



See every bit, byte, and packet[®]

Garland Technology M1GXXCE Packet Broker System

Garland Technology: Modular Aggregation/Filtering

Chassis Firmware Rev Level: 1.0.55

New York, Texas and Germany

Office: 716-242-8500

www.garlandtechnology.com/support

Copyright © 2021 Garland Technology LLC. All Rights Reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted, in any form, or by any means, electronic or otherwise, including photocopying, reprinting, or recording, for any purpose, without the express written permission of Garland Technology.

TRADEMARKS GARLAND TECHNOLOGY and THE GARLAND TECHNOLOGY LOGO are trademarks of Garland Technology LLC in the U.S. and other countries. The use of any of these trademarks without Garland Technology prior written consent is strictly prohibited. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Garland Technology LLC disclaims any proprietary interest in the trademarks and trade names other than its own.

DISCLAIMER The information in this book is provided “as is”, with no warranties whatsoever, including any warranty of merchantability, fitness for any purpose or any warranty otherwise arising out of any proposal, specification or sample. This document is provided for informational purposes only and should not be construed as a commitment on the part of Garland Technology. Information in this document is subject to change without notice.

REQUESTS for information or obtaining permission for use of material of this work, please submit a written request to: Corporate Marketing and Legal, Garland Technology on www.garlandtechnology.com.

DOCUMENT No.: M1GXXCE_v1.0.55

Contents

1. Introduction	8
1.1 Purpose	8
1.2 Scope	8
1.3 General Information	8
1.4 M1GXXF TAP Series	9
1.4.1 Setting up the Filter TAP to operate as a Legacy TAP	9
1.4.2 Traffic flow for Breakout TAP mode	10
1.4.3 Traffic flow for Aggregation Mode	10
1.4.4 Traffic flow for SPAN mode	10
1.4.5 Direct and aggregate all the traffic on slots 1, 2, and 3 out to slot 4	10
1.5 Legacy TAPs	11
2. Installation	13
3. Features	14
4. Front View	15
5. Rear View	16
6. Administration	17
6.1 Network Configuration	18
6.2 Key Press Timeout	18
6.3 NTP Setup	19
6.4 Time Zone Menu	19
6.5 Date & Time Setup	20
6.6 Syslog Configuration Menu	20
6.6.1 What is Syslog?	21
6.6.2 What will Syslog Report on?	21
6.7 snmp Configuration Menu	22
6.7.1 What will snmp Report on?	22
6.8 Back to the Main Menu	23
6.9 Setting up the Users	23
6.9.1 User ADMIN	24
6.9.2 User OPERATOR	24
6.9.3 User LOGGER	24
6.9.4 User BYPASS	24
6.9.5 Password Policy	24
6.9.6 The 'Add User' Help Menu for setting up Users	24
7. Web Interface Login	25
7.1 Configuring the installed Modules	25
7.2 Configuring the System	29
7.2.1 Syslog Configuration	29
7.2.2 snmp Configuration	30

7.2.3	Export Configuration	30
7.2.4	Import Configuration	30
7.2.5	Update Firmware	31
8	M1GXXF Module Series	32
8.1	TAP Modules Descriptions	33
8.1.1	M1GCCF Module	33
8.1.2	M1GCCF Configuration	34
8.1.3	M1GCSF Module	40
8.1.4	M1GCSF Configuration	40
8.1.5	M1GMCF Module	46
8.1.6	M1GMCF Configuration	46
8.1.7	CM1GMSF Module	50
8.1.8	M1GMSF Configuration	51
8.1.9	M1GSCF Module	53
8.1.10	M1GSCF Configuration	54
8.1.11	M1GSSF Module	58
8.1.12	M1GSSF Configuration	58
8.2	Filter Configuration	63
8.2.1	Layer 2 Filter set up	63
8.2.2	Layer 3 Filter set up	71
8.2.3	Layer 4 Filter set up	73
9	M1GXXBP Module Series TAPs	78
10	M1GXXA Module TAP Series	79
11	Part Numbers and Descriptions	79
11.1	1U and 2U Packet Broker Chassis	79
11.2	Modular TAPs designed to operate with the filtering and aggregating backplane	79
11.3	Bypass TAP Modules	80
11.4	Legacy TAP Modules	80
12	Technical Specifications	81
13	Definitions and Help	82
14	Console Cable for M1GXXCE Serial Mgt. port	83

Table of Figures

FIGURE 1: FILTER TAP PASSING PORT 80 TRAFFIC	9
FIGURE 2: FILTER TAP FLOW DIAGRAM PORT 80 TRAFFIC	9
FIGURE 3: FLOW DIAGRAM FOR BREAKOUT, AGGREGATION & SPAN MODE	9
FIGURE 4: TAP 1 FLOW FOR BREAKOUT MODE ON M1GXXF TAP SERIES	10
FIGURE 5: AGGREGATION MODE TRAFFIC FLOW	11
FIGURE 6: BREAKOUT MODE TRAFFIC FLOW	11
FIGURE 7: SPAN MODE TRAFFIC FLOW	11
FIGURE 8: BYPASS TAP NORMAL MODE (INLINE)	11
FIGURE 9: BYPASS TAP BYPASS MODE (BYPASS)	12
FIGURE 10: BLANKING PLATE	13
FIGURE 11: FRONT VIEW 1U PACKET BROKER SYSTEM	15
FIGURE 12: FRONT VIEW 2U PACKET BROKER SYSTEM	15
FIGURE 13: 1U CHASSIS ROW AND SLOT INFORMATION	15
FIGURE 14: 2U CHASSIS ROW AND SLOT INFORMATION	15
FIGURE 15: REAR VIEW 1U PACKET BROKER SYSTEM WITH AC POWER SUPPLIES	16
FIGURE 16: REAR VIEW 2U PACKET BROKER SYSTEM WITH AC POWER SUPPLIES	16
FIGURE 17: REAR VIEW 1U PACKET BROKER SYSTEM WITH DC POWER SUPPLIES	16
FIGURE 18: REAR VIEW 1U PACKET BROKER SYSTEM WITH DC POWER SUPPLIES	16
FIGURE 19: MAIN MENU	17
FIGURE 20: SETTINGS MENU	17
FIGURE 21: NETWORK CONFIGURATION MENU	18
FIGURE 22: KEY PRESS TIMEOUT MENU	18
FIGURE 23: NTP OFF SETUP MENU	19
FIGURE 24: NTP ON SETUP MENU	19
FIGURE 25: TIME ZONE SETUP MENU	19
FIGURE 26: DATE & TIME SETUP MENU TIMEOUT MENU	20
FIGURE 27: SYSLOG CONFIGURATION MENU	20
FIGURE 28: SYSLOG CONFIG MENU TURNED 'ON'	20
FIGURE 29: SNMP CONFIGURATION MENU	22
FIGURE 30: SNMP CONFIGURATION MENU 'NEW SETUP'	22
FIGURE 31: MAIN MENU SCREEN	23
FIGURE 32: USER ADMINISTRATION MENU	23
FIGURE 33: ADD USER MENU	23
FIGURE 34: SET PASSWORD POLICY SCREEN	24
FIGURE 35: ADD USER HELP MENU	24
FIGURE 36: SYSTEM MENU, 1U CHASSIS	25
FIGURE 37: SYSTEM MENU, 2U CHASSIS	25
FIGURE 38: CONFIGURATION MENU FOR A FILTER TAP	26
FIGURE 39: CONFIGURATION MENU FOR A FILTER TAP	27
FIGURE 40: SYSTEM MENU	27
FIGURE 41: MODULE 3 CONFIGURATION MENU	28
FIGURE 42: MODULE 4 CONFIGURATION MENU	29
FIGURE 43: SYSTEM CONFIGURATION MENU	29
FIGURE 44: SYSLOG CONFIGURATION MENU	30
FIGURE 45: SNMP CONFIGURATION MENU	30
FIGURE 46: EXPORT CONFIGURATION MENU	30
FIGURE 47: IMPORT CONFIGURATION MENU	30
FIGURE 48: IMPORT CONFIGURATION MENU	31
FIGURE 49: MAIN MENU	32
FIGURE 50: SELECT THE SLOT NUMBER TO VIEW/MODIFY SCREEN	32
FIGURE 51: SLOT 1 STATUS SCREEN FOR THE M1GCCF	32
FIGURE 52: SLOT 2 STATUS SCREEN FOR THE M1GCCBP	33
FIGURE 53: FRONT VIEW OF M1GCCF	33

FIGURE 54: SLOT 1 STATUS SCREEN.....	34
FIGURE 55: NETWORK PORT SPEED CONFIGURATION	34
FIGURE 56: MONITOR PORT SPEED CONFIGURATION	34
FIGURE 57: LFP MODE CONFIGURATION.....	35
FIGURE 58: RESTORE DEFAULTS SCREEN.....	35
FIGURE 59: PORT UTILIZATION MODULE SCREEN FOR MODULE 1	35
FIGURE 60: SET MAX RECEIVE THRESHOLD TAB.....	36
FIGURE 61: SET PORT A MAX RECEIVE THRESHOLD TO 53%	36
FIGURE 62: SET MAX TRANSMIT THRESHOLD	37
FIGURE 63: SET MAX TRANSMIT THRESHOLD TO 90%	37
FIGURE 64: PORT ERRORS MODULE 1BACKPLANE.....	38
FIGURE 65: SET MAX RECEIVE THRESHOLD	38
FIGURE 66: SET MAX TRANSMIT THRESHOLD	39
FIGURE 67: PORT ERRORS MODULES SCREEN.....	39
FIGURE 68: FRONT VIEW OF M1GCSF.....	40
FIGURE 69: SLOT 1 STATUS SCREEN.....	40
FIGURE 70: NETWORK PORT SPEED CONFIGURATION	40
FIGURE 71: MONITOR PORT SPEED CONFIGURATION	41
FIGURE 72: LFP MODE CONFIGURATION.....	41
FIGURE 73: RESTORE DEFAULTS SCREEN.....	42
FIGURE 74: PORT UTILIZATION MODULE SCREEN FOR MODULE 1	41
FIGURE 75: SET MAX RECEIVE THRESHOLD	42
FIGURE 76: SET MAX TRANSMIT THRESHOLD	43
FIGURE 77: PORT ERRORS MODULES SCREEN.....	43
FIGURE 78: SET MAX RECEIVE THRESHOLD	44
FIGURE 79: SET MAX TRANSMIT THRESHOLD	44
FIGURE 80: PORT ERRORS MODULES SCREEN.....	45
FIGURE 81: FRONT VIEW OF M1GMCF	46
FIGURE 82: SLOT 2 STATUS SCREEN.....	46
FIGURE 83: MONITOR SP. CONF.	47
FIGURE 84: RESTORE DEFAULTS SCREEN.....	47
FIGURE 85: PORT UTILIZATION MODULE SCREEN FOR MODULE 1	47
FIGURE 86: SET MAX RECEIVE THRESHOLD	48
FIGURE 87: SET MAX TRANSMIT THRESHOLD	48
FIGURE 88: PORT ERRORS SCREEN FOR MODULE 3	49
FIGURE 89: SET MAX RECEIVE THRESHOLD	49
FIGURE 90: SET MAX TRANSMIT THRESHOLD	50
FIGURE 91: PORT ERRORS SCREEN FOR MODULE 3	50
FIGURE 92: FRONT VIEW OF M1GMSF	50
FIGURE 93: SLOT 3 STATUS SCREEN.....	51
FIGURE 94: PORT UTILIZATION MODULE SCREEN	51
FIGURE 95: SET MAX RECEIVE THRESHOLD	52
FIGURE 96: SET MAX TRANSMIT THRESHOLD	52
FIGURE 97: PORT ERRORS MODULE SCREEN.....	53
FIGURE 98: SET MAX TRANSMIT THRESHOLD	53
FIGURE 99: FRONT VIEW OF M1GSCF.....	54
FIGURE 100: SLOT 1 STATUS SCREEN	54
FIGURE 101: SLOT 2 MONITOR SPEED CONFIGURATION SCREEN.....	54
FIGURE 102: MONITOR SP. CONF.	55
FIGURE 103: RESTORE DEFAULTS SCREEN.....	55
FIGURE 104: PORT UTILIZATION MODULE SCREEN FOR MODULE 1	55
FIGURE 105: SET MAX RECEIVE THRESHOLD	56
FIGURE 106: SET MAX TRANSMIT THRESHOLD	56
FIGURE 107: PORT ERRORS SCREEN FOR MODULE 3	57

