GARLAND
T E C H N O L O G Y

See every bit, byte, and packet®

User Guide

INT10G8SR56-5/INT10G8SR56-6/INT10G8SR56-7/INT10G8SR56-8/INT10G8SR56-9
INT10G8LR56-5/INT10G8LR56-6/INT10G8LR56-7/INT10G8LR56-8/INT10G8LR56-9

05/2025

Release Version: 5.1.12

User Guide

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.
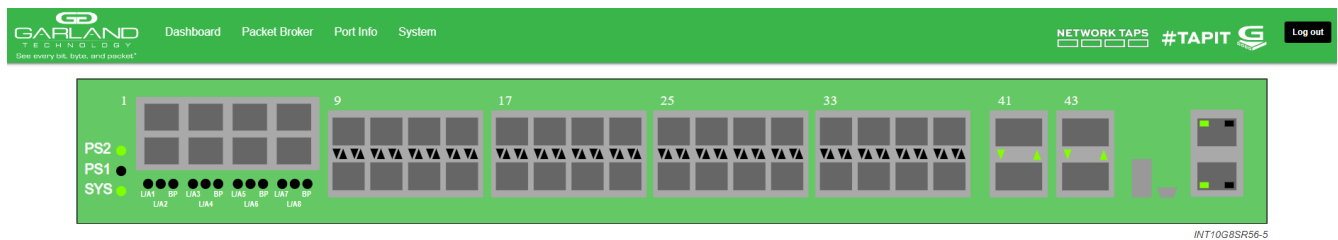
Basic LED Indications

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.

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 of the Dashboard consists of ports 1 through 44.
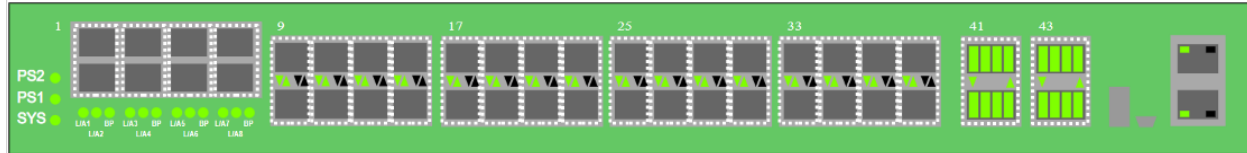
LED Indications

Port 1 L/A1-Port 8 L/A8	Link LED
BP	N/A
Port 1 – Port 39 Left Up Arrow	Link LED
Port 2 – Port 40 Left Down Arrow	Link LED
Port 41 Right Up Arrow	Link/Activity LED
Port 41.1 – 41.4 (split)	Link LEDs
Port 42 Left Down Arrow	Link/Activity LED
Port 42.1 – 42.4 (split)	Link LEDs
Port 43 Right Up Arrow	Link/Activity LED
Port 43.1 – 43.4 (split)	Link LEDs
Port 44 Left Down Arrow	Link/Activity LED
Port 44.1 – 44.4 (split)	Link LEDs

The right up/down arrows for ports 17 through 40 are activity LEDs. These LEDs are N/A in the GUI. The up/down arrow LEDs for ports 41 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   SNMP
General   Export Configuration
Admin   Import Configuration
Network Settings   Software Upgrade
Date & Time   Reboot
Syslog

INT10G8SR56-5
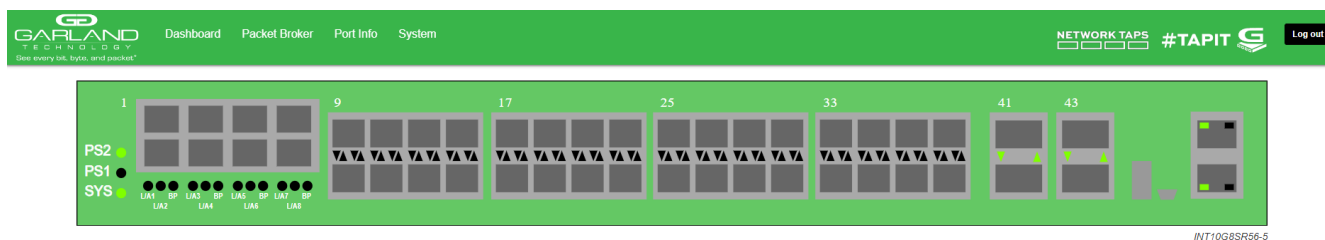
1. Select System on the Dashboard Menu bar.

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

System Info

The System Information panel displays the following.

Chassis Name   Chassis Model   Chassis Serial Number
MAC Address   Software Version

1. Select System Info.

The System Information panel will be displayed.

General

The following configuration options may be displayed or modified.

Chassis Name
Key Press Timeout

1. Select General.

The panel will display the current configuration.

2. Select Edit Configuration.

3. Enable, disable, or modify the desired options.

4. Select Save to save updates.

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

Admin

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

Users
Groups
Authentication
        Local
        TACACS Primary
        TACACS Secondary

1. Select Admin.

The Admin Settings panel will be displayed.

Users

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

1. Select Users + to create a new user.

   The Create New User panel will be displayed.

2. Enter the Username.

   A username may be from 5 to 48 characters, a-z, A-Z, 0-9. A username may not contain any spaces or special characters.

3. Enter the Password.

   *A password may be from 5 to 48 characters, a-z, A-Z, 0-9 and special characters ~ ! @ # % ^ _ [ ] { } ? , . = + - *. A password may not contain any spaces.*

4. Select the group for the user.

5. Select Save to save updates.

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

6. Select Cancel to return to the Admin Settings panel.

7. Edit the username, password or assigned group by selecting the pencil.

8. Delete the user by selecting the red X.

Groups

The group defines the authorization for a user or group of users. A group may be used for local or TACACS authorization. In Use "true" means that there is at least one local user assigned to the group. If a group is used by TACACS, the In Use will indicate "false". There are three defaults groups: admin, OPER and NOC. All three groups may be modified, however only the OPER and NOC groups may be deleted.

