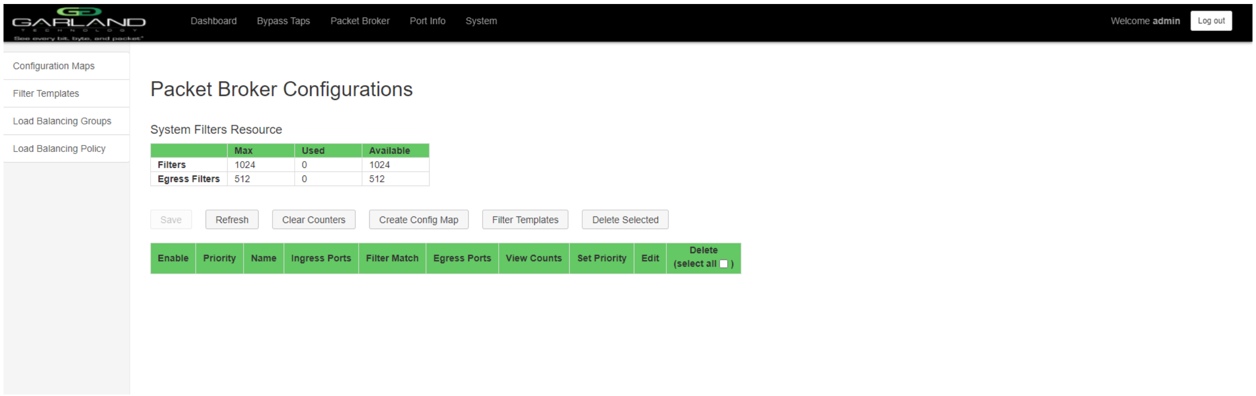
4. Packet Broker

The packet broker section consists of ports 5 through 36. The following configuration options may be displayed, modified, enabled or disabled under the Packet Broker panel.

Configuration Maps	Load Balancing Policy
Filter Templates	Load Balancing Groups



1. Select Packet Broker on the Dashboard menu bar.



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	0	1024
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)

The Packet Broker Configurations panel will be displayed.

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.

   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
   Destination IPv6 Address / Destination IP Mask
   Inner VLAN ID
   Outer VLAN ID
   DSCP
   IP Protocol
   L4 Source Port or Range
   L4 Destination Port or Range

7. Select Save Template.

The new filter template will appear on the Filter Templates panel.

8. Select Cancel to disregard changes and return to the Filter Templates panel.

9. Select the template name to modify the template.

10. Select the red X to delete the template.

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

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

7. Select Save.

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

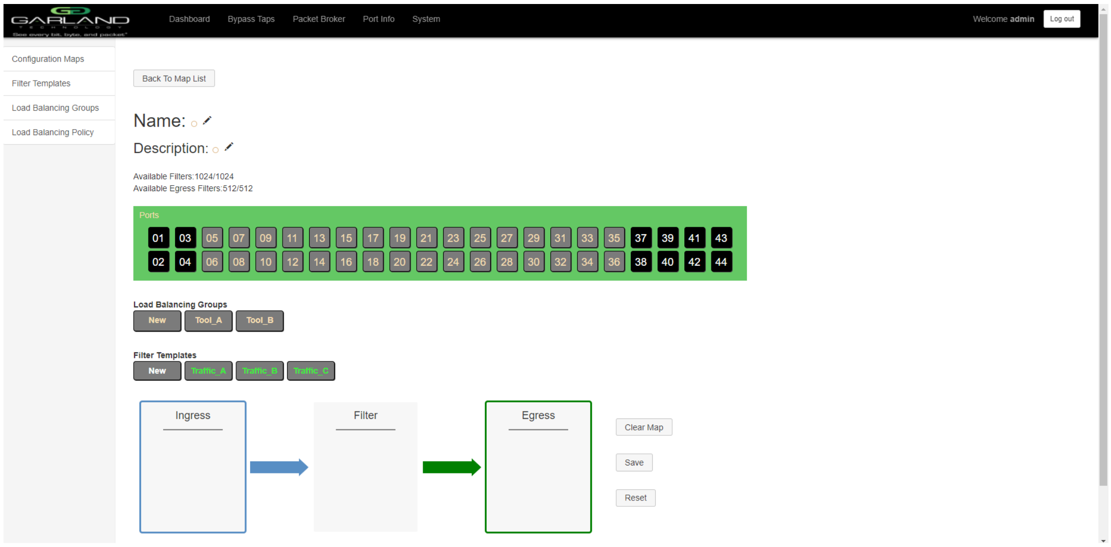
Config Map

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

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

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.