FIGURE 108: SET MAX TRANSMIT THRESHOLD	57
FIGURE 109: FRONT VIEW OF M1GSSF	58
FIGURE 110: NETWORK PORT SPEED CONFIGURATION	58
FIGURE 111: PORT UTILIZATION MODULE SCREEN FOR MODULE 3	59
FIGURE 112: SET MAX RECEIVE THRESHOLD	59
FIGURE 113: SET MAX TRANSMIT THRESHOLD	60
FIGURE 114: PORT ERRORS MODULE SCREEN.....	60
FIGURE 115: SET MAX RECEIVE THRESHOLD	61
FIGURE 116: SET MAX TRANSMIT THRESHOLD	62
FIGURE 117: PORT ERRORS SCREEN FOR MODULE 3	62
FIGURE 118: SET MAX TRANSMIT THRESHOLD	63
FIGURE 119: TAP CONTROL M1G2ACE CHASSIS.....	63
FIGURE 120: ROW 1 FILTERS SCREEN	63
FIGURE 121: EDIT FILTER SCREEN	64
FIGURE 122: CHANGING THE FILTER NAME	64
FIGURE 123: FILTER HAS A NEW NAME	64
FIGURE 124: SELECT INGRESS PORT(S) SCREEN AND FIGURE 125: INGRESS PORT(S) SELECTED	65
FIGURE 126: SELECT EGRESS PORT (S) SCREEN AND FIGURE 127: EGRESS PORT(S) SELECTED	65
FIGURE 128: BACK TO EDIT FILTER SCREEN	65
FIGURE 129: ROW 1 FILTERS SCREEN	66
FIGURE 130: ROW 1 FILTERS SCREEN	66
FIGURE 131: ROW 1 FILTERS SCREEN WITH CASE 432A IN PROGRESS.....	66
FIGURE 132: ROW 1 FILTERS SCREEN WITH NEW FILTER IN 1 ST POSITION.....	67
FIGURE 133: NEW FILTER NAME 'CASE 432A DMAC'	67
FIGURE 134: FILTER ON DESTINATION MAC ADDRESS	67
FIGURE 135: ENTER THE DESTINATION MAC ADDRESS (IN HEX).....	68
FIGURE 136: EDIT FILTER SCREEN SHOWING INVALID CHARACTER ENTERED	68
FIGURE 137: THE DESTINATION MAC IS ENTERED.....	68
FIGURE 138: THE DESTINATION MAC IS ENTERED.....	68
FIGURE 139: BACK TO THE ROW 1 FILTERS SCREEN	69
FIGURE 140: THE CASE 432A DMAC IS SAVED	69
FIGURE 141: THE NEW FILTER HAS A NAME.....	69
FIGURE 142: SELECT INGRESS PORT(S) SCREEN AND FIGURE 143: INGRESS PORT(S) SELECTED	70
FIGURE 144: SELECT EGRESS PORT(S) SCREEN AND FIGURE 145: EGRESS PORT(S) SELECTED	70
FIGURE 146: INGRESS AND EGRESS PORTS DEFINED.....	70
FIGURE 147: CREATING VLAN ID.....	70
FIGURE 148: VLAN ID CREATED	71
FIGURE 149: FILTER CASE432A IS NOW IN FIRST POSITION	71
FIGURE 150: FILTER CASE 432A IS NOW IN FIRST POSITION	71
FIGURE 151: NEW FILTER SRC IP FLTA	72
FIGURE 152: THE SOURCE IP ADDRESS AND MASK IS SET	72
FIGURE 153: SAVE THE SOURCE IP FILTER	72
FIGURE 154: DSCP=21 IS NAMED AND SET TO BE DEFINED	73
FIGURE 155: SAVE THE DSCP=21 FILTER.....	73
FIGURE 156: FILTER DSCP=21 IS SAVED	73
FIGURE 157: <i>FILTER ICMP FILTER IS ALMOST DONE</i>	74
FIGURE 158: FILTER ICMP FILTER IS COMPLETE	74
FIGURE 159: FILTER ICMP FILTER IS READY TO BE SAVED	75
FIGURE 160: NOW HAVE 6 FILTERS COMPLETED	75
FIGURE 161: THE 'EMAIL SEND' IS COMPLETE.....	76
FIGURE 162: THE FILTERS ARE READY TO BE SAVED.....	76
FIGURE 163: THE 'EMAIL SEND' FILTER IS NOW COMPLETE.....	77
FIGURE 164: MAIN MENU SCREEN	77
FIGURE 165: SELECT SLOT NUMBER TO VIEW/MODIFY SCREEN	78

FIGURE 166: SLOT 1 STATUS SCREEN	78
FIGURE 167: HELP SCREEN FOR THE FILTERING MENU	82
FIGURE 168: SERIAL CABLE PINOUT.....	83

1. Introduction

1.1 Purpose

Garland Technology **Packet Broker System (PBS)** is a flexible Network Access System made up of a chassis designed to fit into a standard 19" rack. The chassis comes in two sizes, 1U and 2U. The 1U chassis can receive up to 4 Garland Technology TAP modules. The 2U chassis can receive up to 12 GT TAP modules. Both of Packet Broker Chassis are equipped with dual internal AC or DC power supply units. The System can be managed remotely.

This document describes, in detail, how the chassis and TAP modules can be set up to access your critical network links, aggregate and filter at layers 2, 3 and 4 if required before distributing the traffic out to your monitoring tools and appliances.

1.2 Scope

The scope of this document is limited to Garland Technology Packet Broker System release **M1GXXCE_v1.0.50**. It shows you how to access all the different menus and navigate through the various sections of the program to allow you to set up the functionality of the various TAPs that can be installed into the chassis.

1.3 General Information

The M1GXX CE Filtering Backplane Chassis and the Series M1GXX F Modular TAPs is a Scalable Modular Network Access and Traffic Distribution System for 10Mbps, 100Mbps and 1000Mbps Networks, commonly referred to as a 'Packet Broker System'.

The Garland Technology 1Gbps Packet Broker System (PBS) provides access to a network's 10Mbps, 100Mbps and 1000 Mbps traffic by aggregating copper or fiber links together and sending the aggregated traffic out to multiple network Analysis, Monitoring and/or Security Appliances. The PBS can also filter out the traffic that the tools and appliances have no interest in, to avoid over subscribing the monitoring ports.

The Chassis can receive up to 4 or 12 1Gbps Modules depending on whether the chassis is a 1U chassis or a 2U chassis. Both chassis are equipped with dual internal power supplies for either AC or DC power sources.

The M1GXX CE chassis can be used with all the Garland Technology 1Gbps Modular TAP series. The new M1GXX F series as well as all the legacy TAP series that were developed before this Packet Broker system was released in early 2016. If you have Garland Technology Modules purchased before the GT PBS was released they will operate as they normally did in the chassis they are currently in, by updating their firmware. There is a RJ-45 Serial Management port that allows access to the Command Line Interface (CLI) and an Ethernet RJ-45 Management port, so the Chassis can be connected to the network for remote management once you set up the network configuration.

1.4 M1GXX F TAP Series

The M1GXX F TAP series were designed to take advantage of the 1Gbps Packet Broker system aggregating backplane. These Filtering TAPs allow filtering of the traffic going through them at layers 2, 3 and 4. Because of the backplane built into the M1G1XX CE chassis, not only can you filter the traffic, but you can aggregate the traffic from 1, 2, 3 or 4 TAPs. Various filters can be applied to the network traffic and the results can be routed to any of the monitor ports of the filtering TAPs in the row of the chassis.

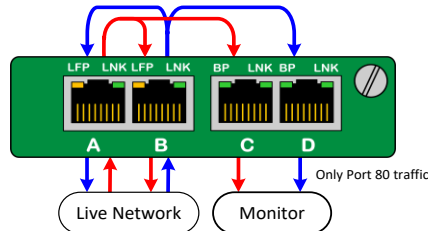


Figure 1: Filter TAP Passing Port 80 Traffic

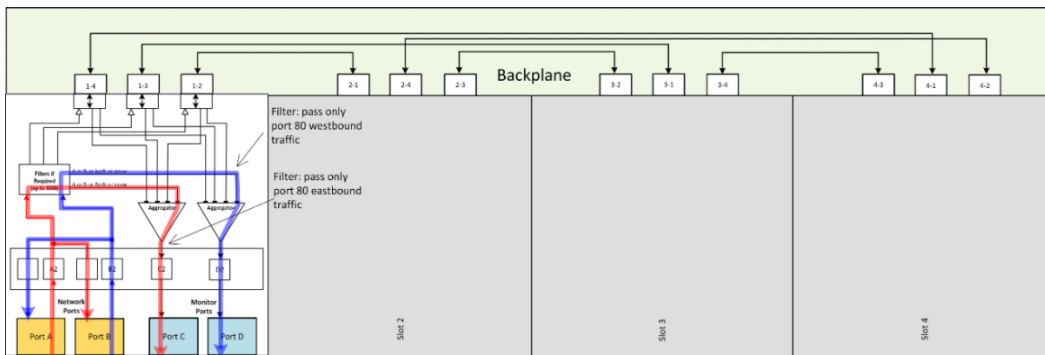


Figure 2: Filter TAP Flow Diagram Port 80 Traffic

1.4.1 Setting up the Filter TAP to operate as a Legacy TAP

The Filter TAPs can be set up to filter on layers 2, 3 and 4 to allow your tools and appliances to only see the traffic that they have an interest in. These TAPs can also be set up to breakout the network traffic to the monitor ports, aggregate the network traffic to the monitor ports and replicate SPAN traffic out to up to 3 different monitor tools just like our legacy TAPs can.