The supported authorization privileges are as follows:

AAA - authentication, authorization, account
ADM – user administrator
DTC – date, time, ntp configuration
DTV – date, time, ntp view
EXC – export/import
IPC – maintenance network ip configuration
IPV - maintenance network ip view
LGC - syslog, snmp configuration
LGV - syslog, snmp view
MIS – miscellaneous

PBC - packet broker configuration
PBV - packet broker view
PTC - port configuration

PTV - port view
RBT - chassis reboot
TPC - tap config
TPV - tap view
UPG - software field upgrade
USR - account configuration

1. Select Groups + to create a new group.

The Create New Group panel will be displayed.

2. Enter the Group Name.

3. Select the desired privileges.

4. Select Save to save updates.

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

5. Select Cancel to return to the Admin Settings panel.

6. Modify the group privileges by selecting the pencil.

7. Deleted the group by selecting the red X.

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

Authentication

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

1. Select Authentication Settings.

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

Local Authentication Disable

1. Deselect Local Authentication.

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

2. Select Save.

Local Authentication Enable

1. Select Local Authentication.

2. Select Save.

TACACS Primary Authentication

1. Select Enable Primary.

> *The TACACS Primary panel will be displayed.*

2. Enter the IP Address, IPv4 or IPv6.

3. Enter the Secret Word, (optional).

4. Enter the Timeout value, (5-60 sec).

5. Select Save to save updates.

6. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

> *The TACACS Test panel will appear.*

2. Select Primary.

3. Enter the Username.

4. Enter the Password.

5. Select Test.

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

TACACS Ping Test

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

1. Select TACACS 1 Ping.

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

TACACS Secondary Authentication

1. Select Enable Secondary.

The TACACS Secondary panel will be displayed.

2. Enter the IP Address, IPv4 or IPv6.

3. Enter the Secret Word, (optional).

4. Enter the Timeout value, (5-60 sec).

5. Select Save to save updates.

6. Select Cancel to return the Admin Settings panel.

TACACS Test

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

1. Select TACACS Test.

The TACACS Test panel will appear.

2. Select Secondary.

3. Enter the Username.

4. Enter the Password.

5. Select Test.

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

TACACS Ping Test

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

1. Select TACACS 2 Ping.

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

Network Settings

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

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

The default system network configurations are as follows:

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

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

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

1. Select Network Settings.

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

IPv4 / Disable

1. Deselect Enable IPv4.

2. Select Save.

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

3. Select OK.

IPv4 Enable

1. Select Enable IPv4.

2. Enter the desired Address, (www.xxx.yyy.zzz/xx).

3. Enter the desired Gateway.

4. Select Save.

IPv6 Enable

1. Select Enable IPv6.

2. Enter the desired Address.

3. Enter the desired Gateway.

4. Select Save.

IPv6 Disable

1. Deselect Enable IPv6.

2. Select Save.

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

3. Select OK.

Add SSL Certificate

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

1. Select Add SSL Certificate.

The Select Certificate and Select Key File panel will appear.

2. Select Choose File for Select Certificate.

3. Select the desired cert.pem file.

4. Select Open.

5. Select the Choose File for Select Key File.

6. Select the desired key.pem file.

7. Select Open.

8. Select Upload.

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

9. Verify SSL Certificate Loaded "true".

10. Verify Using Uploaded SSL Certificate "true".

Disable Using Uploaded SSL Certificate

1. Select Edit Settings.

2. Deselect Using Uploaded SSL Certificate.

3. Select Save.

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

4. Refresh Browser.

5. Verify SSL Certificate Loaded "true".

6. Verify Using Uploaded SSL Certificate "false".

Date & Time

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

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

1. Select Date & Time.

>*The Date & Time Settings panel will be displayed.*

Timezone

1. Select Edit Settings.

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

3. Select Save.

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

UTC

1. Select Edit Settings.

2. Select the desired UTC using the pull-down panel.

3. Select Save.

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

Manually Set Date & Time

1. Select Edit Settings.

2. Enter the Hours or use the up/down arrows to select.

3. Enter the Minutes or use the up/down arrows to select.

4. Enter the Date, MM/DD/YYYY or use the calendar to select.

5. Select Save.

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

NTP No Authentication (Symmetric)

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

must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

1. Select Edit Settings.

2. Select NTP timing.

3. Enter the IPv4 or IPv6 Address.

4. Verify Authenticate, None.

5. Select Save.

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

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

NTP Authentication (Symmetric)

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

1. Select Edit Settings.

2. Select NTP timing.

3. Enter the IPv4 or IPv6 Address.

4. Select Authenticate, Symmetric.

5. Select Encryption Type, (MD5, SHA1, SHA224, SHA256, SHA384, SHA512)

6. Enter the Key Number.

7. Enter the Key.

8. Select Save.

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

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

Syslog

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

must be assigned. The system allows for an IPv4 and IPv6 management interface to be assigned simultaneously.

1. Select Syslog.

    The Syslog Configuration panel will be displayed.

2. Select Edit Settings.

3. Select Enable Syslog Config.

4. Enable Unit ID, (optional).

5. Enter the Unit ID, (optional).

6. Enter the IPv4 or IPv6 Address.

7. Enter the desired UDP Port Number or use the default, 514.

8. Select Save.

9. Select Cancel to return the Syslog Configuration panel.

Syslog Test

1. Select Syslog Test.

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

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

SNMP

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

The following SNMP configuration options are supported:

> V2 Read/Write
> V2 Read Only

V3 Auth Type	MD5 / SHA
V3 Priv Protocol	DES / AES

1. Select SNMP.

    The SNMP Configuration panel will be displayed.