Available Filters:1024/1024
Available Egress Filters:512/512

3. Select the name pencil 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. Enter the desired name.

5. Select the Check to apply.

6. Select the No to disregard.

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

8. Enter the desired description.

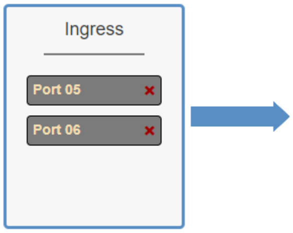
9. Select the Check to apply.

10. Select the No to disregard.

Ingress

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

Figure 8 Ingress



2. Remove a port by selecting the Red X.

Filter

1. Add filters by placing the cursor on the desired filter template. A previously created filter template or the new filter template option may be selected. Select with 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 9 Filter

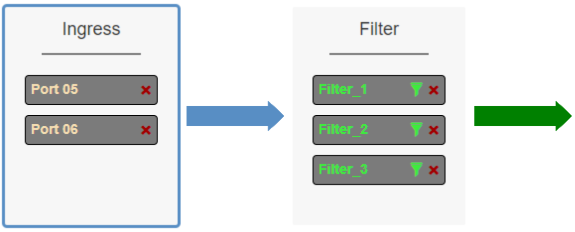
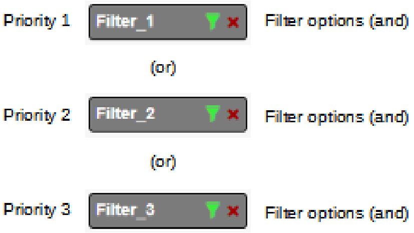


Figure 10 Filter System Considerations



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

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

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

4. Select Accept.

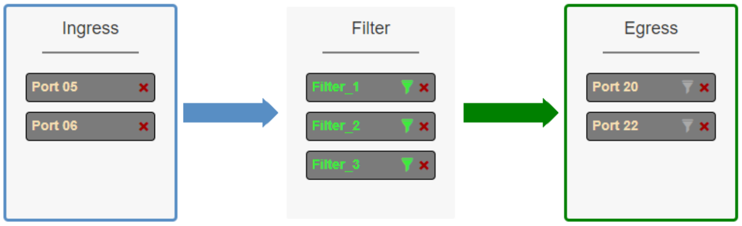
5. Select Cancel to disregard.

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

Egress

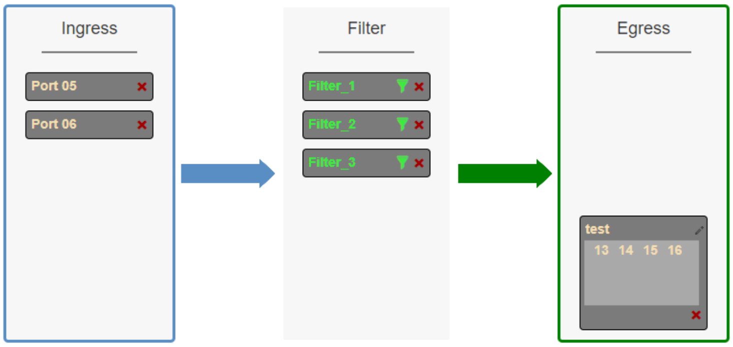
1. Add an egress port by placing the cursor on the desired port. Select with the left mouse button. Drag the port to the Egress panel and release. Repeat for all desired ports. If multiple ports are added, then 100% of the traffic will be sent to each port.