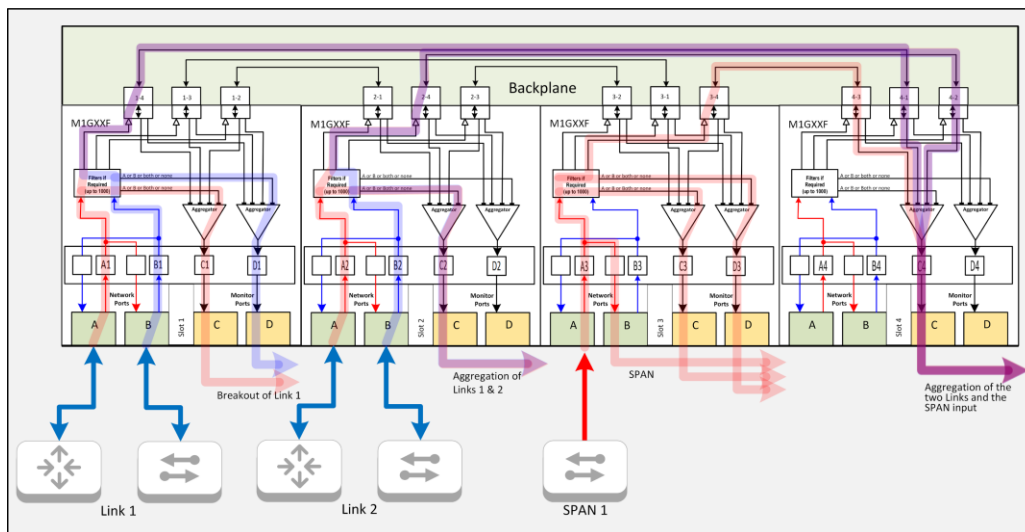


Figure 3: Flow diagram for Breakout, Aggregation & SPAN Mode

1.4.2 Traffic flow for Breakout TAP mode

Slot 1 in Figure 3 above, is showing the traffic flow for the Breakout TAP mode. To set up the TAP to breakout the traffic you would create a filter that will instruct all the ingress eastbound traffic from ingress port 'A1' to go to egress port 'C1'. Next, instruct all the ingress westbound traffic from ingress port 'B1' to go to the egress port 'D1'. Now the TAP will operate like a Breakout TAP sending all the ingress eastbound traffic out to egress port 'C1' and all the ingress westbound traffic out to egress port 'D1'.

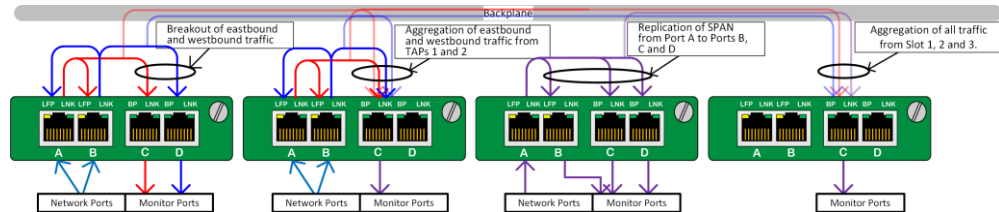


Figure 4: TAP 1 flow for Breakout Mode on M1GXXF TAP series

1.4.3 Traffic flow for Aggregation Mode

Slot 2 in figure 4 page 10, is showing the traffic flow for the Breakout mode. To set up the TAP to aggregate the traffic coming in to the TAP in Slot 2, you would instruct all the ingress traffic coming in to ingress port 'A2' to go to egress Port 'C2'. Next, instruct all the traffic coming into ingress port 'B2' to go to egress port 'C2'. Next, instruct all the Eastbound traffic from Slot 1 TAP port 'A1' to slot 2 port 'C2' and all the westbound traffic from slot 1 port 'B1' to slot 2 port 'C2'. Now all the traffic from slot 1 and from slot 2 will be directed to the Egress port 'C2' on slot 2.

1.4.4 Traffic flow for SPAN mode

Slot 3 in figure 4 above, is showing the traffic flow for the SPAN mode. To set up the TAP to replicate the SPAN traffic that ingresses on port A, out to ports B, C and D, you would instruct all the ingress traffic from ingress port 'A3' to go to port 'C3' and to port 'D3'. All the traffic from 'A3' will automatically go to port 'B3'. Now all the ingress traffic from port 'A3' will go to ports 'B3', 'C3' and 'D3'.

1.4.5 Direct and aggregate all the traffic on slots 1, 2, and 3 out to slot 4

If we wanted to direct all the ingress traffic on slots 1, 2 and 3 out to a single port on slot 4, we can instruct the all ingress traffic on port 'A1' and 'B1' on slot 1 to go to egress port 'C4' on slot 4., next all the ingress traffic on port 'A2' and 'B2' on slot 2 to go to egress port 'C4' on slot 4 and finally, all the ingress traffic on port 'A3' on slot 3 to go to egress port 'C4' on slot 4. Now all the ingress traffic from TAPs 1, 2 and 3 will be aggregated to egress out on port 'C4'. If there is more traffic than the egress port 'C4' can handle (more than 1Gbps), you can add filters to only allow the traffic that the monitor tool/s are interested in. Like only allowing port 80 traffic or conversely allowing everything except port 80 to go to port 'C4'.

As we have shown in this chapter, the M1GXX F Series of TAPs can function like our legacy TAPs except for our Bypass TAP. Plus, this series of TAPs also has the filtering feature which allows you to eliminate any traffic that the monitoring tools have no interest. The other big feature is to allow traffic of more than one link to be aggregated together using the chassis backplane.

1.5 Legacy TAPs

Network test access points (TAPs) are a hardware tool that allows you to monitor your network.

Aggregation mode is used to capture full duplex network traffic. In aggregation mode, the bidirectional traffic on the network ports is aggregated and routed to the monitor ports.

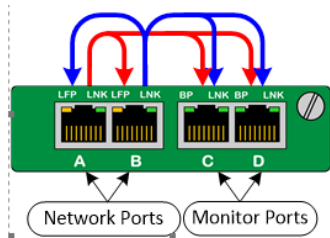


Figure 5: Aggregation Mode Traffic Flow

Breakout Mode is used when each direction on the network port needs to be analyzed separately. Each network port incoming traffic is mirrored to a different monitor port.

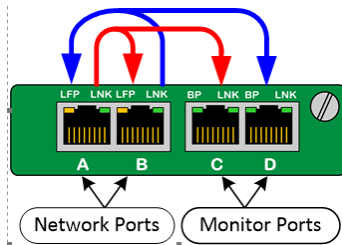


Figure 6: Breakout Mode Traffic Flow

SPAN Mode is used when the TAP is not used inline, but has already been tapped. The single network port is mirrored to the three remaining monitor ports.

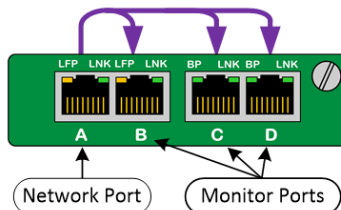


Figure 7: SPAN Mode Traffic Flow

Bypass Mode is useful when placing Inline Appliances in to the network. The monitor ports are placed inline in the network. A heartbeat protects the network by bypassing the monitor device in the event of failure.

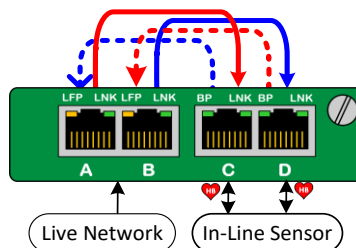


Figure 8: Bypass TAP Normal Mode (inline)

When the Bypass TAP is in the normal mode, it is routing the network traffic through the Inline appliance. If the inline appliance were to go offline for any reason, the TAP will bypass the appliance and reconnect the critical link until the appliance is placed back online.

The TAP does this by sending a Heartbeat packet out to the inline appliance and if the inline appliance is on-line, it will send the heartbeat packet back to the TAP. If the HB packet is not returned to the TAP, it is an indication that the appliance is off-line for some reason. TAP will bypass the appliance but keep the link up.

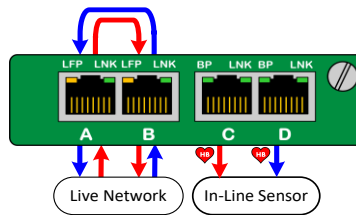


Figure 9: Bypass TAP Bypass Mode (Bypass)

2. Installation

To Deploy the M1GXX CE Modular Chassis with Filtering Backplane into the network, the following steps apply:

- Carefully un-pack the chassis and install it into a 19" equipment rack.
- The model M1G1XCE will require 1U of rack space and the model M1G2XCE will require 2U of rack space.
- You will need 2 AC or DC connections to apply power to the two internal power supplies, depending on whether the AC or the DC configuration was purchased.
- Now insert your Garland Technology Modular TAPs by carefully sliding them into the available slots in the chassis.
- If you are installing F Series Modules, you will need to connect to the Chassis Management port to set up the type of Filtering you require for your application.
- If you are installing legacy modules you will be able to manage them through the management port as you would in the standard Managed Chassis (for A series modules or BP series modules) or by setting up the DIP switches located on the Module's logic board.
- Connect a power cable to each of the M1GXXCE power supplies and plug them into an available power source. Garland Technology recommends plugging the cables in to different power sources in case one should fail the other may not.



Figure 10: Blanking Plate

Note: Do not leave module slots uncovered on the chassis. Install a Blanking Plate on any unused slot so that proper internal air circulation is maintained.

3. Features

Design your own 1G chassis (1U or 2U) with modular TAPs that support breakout, aggregation, filtering, regeneration/SPAN and bypass modes. This modular system allows you to fully deploy and manage your analysis, monitoring and security appliances.

- **Scalable Modular TAPs System:**

- 2U chassis holds up to 12 TAPs - backplane filtering between TAPs within a row (there are three rows of 4 TAPs).
- 1U holds up to 4 TAPs - backplane filtering between TAPs.

- **Management and Non-Management options:**

- Remote management of the Packet Broker System is provided through the Management Card. The serial port provided local access to the PBS so that the network parameters can be set up locally. Once this is accomplished, the PBS can be accessed remotely through the Ethernet port.
- A non-management chassis is available (management card can be added at later date)

- **Syslog Reporting:**

- Significant events reported via syslog

- **Snmp Management:**

- configuration and event traps available via snmp

- **Port Mapping:**

- filter allows granular selection of network traffic at layers 2, 3 and 4 of the packet to provide monitoring tools only to the traffic they are designed (or intended) to inspect.

- **Port Utilization:**

- Records and displays network and monitor port packet counts, percent utilization, max utilization
- Allows user to set max utilization on receive or transmit which sends a syslog and/or snmp trap when surpassed

- **Multi-Tier Filtering Supports:**

- Layer 2, 3 and 4 Filtering (MAC, VLAN, IP, DSCP, TCP, UDP)

- **Dual internal AC or DC power supplies**

- **TAP modules are hot swappable, fully configurable and interchangeable**

- **Accommodates GT legacy modular TAPs**

- **Network Failsafe:**

- recognizes power outages and automatically closes the relay circuitry in less than 8 milliseconds then, reconnects the two network devices connected to Ports A & B.

- **Supports jumbo frames and passes physical errors.**

- **Packet Slicing and Packet Injection:**

- when in aggregate mode on copper network port TAPs

- **Import/Export Configuration**

- Allows the user to Export/Import the Chassis and Module configuration

- **Password Policy**

- Allows the administrator to specify the complexity of a user's password.

- **Made, tested and certified in USA**

4. Front View

Front View of the 1U and 2U Modular Packet Broker System. The 1U Packet Broker System has four modular TAP S lots and 1 Management Module Slot. The 2U Packet Broker System has twelve modular TAP S lots and one Management Module Slot. The modules can be any of the Modular 10Mbps, 100Mbps or 1Gbps TAP s.