2. Select Edit Configuration.

3. Select Enable SNMP Config.

4. Enter the desired Access Port number or use the default, 161.

5. Enter the desired Trap Port number or use the default, 162.

6. Enter the IPv4 or IPv6 Address.

7. Select the desired Protocol, (V2 Read/Write or V2 read Only).

8. Enter the desired V2 Community Password.

9. Select the desired Protocol, (V3).

10. Enter the desired V3 User.

11. Enter the desired V3 Auth Password.

12. Enter the desired V3 Priv password.

13. Select Save.

14. Select Cancel to return the SNMP Configuration panel.

SNMP Test

1. Select SNMP Test.

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

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

Export Configuration

This option creates a configuration file (exportCfg.json) that may be used to recover a unit. The exportCfg.json file may be renamed if desired. The exportCfg.json file does not contain Usernames, Passwords, Groups or Network Settings.

1. Select Export Configuration.

    The Export Configuration panel will be displayed.

2. Select Export.

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

Import Configuration

This option allows a previously created configuration file (exportCfg.json) to be uploaded to the unit. The Chassis Model is the only option that is considered and must match, otherwise the unit will reject the exportCfg.json file.

1. Select Import Configuration.

   The Import Configuration panel will be displayed.

2. Select Choose File.

3. Select the desired exportCfg.json file.

4. Select Open.

5. Select Upload.

   The unit will automatically verify the selected exportCfg.json file.

6. Select Configure.

   The unit will import and load the exportCfg.json. An "import done" message will be displayed when complete. A reboot is not required.

Software Upgrade

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

Reboot

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

1. Select Reboot.

   The Reboot Device panel will be displayed.

2. Select Reboot.

   The unit will present an "Are you sure?" message.

3. Select OK.

   The GUI will display a "rebooting" as well as a "Session timed out. Go to Login screen" message.
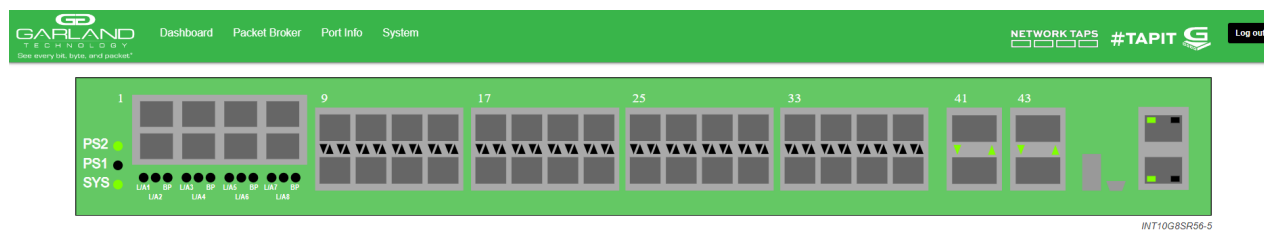
4. Select Go.

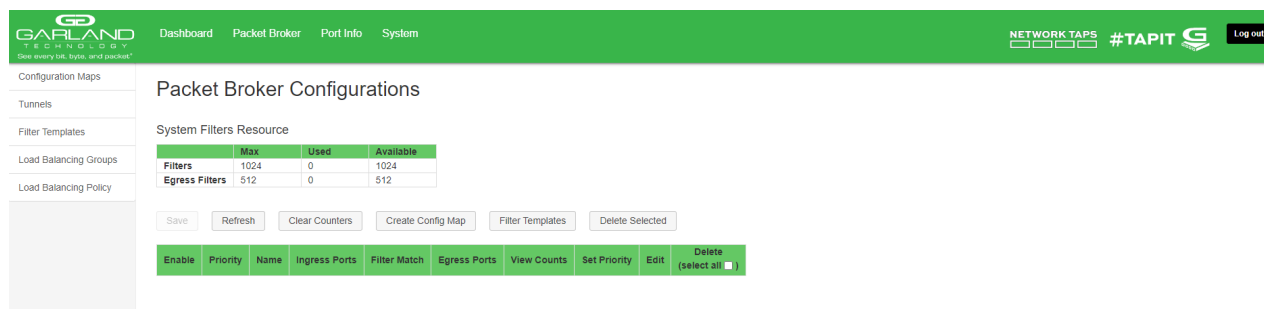   *The Login panel will be displayed.*

3. Packet Broker

The packet broker section consists of ports 1 through 44.

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

Configuration Maps   Load Balance Groups
Tunnels   Load Balance Policy
Filter Templates

1. Select Packet Broker on the Dashboard menu bar.

*The Packet Broker Configurations panel will be displayed.*
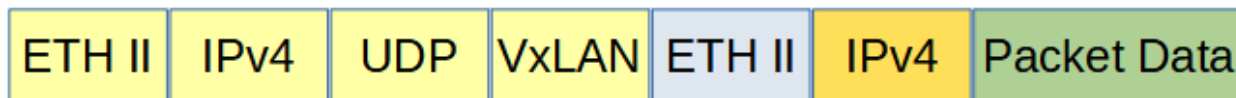
Tunnels

The system supports the ability to:

- Encapsulate VXLAN packets

- Decapsulate VXLAN packets

- Encapsulate l2GRE packets

- Decapsulate l2GRE packets

Encapsulate VXLAN Packets (VXLAN TX Only)

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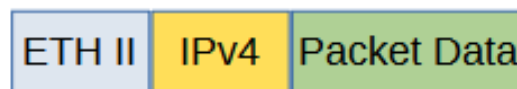
ETH II	IPv4	Packet Data

Original Packet

ETH II	IPv4	UDP	VxLAN	ETH II	IPv4	Packet Data

VXLAN Encapsulated Packet

1. Select Tunnels.

   The Tunnels panel will be displayed.

2. Select Create Tunnel.

   The Create Tunnels panel will be displayed.

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

Ports

| 01 | 03 | 05 | 07 | 09 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 33 | 35 | 37 | 39 | 41 | 43 |
| 02 | 04 | 06 | 08 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 | 38 | 40 | 42 | 44 |

Ingress

Port 17 ✕

Configure 🔧

Egress

Clear

Save

Back

4. Add an egress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Egress panel and release.

Ports

| 01 | 03 | 05 | 07 | 09 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 33 | 35 | 37 | 39 | 41 | 43 |
| 02 | 04 | 06 | 08 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 | 38 | 40 | 42 | 44 |

Ingress

Port 17 ✕

Configure 🔧

Egress

Port 18 ✕

Clear

Save

Back

5. Select Configure.

   The Configure panel will be displayed.