Figure 11 Egress Port(s)



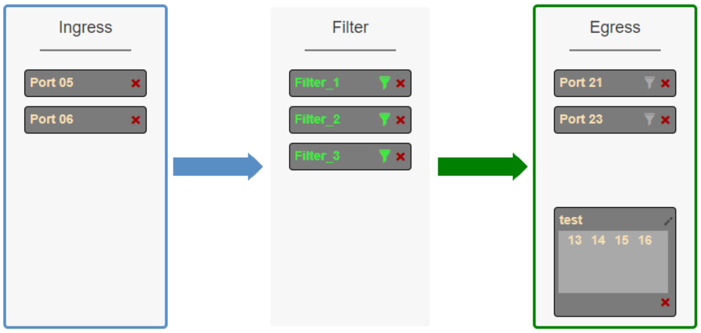
2. Add a load balancing group by placing the cursor on a previously created load balancing group or new load balancing group. Select with the left mouse button. Drag the load balancing group to the Egress panel and release. Ports may be added or removed from any load balancing group. If ports are added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

Figure 12 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 13 Egress Load Balancing Group and Port(s)

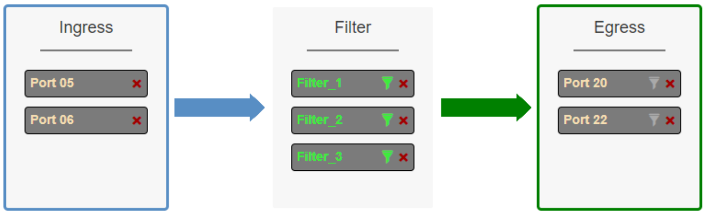


4. Remove a port or load balancing group by selecting the Red X.

Egress Filter

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

Figure 14 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 with 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 15 Port XX Egress Filters

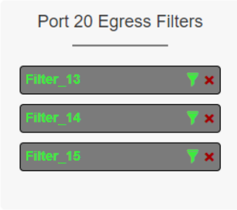
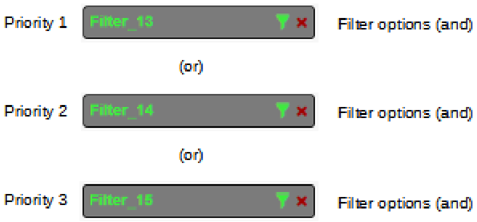


Figure 16 Egress Filter System Considerations



3. If new is selected, the Edit Filter panel will 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, eFltPXX, eFltPXX(2), eFltPXX(3) etc.

5. Select Accept.

6. Select Cancel to disregard.

7. Remove a filter template by selecting the Red X.

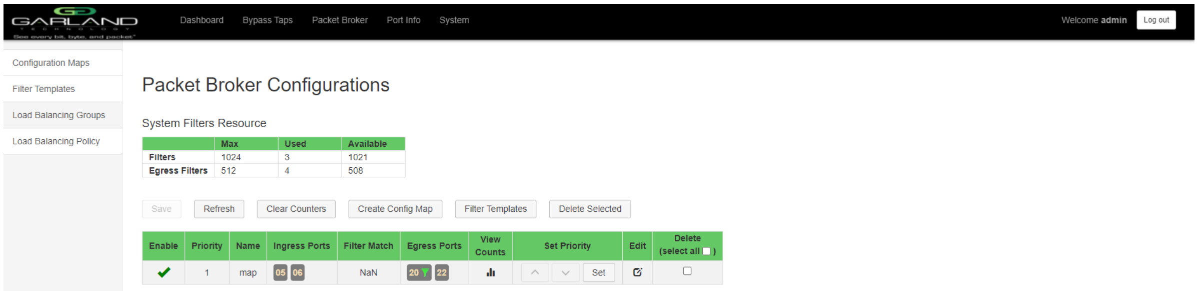
Config Map Save

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.

3. Select Cancel to disregard.



Packet Broker Configurations

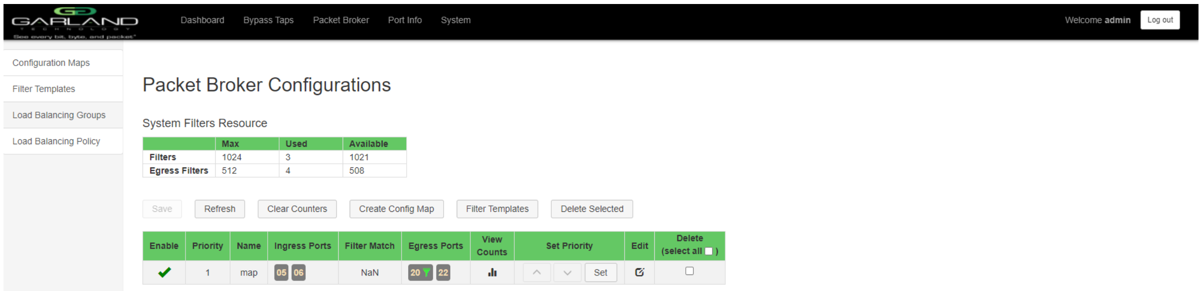
System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	4	508