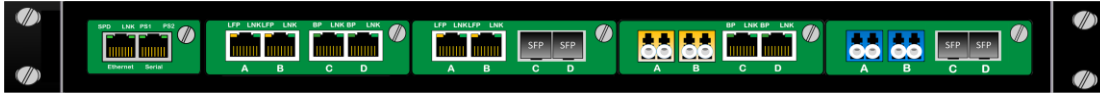


Figure 11: Front View 1U Packet Broker System

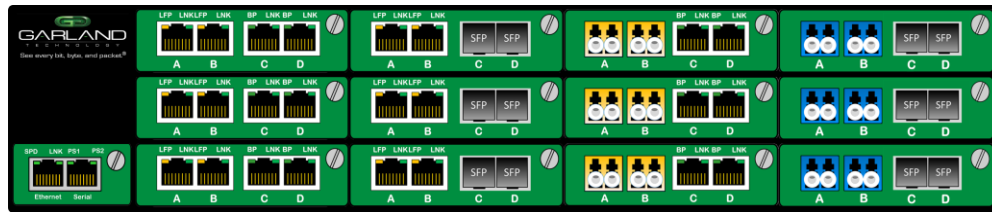


Figure 12: Front View 2U Packet Broker System



Figure 13: 1U Chassis Row and Slot Information

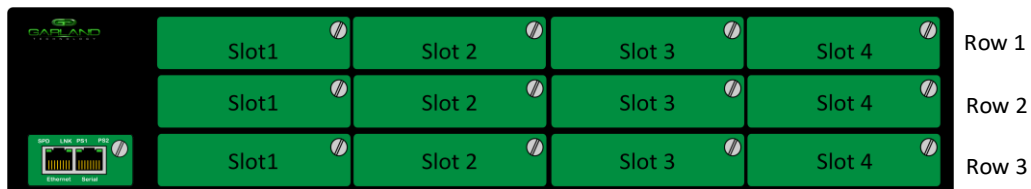


Figure 14: 2U Chassis Row and Slot Information

5. Rear View

Rear View of the 1U and 2U 1Gbps Packet Broker System



Figure 15: Rear View 1U Packet Broker System with AC Power Supplies

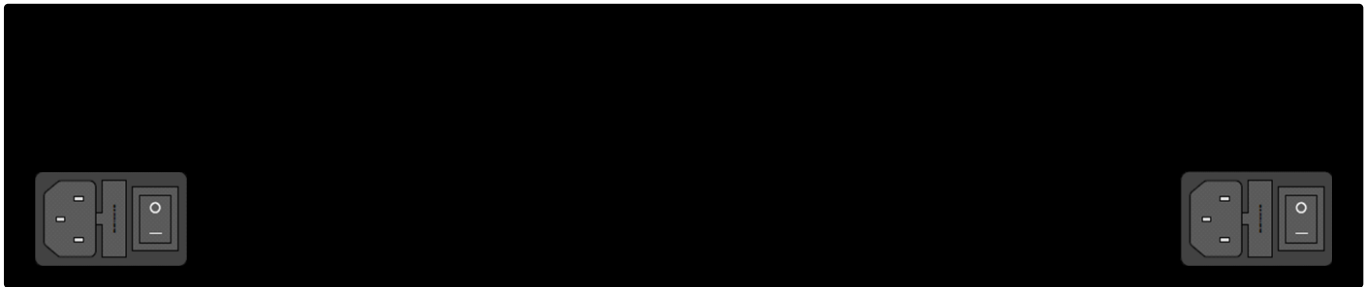


Figure 16: Rear View 2U Packet Broker System with AC Power Supplies

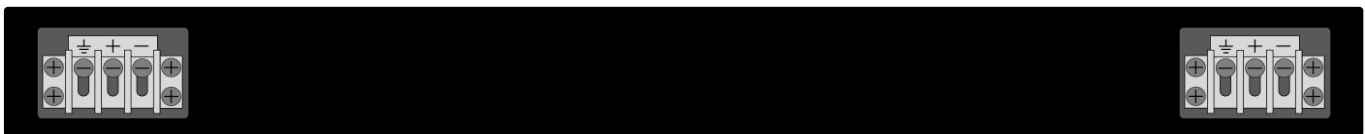


Figure 17: Rear View 1U Packet Broker System with DC Power Supplies

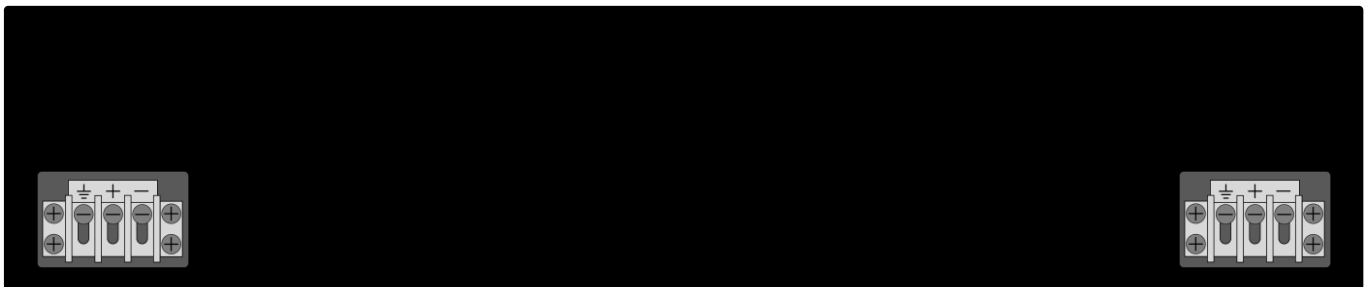


Figure 18: Rear View 1U Packet Broker System with DC Power Supplies

6. Administration

You will need to change the network IP address . To do this, you will need to connect to the serial management port, so you can set up the Network parameters, using the furnished RS 232 to DB 9 cable;

1. Connect the RJ45 end to the RJ45 Serial Port on the M1GXX CE chassis.
2. Connect the other side of the RS 232 cable to your PC's RS 232 port.
3. Use any terminal emulation software (PuTTY, HyperTerminal, Etc.) to connect to the CLI interface to manage the M1GXX CE chassis.
4. Set up the following terminal communication parameters on the terminal emulation software:

Speed:	115200 -default
Data Bits:	8
Parity:	none
Stop Bits:	1
Flow Control:	No flow control
5. Power up the M1GXX CE chassis
6. The Login prompt will appear in the terminal window
7. Enter the default Login name (**admin**)
8. Enter the default password (**gtadmin1**)

CAUTION: AT THIS POINT IT IS HIGHLY RECOMMENDED THAT YOU MODIFY THE DEFAULT ADMINISTRATOR USERNAME AND PASSWORD BY SELECTING ITEM 3 IN FIGURE 19.

Following the above procedure will log you into the PBS and bring up the Main Menu.

```
Garland Technology M1G1ACE (Code Version: 1.0.50)

Main Menu

Select:

1. Change/View Module Configuration
2. Filtering
3. Username/Password
4. Settings
5. Users
0. Logout
Select: █
```

Figure 19: Main Menu

From the Main Menu, **press '4'** to get to the Settings Menu.

```
Garland Technology M1G1ACE

Settings Menu

1. NetworkConfig
2. Key Press Timeout
3. NTP setup
4. Time Zone setup
5. Date & Time setup
6. syslog Setup
7. snmp Setup
8. System reboot
0. Exit
Select: █
```

Figure 20: Settings Menu

6.1 Network Configuration

After logging in, go to the Network Configuration menu on the Settings Menu if you plan to use the management Ethernet port, set up IP address, net mask and gateway parameters. The default IP address is **10.10.10.200** and the Network mask is **255.255.255.0** and the Gateway **10.10.10.1**.

Press '1' to bring up the Network Configuration Menu to set up the proper network addresses to allow the Packet Broker to operate in its local environment.

```
Garland Technology M1G1ACE

Network Configuration
Warning: This session depends on the current network config.
        Applying network config may drop this session.
link: up
current ip add:10.10.10.200
current config:static add: 10.10.10.200 mask:255.255.255.0 gwy:10.10.10.1
new config:static add: 10.10.10.200 mask:255.255.255.0 gwy:10.10.10.1
  1.re-init interface
  3.ip address
  4.netmask
  5.gateway
  6.dns1
  7.dns2
  8.ping
  0.exit with new config
ctrl-c.exit with NO new config
select:
```

Figure 21: Network Configuration Menu

Once you enter the network settings, **pressing '0'** will exit back to the settings menu with the new configuration.

While we are on the Settings Menu, we can finish setting up the Key Press Timeout, Date and Time setup, and the Syslog setup.

6.2 Key Press Timeout

The Management portal of the Packet Broker is designed to log off after 5 minutes (default setting) of no activity (no key press). The Key Press Timeout Menu allows changing the timeout from 1 to 60 minutes.

Press '2' on the Settings Menu to bring up the Key Press Timeout Menu to change the Timeout Setting.

```
Garland Technology M1G1ACE

Key press timeout Menu

current timeout: 50 minutes.
ctrl-c to exit menu with no change.
Enter a value between 1-60 (minutes) :
```

Figure 22: Key Press Timeout Menu

Type in the new timeout period and **press <enter>** to return to the **'Settings Menu'**.

6.3 NTP Setup

From the Settings menu, **press '3'** to get to the **'NTP Setup Menu'**.

```
Garland Technology  M1G1ACE

NTP Setup Menu

current NTP configuraton: OFF
    new NTP configuraton: OFF
1. ntp ON
0. Exit
Select: █
```

Figure 23: NTP OFF Setup Menu

Setting the Network Time Protocol (NTP) is handled from the setup screen. **Press '1'** to turn 'NTP' on.

```
Garland Technology  M1G1ACE

NTP Setup Menu

current NTP configuraton: OFF
    new NTP configuraton: ON    ip:192.168.1.100
ping 192.168.1.100...FAIL
1. ntp OFF
2. change ip
3. use pool.ntp.org
a. apply
0. Exit
Select: █
```

Figure 24: NTP ON Setup Menu

6.4 Time Zone Menu

Press '4' to bring up the **'Time Zone Setup Menu'**.

```
Garland Technology  M1G1ACE

Time Zone Setup Menu

current time zone: America/Chicago
    new time zone: America/Chicago
1. Africa
2. America
3. Asia
4. Australia
5. GMT+-x
6. Europe
7. Pacific
0. Exit
Select: █
```

Figure 25: Time Zone Setup Menu

6.5 Date & Time Setup

The Date & Time Setup Menu provides you the ability to set up the date, time, and year for your chassis. These menus are self-explanatory. After you finish setting up the Date and Time information on this menu, **Press '0'** to return to the Settings Menu.

```
Garland Technology M1G1ACE
Date & Time Setup Menu
current date/time: 11/5/2016 20:16
new date/time: 11/5/2016 20:16
1. Change month
2. Change day of month
3. Change year
4. Change hour
5. Change minute
0. Exit
Select:
```

Figure 26: Date & Time Setup Menu Timeout Menu

6.6 Syslog Configuration Menu

Syslog is a standard for Message logging. Syslog is a way for network devices to send event messages to a logging server – usually known as a Syslog server. The Syslog protocol is supported by a wide range of devices and can be used to log different types of events.

For example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events.