6. Select VXLAN TX Only

7. Enter the Tunnel IP Address, (VXLAN Header SIP).

8. Enter the Remote IP Address, (VXLAN Header DIP).

9. Enter the Remote MAC Address, (VXLAN Header DMAC).

10. Enter the VNID, (1-16777215).

   The default UDP destination port is 4789.

11. Select Advanced to modify the UDP destination port, (1-65535).

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

12. Select Advanced to select an alternative SMAC or to manually enter the SMAC, (VXLAN Header SMAC).

13. Select Advanced to add a VLAN ID to the VXLAN Header, optional, (1-4095).

14. Select Set.

15. Select Cancel to disregard.

16. Select Save.

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

Create Tunnel

Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID	
1	234		vxlan-tx-only	10.10.10.10	f2:93:c5:e5:30:44	10.10.10.25	f0:93:c5:a1:a1:a1	4789	18	17		x

17. The tunnel may be deleted by selecting red X.
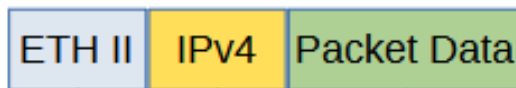
Decapsulate VXLAN Packets (VXLAN RX Only)

When the VXLAN header is decapsulated from a packet, the VXLAN header segments are removed as shown below.
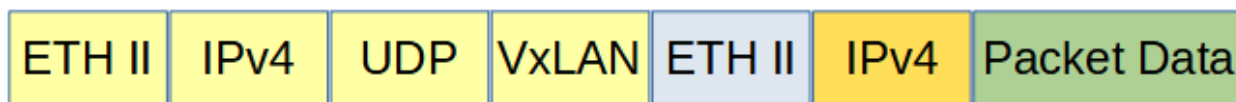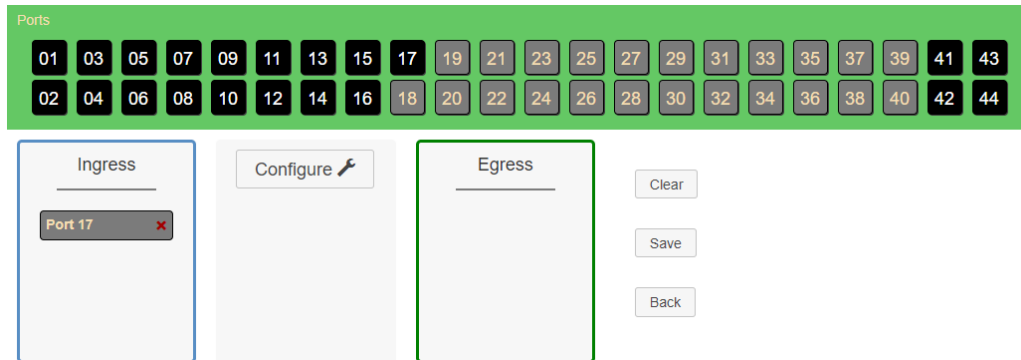

VXLAN Encapsulated Packet

VXLAN Decapsulated Packet

1. Select Tunnels.
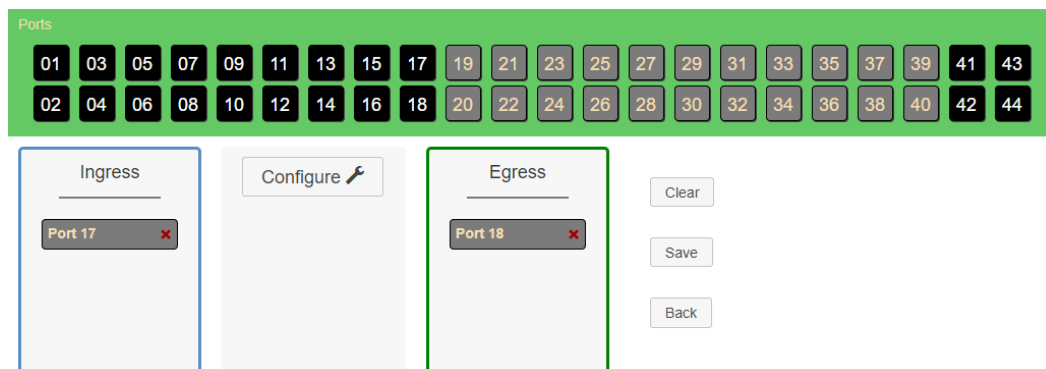
The Tunnels panel will be displayed.

2. Select Create Tunnel.

The Create Tunnels panel will be displayed.

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

4. Add an egress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Egress panel and release.

5. Select Configure.

The Configure panel will be displayed.

6. Select VXLAN RX Only

7. Enter the Tunnel IP Address, (VXLAN Header DIP).

8. Enter the Remote IP Address, (VXLAN Header SIP).

9. Enter the VNID, (1-16777215).

The default UDP destination port is 4789.

10. Select Advanced to modify the UDP destination port, (1-65535).

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

11. Select Advanced to select an alternative DMAC or to manually enter the DMAC, (VXLAN Header DMAC).

12. Select Advanced to add a VLAN ID, optional, (1-4095).

13. Select Set.

14. Select Cancel to disregard.

15. Select Save.

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

Create Tunnel

Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID	
1	456	✎	vxlan-rx-only	20.20.20.20	f2:93:c5:e5:30:44	20.20.20.25		4789	18	17		x

Secondary VNIDs may be added to the tunnel.