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	map	05 06	NaN	20 22		Set		□

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	1024	3	1021
Egress Filters	512	4	508

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	map	05 06	NaN	20 22		Set		□

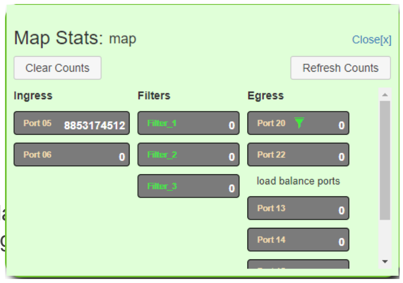
Config Map Statistics

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 for ingress ports, filters, egress ports and load balancing group ports.



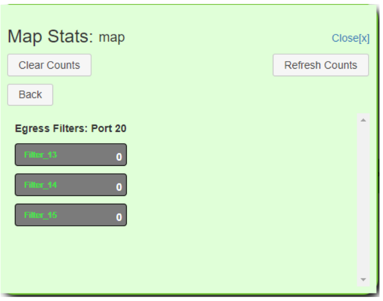
Map Stats: map

Ingress		Filters		Egress	
Port 05	8853174512	Filter_1	0	Port 20	0
Port 06	0	Filter_2	0	Port 22	0
		Filter_3	0	load balance ports	
				Port 13	0
				Port 14	0

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.



Map Stats: map

Egress Filters: Port 20

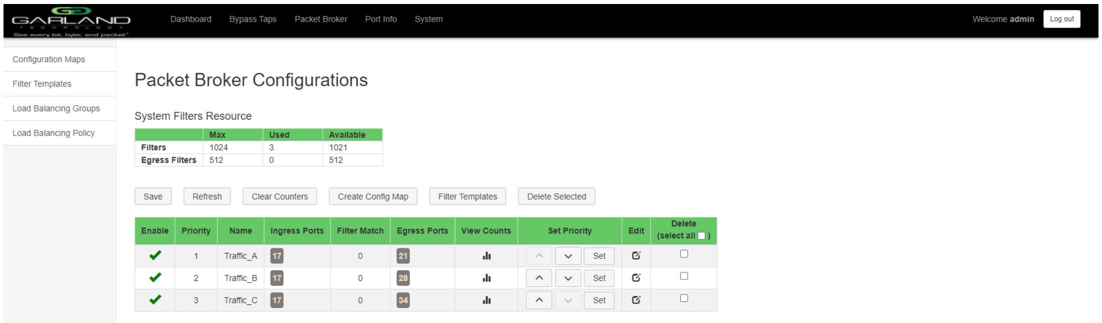
Filter_13	0
Filter_14	0
Filter_15	0

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).



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

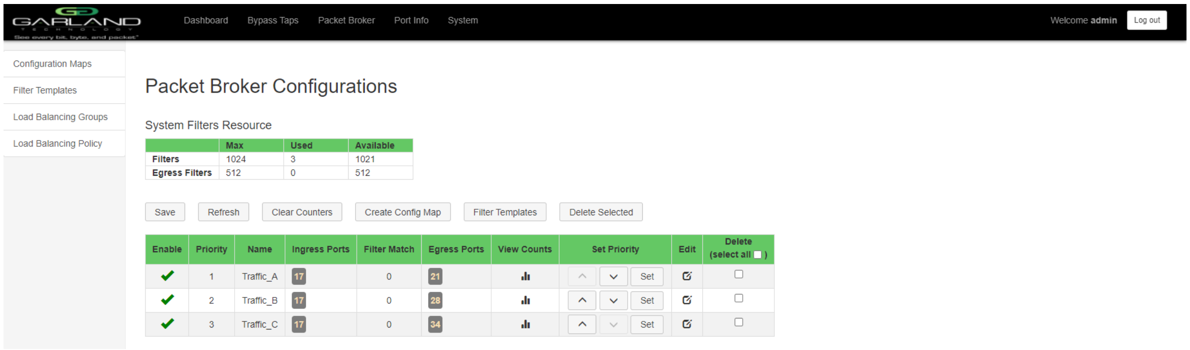
Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Traffic_A	17	0	21	ılı	^ v Set	☑	□
✓	2	Traffic_B	17	0	28	ılı	^ v Set	☑	□
✓	3	Traffic_C	17	0	34	ılı	^ v Set	☑	□

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, 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 17. 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.