Press '6' on the Settings Menu to bring up the Syslog Configuration Menu

```
Garland Technology M1G1ACE
Syslog Configuration Menu
current syslog setting: OFF
new syslog setting: OFF
1. turn syslog ON
0. Exit
Select:
```

Figure 27: Syslog Configuration Menu

Press '1' to turn Syslog 'ON'

```
Garland Technology M1G1ACE
Syslog Configuration Menu
current syslog setting: OFF
new syslog setting: ON ip:192.168.1.100 UDP:514
ping 192.168.1.100...FAIL
1. turn syslog OFF
2. turn unit identifier ON
3. send test syslog
4. change ip
5. use TCP
6. change port
a. apply changes
0. Exit
Select:
```

Figure 28: Syslog Config Menu Turned 'ON'

When Sy slog is **ON** the Syslog Menu lets you;

1. Turn Sy slog ON or OFF
2. Turn Un it Identifier ON or OFF
3. Send a Test Syslog
4. Change the ip Address

Once you have Sy slog set the way you want it, **press ‘a’** to apply the changes then **press ‘0’** to **‘EXIT’** and return to the **‘Settings Menu’**.

6.6.1 What is Syslog?

Syslog is a way for network devices to send event messages to a logging server – usually known as a Syslog server. The Syslog protocol is supported by a wide range of devices and can be used to log different types of events.

Syslog is a way for network devices to send event messages to a logging server – usually known as a Syslog server.

The Syslog protocol is supported by a wide range of devices and can be used to log different types of events.

For example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events. The following is a list of events that Syslog can report on for the GT Packet Broker System

6.6.2 What will Syslog Report on?

Syslog will send an event message on the following condition changes:

-System Startup	When the System comes up after a Power Up cycle or software upgrade.
-Module enters Bypass Mode	Bypass TAP Module enters bypass mode.
-Module enters In-line Mode	Bypass TAP enters In-Line Mode
-Module Link Down	a Module's Network or Monitor port has lost Link.
-Module Link Up	a Module's Network or Monitor port has linked up.
-New Module detected	a new module has been detected on the Backplane.
-Module no longer present	a module has been unplugged.
-Power Supply Down	Power Supply A or B has gone down.
-Both Supplies Up	Both Supplies now up.
-System Software Upgrade	A system software is being installed.
-Module Software Upgrade	A Module software is being installed.
-User Login	User has logged in.
-User Logout	User has logged out.
-Port receive traffic exceeded max	Receive traffic on a port went over configured max.
-Port xmit traffic exceeded max	Transmit traffic on a port went over configured max.
-Intermodule traffic rec exceeded max	Inter-module traffic went over configured max.
-Intermodule traffic xmit exceeded max	Inter-module traffic went over configured max.
- NTP configuration has been changed	NTP Configuration has changed
- Filter configuration has been changed	Filter Configuration has changed
- Module configuration has been changed	Module Configuration has changed
- Port Utilization threshold has been changed	Port Utilization Threshold has changed
- SNMP configuration has been changed	SNMP Configuration has changed
- Date and Time config has been changed	Date & Time Config has changed
- Time Zone config has been changed	Time Zone configuration has changed
- A user has been added	A user was added
- A user has been deleted	A user was deleted
- A user's privilege has been changed	A user's privilege was changed
- A user had a login failure	A user's login failed

6.7 snmp Configuration Menu

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

```
Garland Technology M1G1ACE

snmp Configuration Menu

current:
off
    new:
    off
1. turn snmp ON
0. Exit
Select:
```

Figure 29: snmp Configuration Menu

Use SNMP management software to monitor any network device on which you install SNMP agent software. The SNMP agent interacts with third-party SNMP management software to enable the sharing of network status information between monitored devices and applications and the SNMP management system that monitors them. If you make any changes remember to **press 'a'** to apply them before leaving this screen.

```
Garland Technology M1G1ACE

snmp Configuration Menu

current:
off
    new:
V2c community:public    port:161    ip:127.0.0.1    :162
ping 127.0.0.1...PASS
1. turn snmp OFF
2. send test snmp trap
3. change trap ip
4. change trap port
5. change access port
7. V2c community password
8. V2c readwrite
9. V2c readonly
a. apply changes
0. Exit
Select:
```

Figure 30: snmp Configuration Menu 'New setup'

Press '0' to go back to the Settings Menu, **Press '8'** if you want to execute a **'System Reboot'** else **press '0'** again to return to the **'Main Menu'**.

6.7.1 What will snmp Report on?

Snmp will send an event message on the following condition changes:

-System Startup	When the System comes up after a Power Up cycle or software upgrade.
-Module enters Bypass Mode	Bypass TAP Module enters bypass mode.
-Module enters In-line Mode	Bypass TAP enters In-Line Mode
-Module Link Down	a Module's Network or Monitor port has lost Link.
-Module Link Up	a Module's Network or Monitor port has linked up.
-New Module detected	a new module has been detected on the Backplane.
-Module no longer present	a module has been unplugged.
-Power Supply Down	Power Supply A or B has gone down.
-Both Supplies Up	Both Supplies now up.

-System Software Upgrade

a system software is being installed.

-Module Software Upgrade

a Module software is being installed.

-User login

User has logged in.

-User logout

User has logged out.

-Port receive traffic exceeded max

Receive traffic on a port went over configured max.

-Port xmit traffic exceeded max

Transmit traffic on a port went over configured max.

-Intermodule traffic rec exceeded max

Inter-module traffic went over configured max.

-Intermodule traffic xmit exceeded max

Inter-module traffic went over configured max.

6.8 Back to the Main Menu

```
Garland Technology M1G1ACE (Code Version: 1.0.50)

Main Menu

Select:

1. Change/View Module Configuration
2. Filtering
3. Username/Password
4. Settings
5. Users
0. Logout
Select:█
```

Figure 31: Main Menu Screen

6.9 Setting up the Users

The last area of the **PBS** that needs to be set up is the User section where we assign who has access to what sections of the Packet Broker's administration.

Selecting '5' on the Main Menu Screen will show the '**User Administration**' menu. This menu will only be seen by the ADMIN. The assigned Users will see only the menus that are applicable to their privileges (see Users Help Menu).

```
Garland Technology M1G1ACE

User Administration

Select:

1. Add User
2. Delete User
3. Change Password
4. Change Privilege
5. Password Policy
0. Return█
```

Figure 32: User Administration Menu

There are up to 20 users and one ADMIN that can be assigned to manage the M1GXX CE chassis. The ADMIN has full privilege to all operations. **Press '1'** to add a new User.

```
Garland Technology M1G1ACE

Add User Menu

new user name:user. privilege:OPERATOR.
Select:

1. Change Username
2. Change privilege to operator.
3. Change privilege to logger.
4. Change privilege to bypass.
h. Help.
x. Abort and Return
0. Apply Return█
```

Figure 33: Add User Menu

6.9.1 User ADMIN

There is only one administrator per PBS. The ADMIN can create or delete a USER. To create a User, the ADMIN will log into the Packet Broker and assign a USERNAME and PASSWORD for the USER. For example, the assigned username is 'samhill'. So, the assigned password will also be 'samhill' (in this process the Password is the same as the Username. The user can change his username and password after he logs in for the first time, making sure he observes the rules in the 'Add User Help Menu'.

6.9.2 User OPERATOR

The operator user can change/view module configuration, manage the creating or deleting of filters. The operators cannot add or delete Users.

6.9.3 User LOGGER

The logger user has the ability to manage whatever is happening in Syslog and SNMP.

6.9.4 User BYPASS

The BYPASS user has the ability to view module configurations and filters of and the managing the bypass function of the Bypass TAP modules that are installed into the chassis.

6.9.5 Password Policy

Password policy allows the administrator to specify the complexity of a user password. It also allows the administrator to specify that the user to be locked out for an amount of time after a number of consecutive failed login attempts.

```
Garland Technology M1G1ACE
Password Policy

      min low  up spec      fail lock
      len case case chars  digits atts time hist
orig:   6   1   0   0       0   3   20   0
new:    6   1   0   0       0   3   20   0
1. Change minimum length(6-20)
2. Change required number of lower case characters
3. Change required number of upper case characters
4. Change required number of special characters
5. Change required number of digits
6. Change number failed login attempts before account locked(1-10)
7. Change number of minutes account is locked after max fail attempts(20-1440)
8. Change number of last passwords to disallow(0-20)
0. Exit Menu
Select: 1
```

Figure 34: Set Password Policy Screen

6.9.6 The 'Add User' Help Menu for setting up Users

Press 'h' to bring up the 'Add User Help Menu'. This menu will explain the operator privileges.
Press any key to return to the 'Add User Menu'.

```
Garland Technology M1G1ACE
Add User Menu Help
This menu allows the ADMIN to add users.
usernames may be up to 20 lower case alphanumeric characters
as well as the characters '.', '_', or '-',
The first character should be a lower case alpha character (a-z)
Privileges can be one of the following three selections:
OPERATOR...view and modify module config and filters.
LOGGER....change syslog config and SNMP config.
BYPASS....view module config and filters, change bypass config.

Press any key to return to the add user menu.
```

Figure 35: Add User Help Menu

Now that the chassis is set up the way you want it to be, you can exit the serial connection and log back into the chassis using an ethernet cable.

7. Web Interface Login

The 1G Packet Broker System administrator may choose to configure and manage devices via web or graphical user interface. After setting the management port's IP address, you will then be able to access the graphical user interface using a normal web browser application. Simply browse to your devices assigned IP address and login using the credentials below, you can change the username and password to any valid Username and password.

https://<ip_addr>
Username: admin
Password: gtadmin1

Only **Firefox** and **Chrome** browsers are supported.

7.1 Configuring the installed Modules

A successful Login will open the following screen.

This screen indicates that you are connected to a 1U Chassis and that there is a management card, two M1GCCF TAPs in slots one and two, Slot three has a M1GCCBP TAP and there is a M1GCCA TAP in slot 4. From this menu you will be able to configure the modules that are installed in the chassis one at a time if you are signed in as the Administrator.

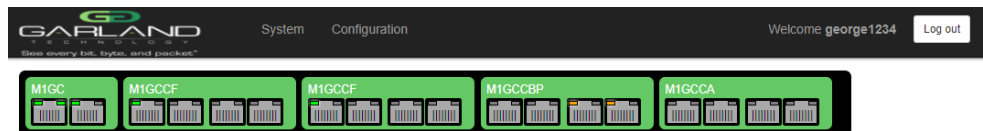


Figure 36: System Menu, 1 U chassis

This is what the screen might look like if we were logging into a 2 U chassis depending on the installed modules.



Figure 37: System Menu, 2 U chassis

The different modules have their own unique configuration menus. Clicking on Slot 1 or Slot 2 of the 1U chassis will bring up the configuration menu for the filtering Module M1GCCF.

From this menu, you can configure the module's;

Network Speed	Autonegotiate	1G
	Autonegotiate	100M
	Autonegotiate	10M
	Forced Gig Full Duplex	
	Forced 100M Full Duplex	
	Forced 10M Full Duplex	
	Synchronize	
Monitor Speed	1G	
	100M	

LFP On or Off NO
YES

This is Module 1 of the 1U chassis we are connected to. If we were connected to slot 12 of the 2U chassis the screenshot would look like Figure 39 on page 27 below.

GARLAND System Configuration Welcome george1234 Log out

Module 1 Configuration

M1GCCF serial number:21270012345 software version:1.2.58

Network Speed: 100M_auto
Autonegotiate 100M

Monitor Speed: 100M
100M

LFP ON: YES
YES

Port A
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port B
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port C
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port D
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 2
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 3
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 4
Receive Threshold: 100 Transmit Threshold: 100
100 100

NO CHANGE DEFAULT SAVE

Figure 38: Configuration menu for a Filter TAP

Once you have configured the module, you need to save your configuration so that you do not lose your changes.