16. Select the Secondary VNID edit icon.

    The VNIDs panel will be displayed

17. Enter the desired Secondary VNID.

18. Select +.

Create Tunnel

Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID
1	456	678 ✎	vxlan-rx-only	20.20.20.20	f2:93:c5:e5:30:44	20.20.20.25		4789	18	17	

The vxlan-rx-only tunnel with the Secondary VNID will be displayed on the Tunnels panel. The tunnel may be deleted by selecting the red X. However, all Secondary VNIDs must be removed first.

19. Select the Secondary VNID edit icon.

    The VNIDs panel will be displayed.
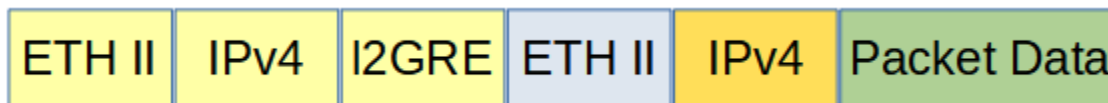
20. Select the red X for each Secondary VNID.

21. The tunnel may be deleted by selecting red X.

Encapsulate l2GRE Packets (GRE TX Only)

When a packet is encapsulated with a l2GRE header the new l2GRE header segments are added to the original packet. The l2GRE header segments consists of Ethernet II, IPv4 and l2GRE as shown below.
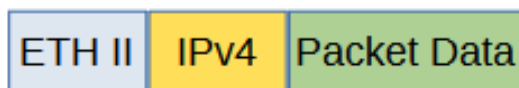
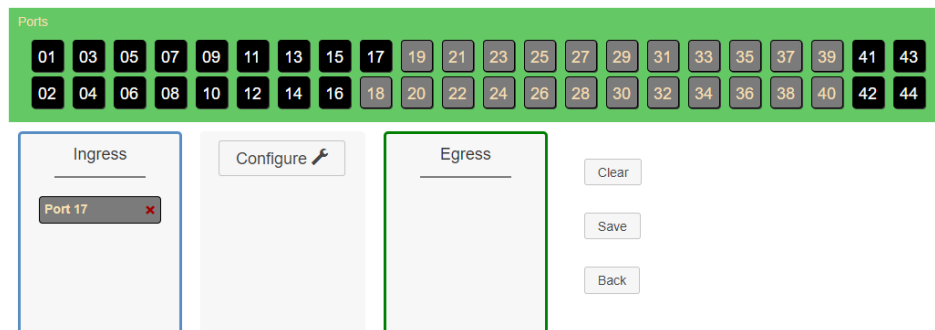
Original Packet

I

2GRE Encapsulated Packet

1. Select Tunnels.

   The Tunnels panel will be displayed.

2. Select Create Tunnel.

   The Create Tunnels panel will be displayed.

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

4. Add an egress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Egress panel and release.

5. Select Configure.

   The Configure panel will be displayed.

6. Select GRE TX Only.

7. Enter the Tunnel IP Address, (l2GRE Header SIP).

8. Enter the Remote IP Address, (l2GRE Header DIP).

9. Enter the Remote MAC Address, (l2GRE Header DMAC).

10. Enter the Key, (1-16777215).

    The default l2GRE Header SMAC is automatically defined by the system. There are five predefined SMACs.

11. Select Advanced to select an alternative SMAC or to manually enter the SMAC.

12. Select Advanced to add a VLAN ID, optional, (1-4095).

13. Select Set.

14. Select Cancel to disregard.

15. Select Save.

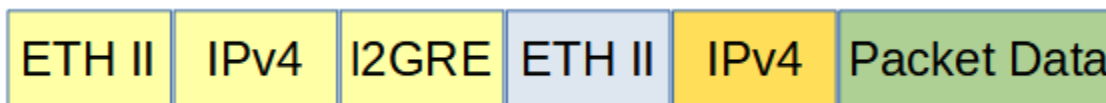   The gre-tx-only tunnel will be displayed on the Tunnels panel.

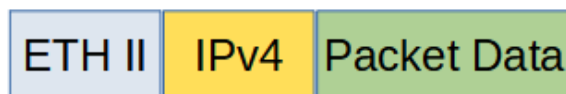| Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID	
1	345		gre-tx-only	30.30.30.30	f2:93:c5:e5:30:44	30.30.30.25	f0:93:c5:b1:b1:b1		18	17		x

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

Decapsulate l2GRE Packets (GRE-RX Only)

When a l2GRE packet is decapsulated the l2GRE header segments are removed from the packet.

| ETH II | IPv4 | l2GRE | ETH II | IPv4 | Packet Data |

2GRE Encapsulated Packet

l2GRE Decapsulated Packet

| ETH II | IPv4 | Packet Data |

1. Select Tunnels.

   The Tunnels panel will be displayed.

2. Select Create Tunnel.

   The Create Tunnels panel will be displayed.

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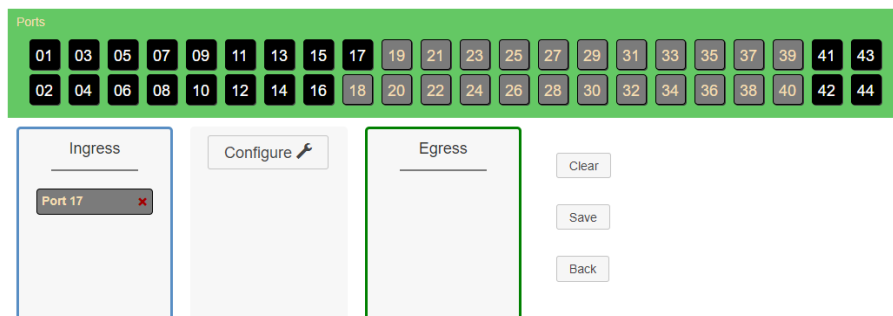
4. Add an egress port by placing the cursor on the desired port. Select the left mouse button. Drag the port to the Egress panel and release.
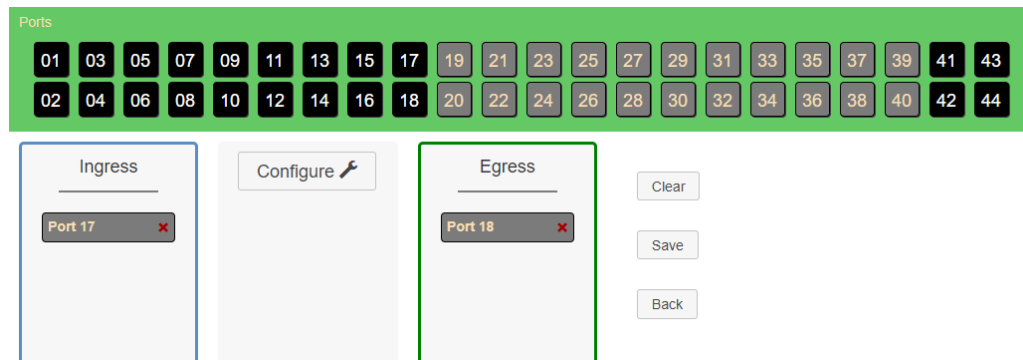
5. Select Configure.