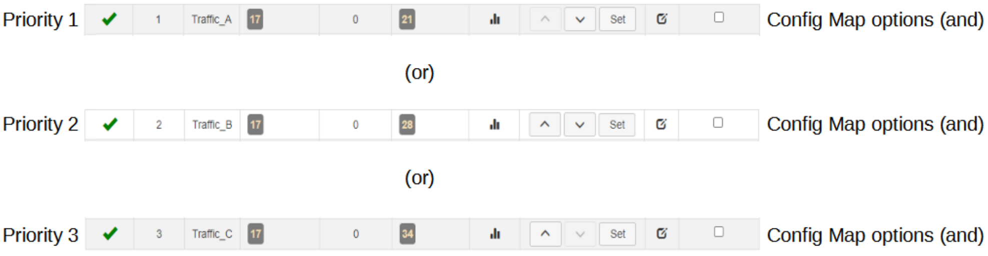
Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Traffic_A	17	0	21	📊	^ v Set	✎	□
✓	2	Traffic_B	17	0	28	📊	^ v Set	✎	□
✓	3	Traffic_C	17	0	34	📊	^ v Set	✎	□

Figure 17 Config Map System Considerations



Method 1

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

2. Select Save to save updates.

Method 2

1. Select Set.

The Set Priority panel will be displayed.

2. Enter the priority in the Set New Priority panel.

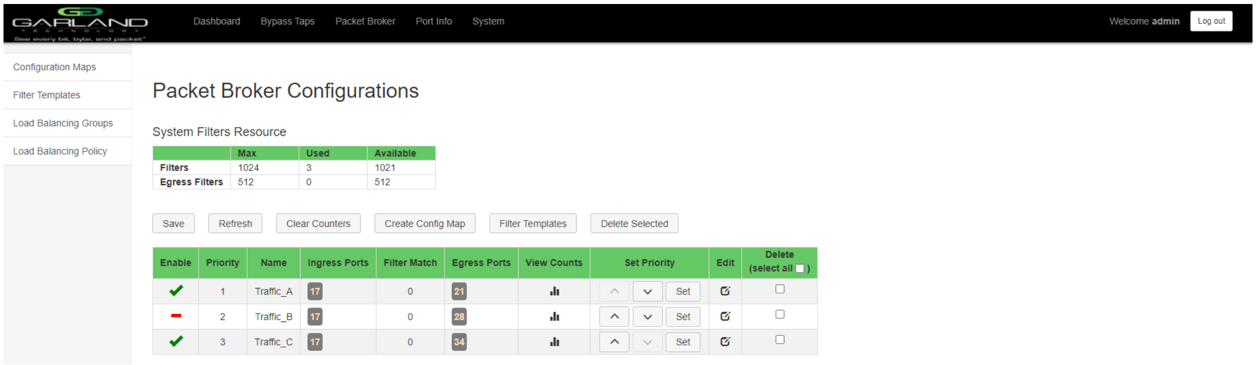
3. Select Set to accept the priority value.

4. Select Cancel to disregard.

5. Select Save to save updates.

Enable/Disable Config Map

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



Packet Broker Configurations

System Filters Resource

	Max	Used	Available
Filters	1024	3	1021
Egress Filters	512	0	512

Enable	Priority	Name	Ingress Ports	Filter Match	Egress Ports	View Counts	Set Priority	Edit	Delete (select all □)
✓	1	Traffic_A	17	0	21	▮	^ v Set	✎	□
–	2	Traffic_B	17	0	28	▮	^ v Set	✎	□
✓	3	Traffic_C	17	0	34	▮	^ v Set	✎	□

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.