Module 12 Configuration

M1GCCF serial number:21270012345
software version:1.2.58

Network Speed: 100M_auto
Autonegotiate 100M

Monitor Speed: 100M
100M

LFP ON: YES
YES

Port A
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port B
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port C
Receive Threshold: 100 Transmit Threshold: 100
100 100

Port D
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 2
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 3
Receive Threshold: 100 Transmit Threshold: 100
100 100

to/from module 4
Receive Threshold: 100 Transmit Threshold: 100
100 100

NO CHANGE DEFAULT SAVE

Figure 39: Configuration menu for a Filter TAP

Always remember, that if you reconfigure a module, you need to press save to retain the changes. After you save your changes, press **'System'** to return to the System configuration menu.

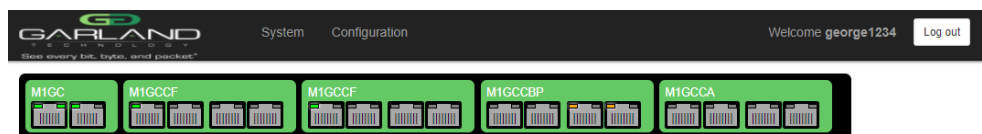



Figure 40: System Menu

Clicking on Slot 3 of the 1U chassis will bring up the 'M1GCCBP' TAP's configuration Menu. From this menu, you can set up the Bypass TAP's;

Operating Mode	Aggregate Mode
	Breakout Mode
	SPAN Mode
	Bypass Mode
Speed	1Gig
	100M


LFP On or OFF	No Yes
Forced Bypass	NO YES
Reverse Bypass	No Yes



[System](#)
[Configuration](#)

Welcome **george1234**
[Log out](#)

Module 3 Configuration



serial number:2076-0012345
software version:1.1.1

Operating Mode: bypass

aggregate

Speed: 1G

1G

LFP ON: YES

YES

Packet Injection Port C: NO

NO

Packet Injection Port D: NO

NO

Packet Slicing: NO

NO

NO CHANGE

DEFAULT

SAVE

Figure 41: Module 3 Configuration Menu

Once you have configured the module, you need to save your configuration.

Clicking on S lot 4 of the 1 U chassis will bring up the 'M1G CCA ' TAP's configuration Menu. From this menu you can set up the Aggregating TAP's;

Operating Mode	Aggregate Mode
	Breakout Mode
	SPAN Mode
Speed	1Gig
	100M
Packet Injection Port C:	NO
	YES
Packet Injection Port D:	NO
	YES

The screenshot shows the 'Module 4 Configuration' page. At the top, there's a header with the Garland logo and navigation links for 'System' and 'Configuration'. A welcome message 'Welcome george1234' and a 'Log out' button are on the right. The main content area is titled 'Module 4 Configuration' and features a green icon for 'M1GCCA' with its serial number (2076-0033662) and software version (1.1.1). Below this, several configuration options are listed with dropdown menus: 'Operating Mode' (set to 'aggregate'), 'Speed' (set to '1G'), 'LFP ON' (set to 'YES'), 'Packet Injection Port C' (set to 'NO'), 'Packet Injection Port D' (set to 'NO'), and 'Packet Slicing' (set to 'NO'). At the bottom, there are three buttons: 'NO CHANGE' (grey), 'DEFAULT' (red), and 'SAVE' (green).

Figure 42: Module 4 Configuration Menu

Once you have configured the module, you need to save your configuration.

7.2 Configuring the System

Pressing '**Configuration**' will bring up the System Configuration screen. Here you will see the System Information and be able to configure **Syslog**, **SNMP**, **Export Configuration**, **Import Configuration** and do a **Software Upgrade**.

The screenshot shows the 'System Configuration' page. It has a similar header to Figure 42. On the left, there's a sidebar menu with links: 'System Info', 'Syslog', 'Snmp', 'Export Configuration', 'Import Configuration', and 'Software Upgrade'. The main content area is titled 'System Information' and displays the following details: 'chassisModel: M1G1ACE', 'chassisSerial: 21870020100', and 'swVersion: 1.0.50j'.

Figure 43: System Configuration Menu

7.2.1 Syslog Configuration

Selecting '**Syslog**' will bring up the Syslog Configuration screen to turn Syslog on or off and/or configure Syslog

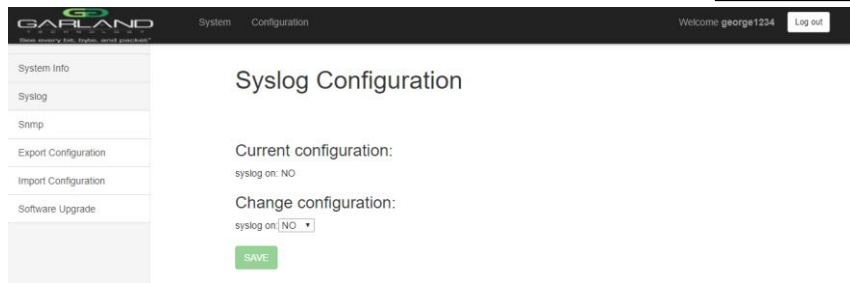


Figure 44: Syslog Configuration Menu

7.2.2 snmp Configuration

Selecting **‘Snmp’** allows you to turn snmp on or off and to set snmp configuration the way you want.

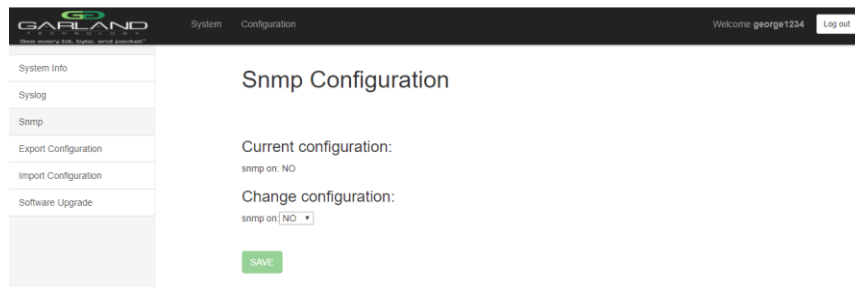


Figure 45: snmp Configuration Menu

7.2.3 Export Configuration

Selecting **‘Export Configuration’** allows you to export your configuration so you do not have to recreate it in the future.

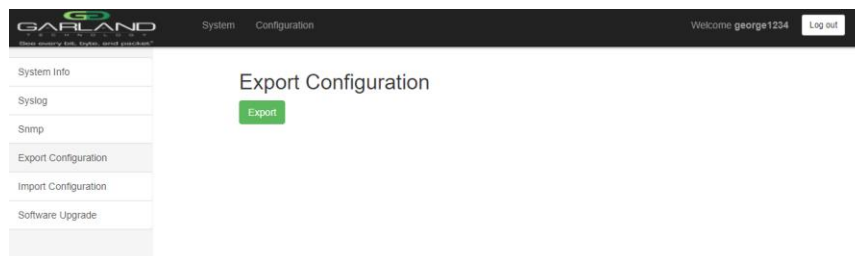


Figure 46: Export Configuration Menu

7.2.4 Import Configuration

Selecting **‘Import Configuration’** allows you to import a configuration

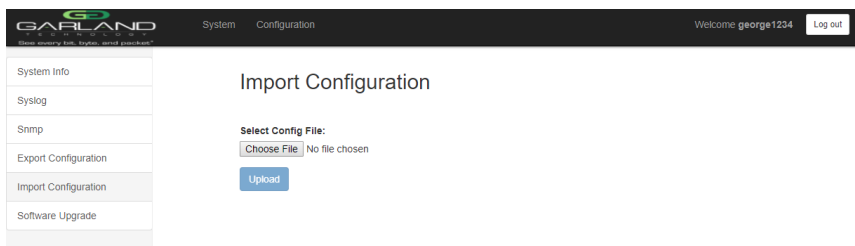


Figure 47: Import Configuration Menu

7.2.5 Update Firmware

Selecting 'Update Firmware' provides the ability to upgrade your firmware in the event of a new firmware release.

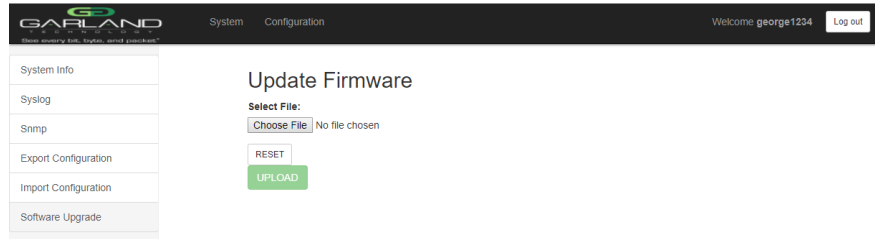


Figure 48: Import Configuration Menu

Remember only the Administrator has access to all of the PBS system. The other users ;

Operator

Logger

Bypass

have access to the PBS system as outlined in the 'Add User' menu, Figure 35 located on page 24.

8 M1GXX F Module Series

The M1GXX F module series was designed to take advantage of the features designed into the M1GXX CE chassis. Once the M1GXX F modules are installed into the chassis you will need to log into the chassis and configure the module to perform the task that you need them to do.

As we learned when we were setting up the administration section of the Packet Broker System, the first menu to come up after the log in procedure is the Main Menu.

```
Garland Technology M1G1ACE (Code Version: 1.0.50)

Main Menu

Select:

1. Change/View Module Configuration
2. Filtering
3. Username/Password
4. Settings
5. Users
0. Logout
Select: █
```

Figure 49: Main Menu

From the Main Menu Screen, **press '1'** to bring up the **'Select the slot number to view/modify'** screen to view and/or modify the TAP modules that are installed in the chassis.

```
Select slot number to view/modify
Chassis Serial Number: 21870020242 Controller Serial Number: 21910020238

Power Supply 1: Up
Power Supply 2: Down

# Module Type
Operating Mode (Current State)
-----
1: M1GCCF          2: M1GCCBP          3: M1GMSA          4: M1GCCA
                   Bypass(Bypass)      Aggregate Mode      SPAN Mode

Press
1: Select Slot 1   2: Select Slot 2   3: Select Slot 3   4: Select Slot 4
0: Exit
█
```

Figure 50: Select the slot number to view/modify screen.

This screen will provide information about the Packet Broker chassis like the serial number of the chassis, the serial number of the management controller, if one is present, and the model number of the modules that are installed. In the case of the legacy modules, the TAP mode the module is currently set in.