   The Configure panel will be displayed.

6. Select GRE RX Only.

7. Enter the Tunnel IP Address, (l2GRE Header DIP).

8. Enter the Remote IP Address, (l2GRE Header SIP).

9. Enter the Key, (1-16777215).

   The default l2GRE Header SMAC is automatically defined by the system. There are five predefined SMACs.

10. Select Advanced to select an alternative DMAC or to manually enter the DMAC, (l2GRE Header DMAC).

11. Select Advanced to add a VLAN ID, optional, (1-4095).

12. Select Set.

13. Select Cancel to disregard.

14. Select Save.

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

Create Tunnel

Tunnel ID	Primary VNID	Secondary VNIDs	Type	IP Address	MAC Address	Remote IP	Remote MAC	UDP Port	Egress Port	Ingress Port	Tunnel VLAN ID	
1	1234		gre-rx-only	40.40.40.40	f2:93:c5:e5:30:44	40.40.40.25			18	17		x

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

Filter Template

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

1. Select Filter Templates.

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

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

7. Select Save.

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

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

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

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

Load Balancing Policy

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

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

1. Select Load Balancing Policy.

   The Load Balancing Policy panel will be displayed.

2. Select or deselect the desired load balancing policy options.

3. Select Save to save updates.

4. Select Cancel to disregard changes.

Config Map

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

1. Select Configuration Maps.

   The Packet Broker Configurations panel will be displayed.

2. Select Create Config Map.

   The Create Config Map panel will be displayed. Any previously created load balancing groups or filter templates will be displayed along with the new options. Any port shaded gray can be used for a config map, any port shaded black may not be used.
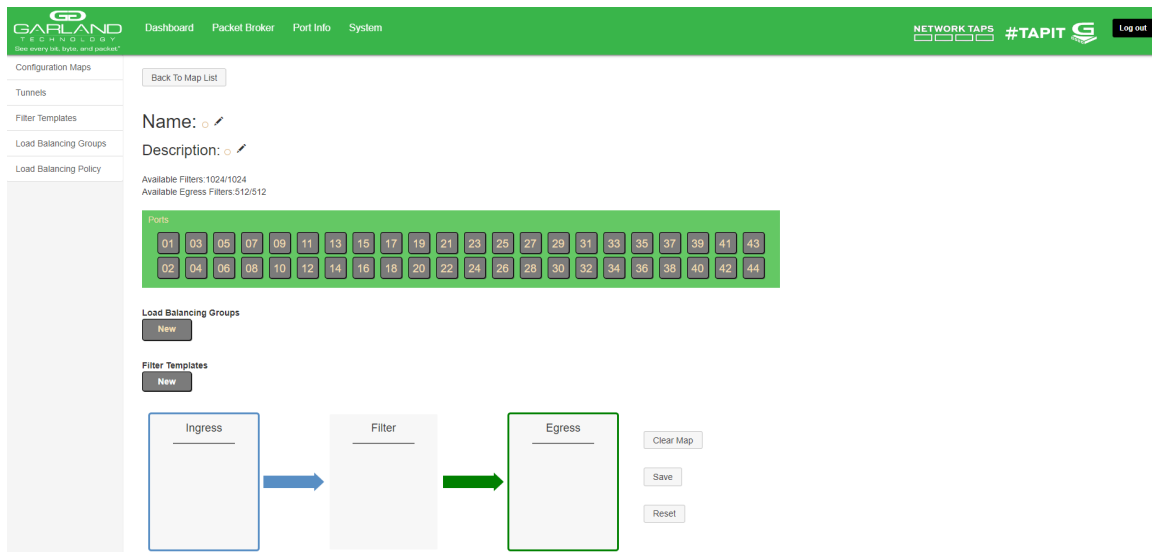
3. Select the name pencil to apply a name, optional. If no name is entered the system will automatically apply a name to the config maps as follows, map, map(1), map(2) etc.

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 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 29 Ingress
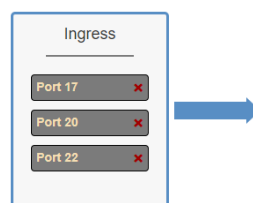
2. Remove a port by selecting red X.

Filter

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

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

   Figure 30 Filter
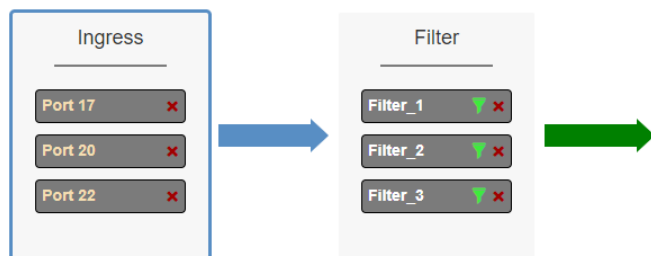
Figure 31 Filter System Considerations
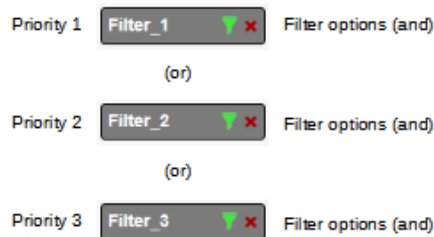
2. Filter templates may be modified by selecting the green filter icon for the desired template.