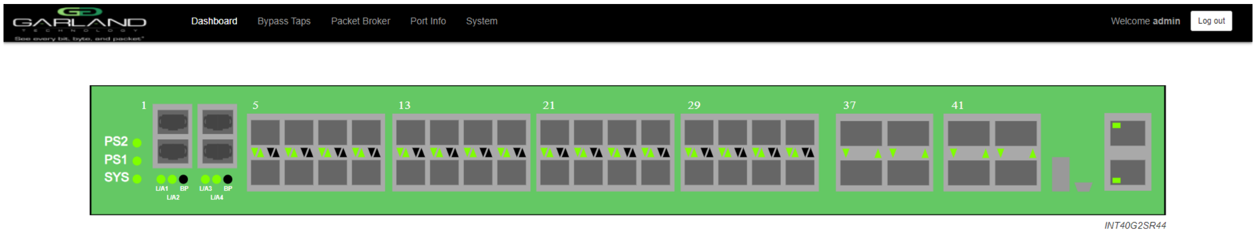
   The red dash will change to a green check.

2. Select Save.

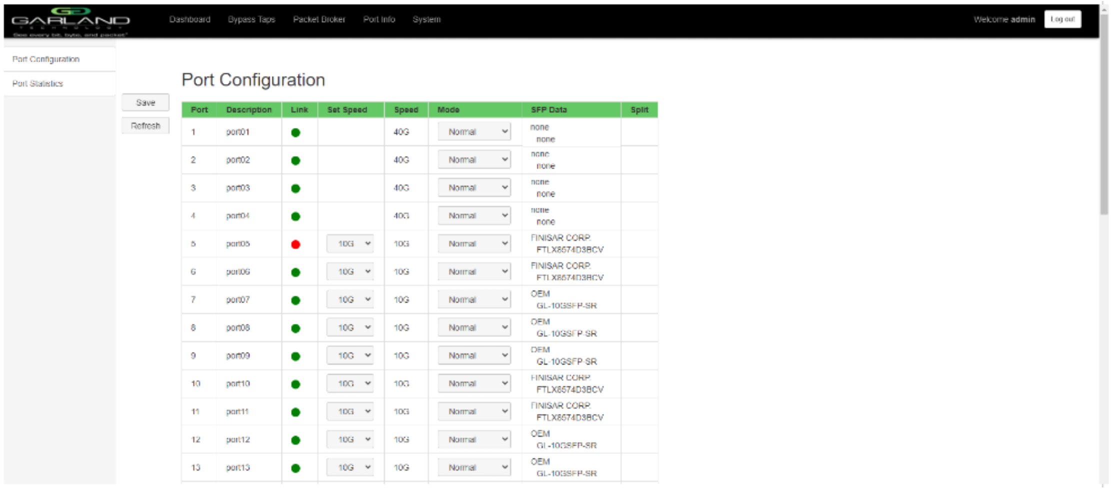
5. Port Info

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

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



1. Select Port Info on the Dashboard menu bar.



Port Configuration

Port	Description	Link	Set Speed	Speed	Mode	SFP Data	Split
1	port01	🟢		40G	Normal	none none	
2	port02	🟢		40G	Normal	none none	
3	port03	🟢		40G	Normal	none none	
4	port04	🟢		40G	Normal	none none	
5	port05	🔴	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
6	port06	🟢	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
7	port07	🟢	10G	10G	Normal	OEM GL-10GSFP-SR	
8	port08	🟢	10G	10G	Normal	OEM GL-10GSFP-SR	
9	port09	🟢	10G	10G	Normal	OEM GL-10GSFP-SR	
10	port10	🟢	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
11	port11	🟢	10G	10G	Normal	FINISAR CORP. FTLX8574D3BCV	
12	port12	🟢	10G	10G	Normal	OEM GL-10GSFP-SR	
13	port13	🟢	10G	10G	Normal	OEM GL-10GSFP-SR	

The Port Configuration panel will be displayed.

Port Configuration

The port configuration is displayed by default. The Description, Set Speed and Mode may be modified. All other options are display 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 Packets
Receive Discards
Receive Errors
Transmit Packets
Transmit Discards
Transmit Errors

1. Select Port Statistics on the Port Configuration panel.

   The Port Statistics panel will be displayed.

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

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 5 through 36.

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 5 through 36.

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.