Next **press '1'** to bring up the **'Slot 1 Status'** screen where a **M1GCCF** module is installed. This screen will show how the module is currently set and provide you the selections you need to change the speed, the duplex mode, the LFP mode, restore the default settings of the modules or see the Port Utilization screens. The features on the screens will vary depending on the type of modules are plugged into the slots. Once you get to the screen pertinent to each type of module, the status screen is pretty much self-explanatory.

```
Slot 1 Status:
=====
Link State:  Port A  Port B  Port C  Port D
Speed:       1G     1G     1G     1G
Duplex:      Full   Full   Full   Full
Media Type:  RJ45   RJ45   RJ45   RJ45
Serial Number: 21270020400
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 1 Select Option:
=====
Press
1: Set Network Ports Speed(Autonegotiate 1G)
2: Set Monitor Ports Speed(Forced Gbit Full Duplex)
3: Set LFP Mode(ON)
0: Restore Defaults
c: Port Utilization
Press 'Enter' to refresh this status screen
0: Exit
```

Figure 51: Slot 1 Status Screen for the M1GCCF

For example, there is a legacy Bypass TAP module in slot 2 of the PBS, the screen that would come up when you **press '2'** would reflect the features of the M1GCC BP TAP module with their current settings.

```

=====
Slot 2 Status:
=====
Current Bypass State: Forced

Link State:      Port A      Port B      Port C      Port D
Duplex:          Auto       Auto       Auto       Auto
Media Type:      RJ45       RJ45       RJ45       RJ45
Serial Number:   2076-0000102
=====
Slot 2 Select Option:
=====
Press
1: Set Operating Mode (Bypass)
2: Set Speed(1G)
3: Set LFP Mode (ON)
4: Set Duplex Mode
5: Set Reverse Bypass Mode (OFF)
6: Set Forced Bypass Mode (ON)
b: Restore Defaults
Press Enter to refresh this status screen
0. Exit
  
```

Figure 52: Slot 2 Status Screen for the M1GCC BP

8.1 TAP Modules Descriptions

In this section, we will show you the description for each TAP in the M1GXX F modular TAP series. They all do basically the same functions and when the TAPs are inserted into the PBS chassis, the combination of the TAP Modules and the PBS chassis provides a whole new level of traffic manipulation. The modules provide filtering and aggregating capabilities and the PBS lets you aggregate the traffic from the links attached to the modules before sending it out to the monitoring tools and appliances, so you can use fewer ports on your monitoring devices.

The M1GXX F Module Group is made up of the following Modules.

1. M1GCC F Copper network ports to copper monitor ports
2. M1GCS F Copper network ports to SFP monitor ports
3. M1G MCF Multi-mode fiber network ports to copper monitor ports
4. M1G MSF Multi-mode fiber network ports to SFP monitor ports
5. M1GSC F Single-mode fiber network ports to copper monitor ports
6. M1GSS F Single-mode fiber network ports to SFP monitor ports

8.1.1 M1GCCF Module

10/100/1000Mbps Filtering TAP Module with Link Speed Synchronization: Two (2) Copper 10/100/1000Mbps RJ-45 Network Ports and two (2) Copper 10/100/1000Mbps RJ-45 Monitoring Ports.

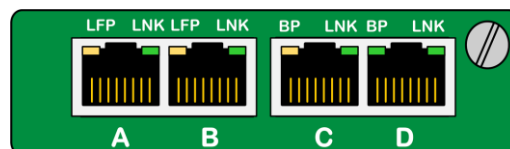


Figure 53: Front View of M1GCCF

This TAP can operate at 10Mbps, 100Mbps or 1000Mbps network speeds. The copper monitor ports can operate at 100Mbps or 1000Mbps speeds.

8.1.2 M1GCCF Configuration

8.1.2.1 Slot '1' Status screen

Press '1' to bring up the **'Slot 1 Status'** screen. This screen will provide the status of the M1GCCF module that is installed in Slot 1 of row 1 of the chassis. In this case, the link state of all the ports is 'Up'. The speed of all the links is 1Gbps Autonegotiate. The Duplex is set for 'Full'. This screen also provides you with the serial number of the module and the software version that is installed.

```

=====
Slot 1 Status:
=====
Link State:      Port A      Port B      Port C      Port D
Speed:           1G          1G          1G          1G
Duplex:          Full       Full       Full       Full
Media Type:      RJ45       RJ45       RJ45       RJ45
Serial Number:   21270020400
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 1 Select Option:
=====
Press
1: Set Network Ports Speed(Autonegotiate 1G)
2: Set Monitor Ports Speed(Forced Gbit Full Duplex)
3: Set LFP Mode(ON)
b: Restore Defaults
c: Port Utilization
Press 'Enter' to refresh this status screen
0. Exit

```

Figure 54: Slot 1 Status screen

8.1.2.2 Network Port Speed Config.

Pressing '1' will allow you to change the Network port speed (currently set for Autonegotiate 1G). There are seven different ways that you can set the speed of the network ports that have copper media. Once you set up the speed that you want, **press '0'** to return to the **'Slot 1 Status screen'** and apply the changes.

```

=====
Slot 1 Network Speed Configuration
=====
Original Network speed: Autonegotiate 1G
New Network speed: Autonegotiate 1G
1: Autonegotiate 1G
2: Autonegotiate 100M
3: Autonegotiate 10M
4: Forced Gbit Full Duplex
5: Forced 100 Mbit Full Duplex
6: Forced 10 Mbit Full Duplex
7: Synchronize
0. Return and Apply

```

Figure 55: Network Port Speed Configuration

8.1.2.3 Monitor Port Speed Config.

On the Slot 1 Status Screen, **pressing '2'** will allow you to change the Monitor ports speed (currently set for 'Forced Gbit Full Duplex'). **Press '0'** to return to the **Slot 1 Status screen** and apply any changes you made.

```

=====
Slot 1 Monitor Speed Configuration
=====
Original Monitor speed: Forced Gbit Full Duplex
New Monitor speed: Forced Gbit Full Duplex
1: 1G
2: 100M
0. Return and Apply

```

Figure 56: Monitor Port Speed Configuration

8.1.2.4 LFP Mode Configuration.

On the Slot 1 Status Screen, **pressing '3'** will allow you to change the **'LFP'** mode (currently set for 'LFP ON').

```
=====
Slot 1 LFP Mode Configuration
=====

Current LFP state: ON
New LFP state: ON

1. ON
2. OFF

0. Return and Apply
```

Figure 57: LFP Mode Configuration

LFP is used mostly for High Availability (HA) designed networks. When turned on, it will sense a network failure and reflect the failure to the adjacent port of the live network allowing the network's failover mechanism to switch over to the secondary network path. **Press '0'** to return and apply to the Slot 1 Status Screen.

8.1.2.5 Reset to default TAP settings.

Back on the Slot 1 Status Screen, **pressing 'b'** will bring up the **"Restore Defaults"** screen to allow you to reset the TAP module to its default values.

```
Slot 1 Restore Defaults
=====

1. Restore defaults
0. Exit without restore
```

Figure 58: Restore Defaults Screen

8.1.2.6 Port Utilization Module screen.

Pressing 'c' will bring up the "Port Utilization Module 1" screen to allow you to see port utilization. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane stats.

Port Utilization Module 1				
	PORT A	PORT B	PORT C	PORT D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
select:				

Figure 59: Port Utilization Module Screen for Module 1

8.1.2.7 Set Max Receive threshold.

From the Port Utilization Module Screen **press '1'** to **'set max receive threshold'**. This will place a **'1'** on the select line at the bottom left of the screen and add a new line that is **'Port (A-D)'**. Select which port that you want to set for the max receive threshold.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:1				
Port (A-D):				

Figure 60: Set max receive threshold Tab

For example, we will set the max receive threshold for Port A to 53%. When we **press 'a'**, a new line will be inserted at the bottom of the screen **'Enter new max receive threshold (0-100):'**. This is where we enter **53** and **press 'ENTER'**. Now, whenever the traffic exceeds 53% on **'Port A'** of **module 1**, a syslog and/or snmp trap to be sent.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:1				
Port (A-D):a				
Enter new max receive threshold(0-100):53				

Figure 61: Set Port A max receive threshold to 53%

8.1.2.8 Set Max Transmit Threshold.

From the Port Utilization Module Screen **press '2'** to **'set max transmit threshold'**. This will place a **'2'** on the select line at the bottom left of the screen and add a new line that is **'Port (A-D):'**. Select which port that you want to set for the max transmit threshold.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	90%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

Select:2
Port (A-D):█

Figure 62: Set max transmit threshold

For example, we will set the max transmit threshold for Port C to 90%. When we **press 'c'**, a new line will be inserted at the bottom of the screen **'Enter new max transmit threshold (0-100):'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Port C'** of **module 1**, a syslog and/or snmp trap will be sent.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	90%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

Select:2
Port (A-D):c
Enter new max transmit threshold(0-100):90 █

Figure 63: Set max transmit threshold to 90%

8.1.2.9 Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **'xmt/rcv max util counters'**.

8.1.2.10 Error Menu screen.

Next, **pressing '5'** will bring up the **'Port Errors module screen'** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module.

This screen gives you the option to clear the errors. **Press '0'** to return to the **Port Utilization Module screen**.

```
Garland Technology  M1G1ACE

Port Errors Module 1

      crc          Port A      Port B      Port C      Port D
      frame        0          0          0          0
      jabber        0          0          0          0
      undersize     0          0          0          0
      oversize      0          0          0          0
      fragments     0          0          0          0
      rcv overrun   0          0          0          0

      1.clear errors
      0.exit

select:█
```

Figure 64: Port Errors Module 1 Backplane.

The last thing we can review on the Port Utilization Modules screen is the traffic that goes from module 1 to the modules 2, 3 and 4 via the Backplane. **Press '6'** to bring up the **Port Utilization Module** for the Backplane.

8.1.2.11 Setting Backplane Max Receive Threshold

To set the max receive threshold, **press '1'** this will add a **'1'** on the **select:** line at the bottom left side of the screen and add the line **'bp port (0-2):'**. **Pressing '2'** will let you set the **column 1** receive threshold, **pressing '1'** will let you set the **column 2** receive threshold, and **pressing '0'** will let you set the **column 3** receive threshold.

```
Port Utilization Module 1

      Module 1      Module 3      Module 4
      rcv bytes      0          0          0
      xmt bytes      0          0          0
      rcv packets    0          0          0
      xmt packets    0          0          0
      rcv util       0%        0%        0%
      xmt util       0%        0%        0%
      rcv max util   0%        0%        0%
      xmt max util   0%        0%        0%
      rcv threshold  0%        0%        90%
      xmt threshold  0%        0%        0%

      1.set max receive threshold
      2.set max transmit threshold
      3.clear counts
      4.clear max util
      5.error menu
      6.backplane
      0.exit

Select:1
Port (0-2):0
Enter new max receive threshold (0-100):90 █
```

Figure 65: Set max receive threshold

8.1.2.12 Setting Backplane Max Transmit Threshold

To set the max transmit threshold, **press '2'** this will add a **'2'** on the **select:** line at the bottom left side of the screen and add the line **'bp port (0-2):'**. **Pressing '2'** will let you set the **column 1** transmit threshold, **pressing '1'** will let you set the **column 2** transmit threshold, and **pressing '0'** will let you set the **column 3** transmit threshold.

```

Port Utilization Module 1
      Module 1      Module 3      Module 4
rcv bytes      0      0      0
xmt bytes      0      0      0
rcv packets    0      0      0
xmt packets    0      0      0
rcv util       0%     0%     0%
xmt util       0%     0%     0%
rcv max util   0%     0%     0%
xmt max util   0%     0%     0%
rcv threshold  0%     0%     90%
xmt threshold  0%     0%     0%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

Select:2
Port (0-2):0
Enter new max receive threshold (0-100):90
  
```

Figure 66: Set max transmit threshold

8.1.2.13 Backplane Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and pressing '4' will clear the **xmt/rcv max util counters**.