   *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 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.
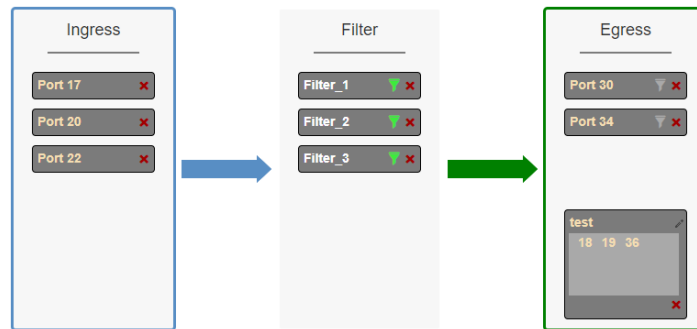
Figure 32 Egress Port(s)
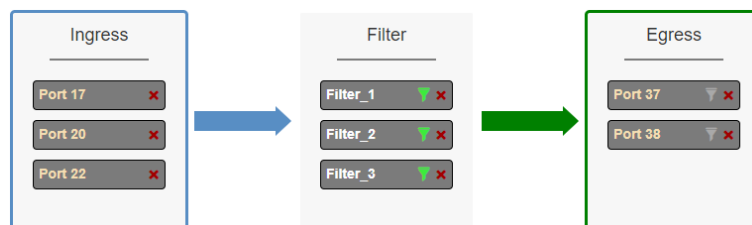
2. Add a load balancing group by placing the cursor on a previously created load balancing group or new load balancing group. Select the left mouse button. Drag the load balancing group to the Egress panel and release. Ports may be added or removed from any load balancing group. If ports are added or removed from a previously created load balancing group, the original load balancing group will also be modified.

Figure 33 Egress Load Balancing Group
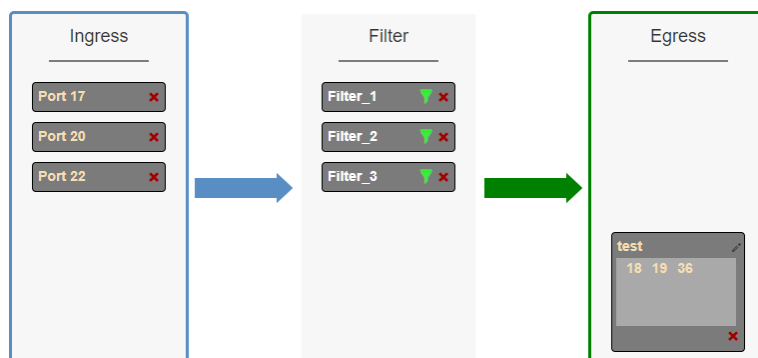
3. One load balancing group plus separate port(s) may be applied. The traffic applied to the ports assigned to the load balancing group will follow the hashing per the load balancing policy. 100% of the traffic will be sent to each of the separate port(s).
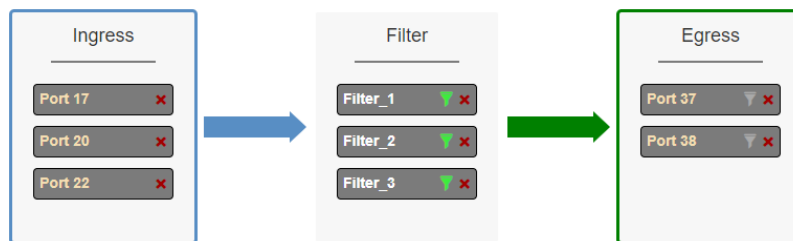
**Figure 34 Egress Load
Balancing Group and Port(s)**

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 35 Egress Filter

The Port XX Egress Filters panel will be displayed.

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

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

Figure 36 Port XX Egress Filters

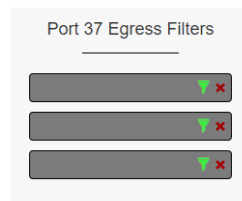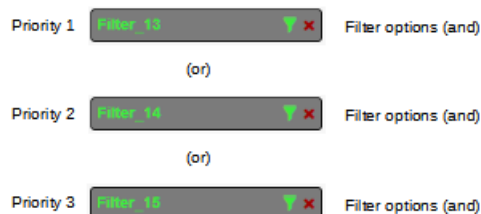

Port 37 Egress Filters

Figure 37 Egress Filter System Considerations

3. If new is selected, the Edit Filter panel will be displayed.

4. Enter the filter name, optional. If no name is entered the system will automatically apply a name to the egress filter as follows, 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.

Modify a Config Map

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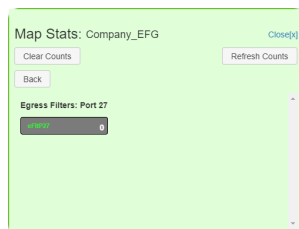

Config Map Statistics

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

1. Select Refresh to refresh the config map statistics.

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

3. Select the View Counts icon to display individual statistics for ingress ports, filters, egress ports and load balancing group ports.
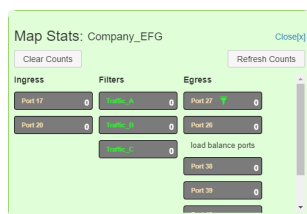
4. Select Refresh Counts to refresh the statistics.

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

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

7. Select Refresh Counts to refresh the statistics.

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

Delete Config Map

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

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	18	📊	∧	∨	Set	✎	☐
✔	2	Traffic_B	17	0	19	📊	∧	∨	Set	✎	☐
✔	3	Traffic_C	17	0	20	📊	∧	∨	Set	✎	☐

Figure 38 Config Map System Considerations

Method 1

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

2. Select Save to save updates.

Method 2

1. Select Set.

   The Set Priority panel will be displayed.

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

3. Select Set to accept the priority value.

4. Select Cancel to disregard.

5. Select Save to save updates.

Enable/Disable Config Map

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

Disable Config Map

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

   The green check will change to a red dash.

2. Select Save.

Enable Config Map

1. Select the red dash for the config map in the Enable column.
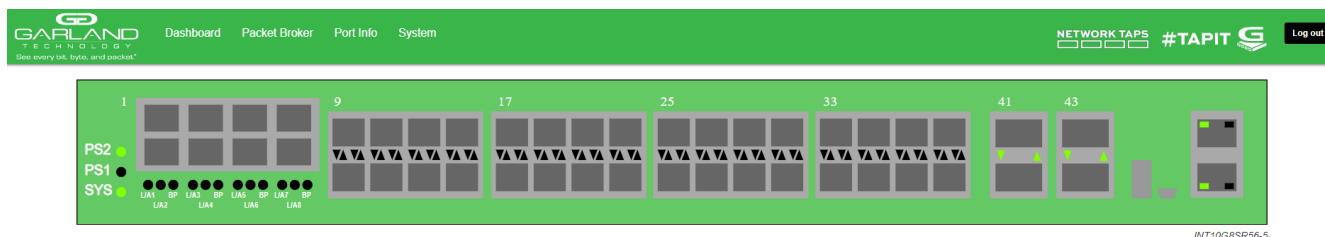
   The red dash will change to a green check.
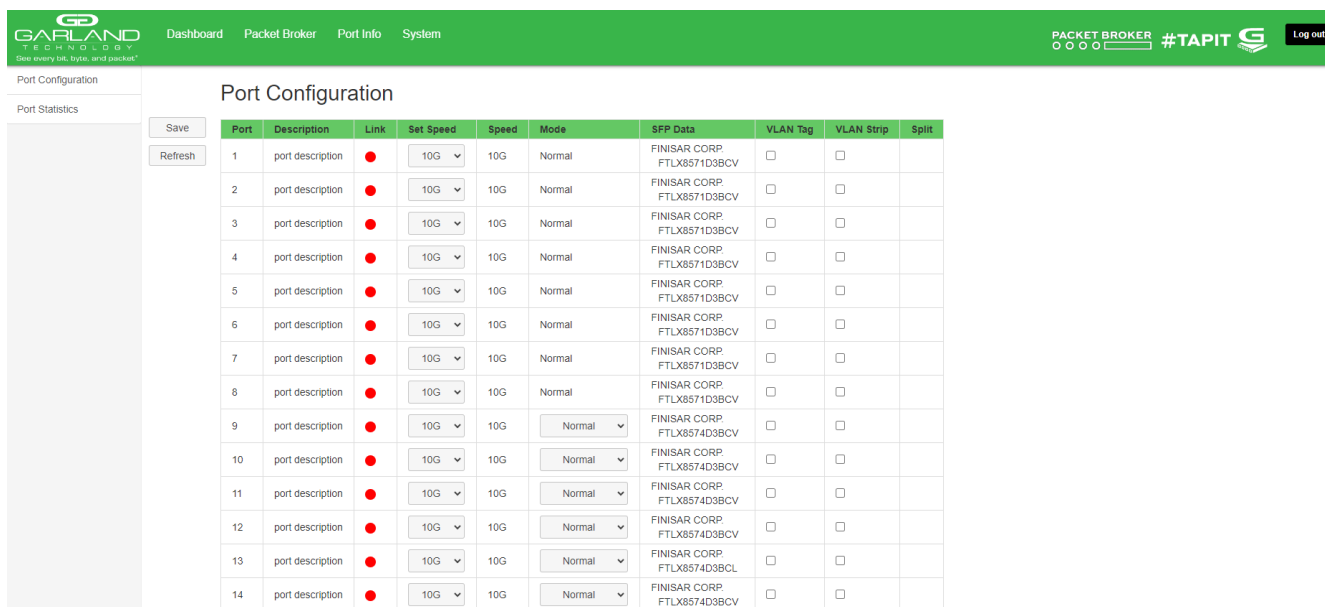
2. Select Save.

4. Port Info

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

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

INT10G8SR56-5

1. Select Port Info on the Dashboard menu bar.

The Port Configuration panel will be displayed.

Port Configuration

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

Port Description

1. Modify the port description by placing the cursor on Port Description for the desired port and press the left mouse button.

   The Edit Description panel will be displayed.

2. Place the cursor in the description field and enter the new description.

3. Select Set to save updates.

4. Select Cancel to return to the Port Configuration panel.

Set Speed

1. Modify the port speed by selecting the pull-down panel for the desired port.

2. Select the desired speed.

3. Select Save to save updates.

Mode

1. Modify the port mode by selecting the pull-down panel for the desired port.

2. Select the desired mode. The available port modes are Normal, Loopback, Listen Only and Force Link.

3. Select Save to save updates.

Port Statistics

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

Port number	Receive Discards	Transmit Discards
Description	Receive Errors	Transmit Errors
Receive Packets	Transmit Packets	

1. Select Port Statistics on the Port Configuration panel.

   The Port Statistics panel will be displayed.

2. Update the statistics by selecting Refresh.

3. Clear and refresh the statistics by selecting Clear.

VLAN Tag

VLAN tag applies a VLAN ID to the packets when the port is configured as an ingress port on a config map. This option is only available for packet brokers ports. The packet broker section consists of ports 1 through 44.

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

2. Enter the desired VLAN ID, (1-4094).

3. Select Save.

4. Disable by deselecting the VLAN Tag option for the desired port.

5. Select Save.

VLAN Strip

VLAN strip removes the outer VLAN ID for packets when the port is configured as an egress port on a config map. This option is only available for packet brokers ports. The packet broker section consists of ports 1 through 44.

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.