8.1.2.14 Backplane Error Menu screen.

Next, pressing '5' will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. Press '0' to return to the '**Port Utilization Module**' screen.

```

Garland Technology M1G1ACE

Port Errors Module 1
      PORT A      PORT B      PORT C      PORT D
      crc         0         0         0         0
      frame       0         0         0         0
      jabber      0         0         0         0
      undersize   0         0         0         0
      oversize    0         0         0         0
      fragments   0         0         0         0
      rcv overrun 0         0         0         0

1.clear errors
0.exit

select:
  
```

Figure 67: Port Errors Modules Screen

Thresholds for intermodule (or backplane) ports work just like the thresholds for the module ports. If traffic exceeds threshold settings, a syslog and/or snmp event will be issued.

8.1.3 M1GCS F Module

10/100/1000 Mbps Filtering TAP Module with Link Speed Synchronization: Two (2) Copper 10/100/1000 Mbps RJ 45 Network Ports with two (2) SFP Gigabit Monitoring Ports.

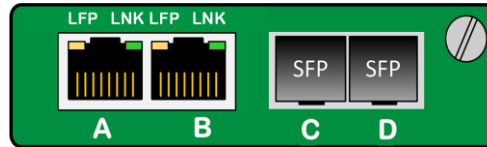


Figure 68: Front View of M1GCS F

The Copper to SFP Modules can operate at 10Mbps, 100Mbps or 1000Mbps speeds on the network ports and 1Gbps on the Monitor ports.

8.1.4 M1GCS F Configuration

Once you have selected the Slot that has the M1GCS F module that you want to configure (in this case, the M1GCS F TAP we want to configure is in Slot 2).

8.1.4.1 Slot '1' Status Screen

Press '1' to bring up the **'Slot 1 Status'** screen. This screen will provide the status of the M1GCS F module that is installed in Slot 1 of row 1 of the chassis. In this case, the link state of all the ports is 'Up'. The speed of all the links is 1Gbps Autonegotiate. The Duplex is set for 'Full'. This screen also provides you with the serial number of the module and the software version that is installed.

```

=====
Slot 1 Status:
=====
Link State:  Port A   Port B   Port C   Port D
Speed:       1G      1G      1G      1G
Duplex:      Full    Full    Full    Full
Media Type:  RJ45    RJ45    RJ45    RJ45
Serial Number: 21270020400
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 1 Select Option:
=====
Press
1: Set Network Ports Speed(Autonegotiate 1G)
2: Set Monitor Ports Speed(Forced Gbit Full Duplex)
3: Set LFP Mode(ON)
h: Restore Defaults
c: Port Utilization
Press 'Enter' to refresh this status screen
0. Exit

```

Figure 69: Slot 1 status screen

8.1.4.2 Network Port Speed Screen

Pressing '1' will allow you to change the Network port speed (currently set for Autonegotiate 1G). There are seven different ways that you can set the speed of the network ports that have copper media. Once you set it up as you want, **press '0'** to return to the Slot 1 Status screen and apply the changes.

```

=====
Slot 1 Network Speed Configuration
=====
Original Network speed: Autonegotiate 1G
New Network speed: Autonegotiate 1G
1: Autonegotiate 1G
2: Autonegotiate 100M
3: Autonegotiate 10M
4: Forced Gbit Full Duplex
5: Forced 100 Mbit Full Duplex
6: Forced 10 Mbit Full Duplex
7: Synchronize
0. Return and Apply

```

Figure 70: Network Port Speed Configuration

8.1.4.3 Monitor Port Speed Screen

The speed of the SFP's cannot be changed from 1G.

```
=====
Slot 1 Monitor Speed Configuration
=====

Original Monitor speed: Forced Gbit Full Duplex
New Monitor speed: Forced Gbit Full Duplex
1: 1G
2: 100M
0. Return and Apply
```

Figure 71: Monitor Port Speed Configuration

8.1.4.4 LFP Mode Configuration.

On the Slot 1 Status Screen, **pressing '3'** will allow you to change the **'LFP'** mode (currently set for 'LFP ON').

```
=====
Slot 1 LFP Mode Configuration
=====

Current LFP state: ON
New LFP state: ON

1. ON
2. OFF
0. Return and Apply
```

Figure 72: LFP Mode Configuration

LFP is used mostly for High Availability (HA) designed networks. When turned on, it can sense a network failure and reflect the failure to the adjacent port of the live network allowing the network's failover mechanism to switch over to the secondary network path. **Press '0'** to apply and return to the **Slot 1 Status Screen**.

8.1.4.5 Port Utilization Modules screen.

Pressing 'c' will bring up the "Port Utilization Module 1" screen to allow you to see port utilization and number of packets. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane stats.

```
Port Utilization Module 1

PORT A          PORT B          PORT C          PORT D
xmt packets      0              0              0              0
rcv packets      0              0              0              0
xmt bytes        0              0              0              0
rcv bytes        0              0              0              0
xmt util         0%            0%            0%            0%
xmt max util     0%            0%            0%            0%
xmt threshold    100%          100%          100%          100%
rcv util         0%            0%            0%            0%
rcv max util     0%            0%            0%            0%
rcv threshold    100%          100%          100%          100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

select:
```

Figure 73: Port Utilization Module Screen for Module 1

8.1.4.6 Reset to default TAP settings.

Back on the Slot 1 Status Screen, **pressing 'b'** will bring up the **"Restore Defaults" screen** to allow you to reset the TAP module to its default values.

```
=====
Slot 1 Restore Defaults
=====

1. Restore defaults
0. Exit without restore
```

Figure 74: Restore Defaults Screen

8.1.4.7 Set Max Receive threshold.

From the Port Utilization Module Screen **press '1'** to **'set max receive threshold'**. This will place a **'1'** on the select line at the bottom of the screen and add a new line that is **'Port (A-D)'**. Select which port that you want to set for the max receive threshold.

```
Port Utilization Module 1
      Port A      Port B      Port C      Port D
xmt packets      0          0          0          0
rcv packets      0          0          0          0
xmt bytes        0          0          0          0
rcv bytes        0          0          0          0
xmt util         0%         0%         0%         0%
xmt max util     0%         0%         0%         0%
xmt threshold    100%      100%      100%      100%
rcv util         0%         0%         0%         0%
rcv max util     0%         0%         0%         0%
rcv threshold    100%      100%      100%      100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

Select:1
Port (A-D):
```

Figure 75: Set max receive threshold

For example, setting the max utilization threshold for Port A receive to 53%, will cause a syslog and/or snmp trap to be sent if the receive traffic on port A exceeds 53%.

8.1.4.8 Set Max Transmit Thres hold.

From the P ort Utilization Module S creen **press '2'** to set max trans mit thres hold. This will place a **'2'** on the s elect line at the bottom of the s creen which will add a new line that is **'Port (A-D):'**. Select the port that you want to set. For ex ample, we want to set the max trans mit thres hold for P ort C to 90%. When we **press 'c'**, a new line will be inserted at the bottom of the s creen **'Enter new max transmit threshold (0-100):'**. This is where we enter **'90'** and **press 'ENTER'**. No w, whenever the traffic exceeds 90% on **'Port C'**, a s yslog and/or s nmp trap will be sent.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold				
2.set max transmit threshold				
3.clear counts				
4.clear max util				
5.error menu				
6.backplane				
0.exit				
Select:2				
Port (A-D):				

Figure 76: Se t max transmit threshold

8.1.4.9 Clear C ounts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **xmt/rcv max util counters**.

8.1.4.10 Error Menu s creen.

Next, **pressing '5'** will bring up the **Port Errors module screen** where you can get a re port on the various errors that may have occurred while m onitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. **Press '0'** to return to the **'Port Utilization Module' screen**.

Garland Technology M1G1ACE				
Port Errors Module 1				
	PORT A	PORT B	PORT C	PORT D
crc	0	0	0	0
frame	0	0	0	0
jabber	0	0	0	0
undersize	0	0	0	0
oversize	0	0	0	0
fragments	0	0	0	0
rcv overrun	0	0	0	0
1.clear errors				
0.exit				
select:				

Figure 77: Port Erro rs Modules Sc reen

8.1.4.11 Backplane.

The last thing we can review on the Port Utilization Module screen is the traffic that goes from module 1 to the modules 2, 3 and 4 via the Backplane. **Press '6'** to bring up the **Port Utilization Module** for the Backplane.

8.1.4.12 Setting Backplane Max Receive Threshold

To set the max receive threshold, **press '1'** this will add a **'1'** on the **select:** line at the bottom left side of the screen and add the line **'bp port (0-2):'**. **Pressing '2'** will let you set the **column 1** receive threshold, **pressing '1'** will let you set the **column 2** receive threshold, and **pressing '0'** will let you set the **column 3** receive threshold.

Port Utilization Module 2			
	Module 1	Module 3	Module 4
rcv bytes	0	0	0
xmt bytes	0	0	0
rcv packets	0	0	0
xmt packets	0	0	0
rcv util	0%	0%	0%
xmt util	0%	0%	0%
rcv max util	0%	0%	0%
xmt max util	0%	0%	0%
rcv threshold	0%	0%	90%
xmt threshold	0%	0%	0%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit			
Select:1			
Port (0-2):2			
Enter new max receive threshold (0-100):53			

Figure 78: Set max receive threshold

8.1.4.13 Setting Backplane Max Transmit Threshold

To set the max transmit threshold, **press '2'** this will add a **'2'** on the **select:** line at the bottom left side of the screen and add the line **'bp port (0-2):'**. **Pressing '2'** will let you set the **column 1** transmit threshold, **pressing '1'** will let you set the **column 2** transmit threshold, and **pressing '0'** will let you set the **column 3** transmit threshold.

Port Utilization Module 2			
	Module 1	Module 3	Module 4
rcv bytes	0	0	0
xmt bytes	0	0	0
rcv packets	0	0	0
xmt packets	0	0	0
rcv util	0%	0%	0%
xmt util	0%	0%	0%
rcv max util	0%	0%	0%
xmt max util	0%	0%	0%
rcv threshold	0%	0%	90%
xmt threshold	0%	0%	0%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit			
Select:1			
Port (0-2):2			
Enter new max receive threshold (0-100):53			

Figure 79: Set max transmit threshold

8.1.4.14 Backplane Clear Co unts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **xmt/rcv max util counters**.

8.1.4.15 Backplane Error Menu screen.

Next, **pressing '5'** will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. **Press '0'** to return to the **'Port Utilization Module' screen**.

```
Garland Technology M1G1ACE

Port Errors Module 1

      PORT A      PORT B      PORT C      PORT D
      crc         0         0         0         0
      frame       0         0         0         0
      jabber      0         0         0         0
      undersize   0         0         0         0
      oversize    0         0         0         0
      fragments   0         0         0         0
      rcv overrun 0         0         0         0

      1.clear errors
      0.exit

select:█
```

Figure 80: Port Errors Modules Screen

Thresholds for intermodule (or backplane) ports work just like the thresholds for the module ports. If traffic exceeds threshold settings, a syslog and/or snmp event will be issued.

8.1.5 M1GMCF Module

1000Mbps Filtering TAP Module: Two (2) Multi-Mode Passive Fiber LC Network Ports with two (2) Copper 1000M RJ-45 Monitoring Ports.

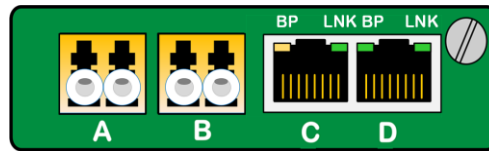


Figure 81: Front View of M1G MCF

The Multi-Mode 1G bps Fiber Network ports to 1G bps Copper Monitor Port Modules can operate at 1000Mbps speeds. Allows you to convert the Multi-Mode network media to connect to Copper Monitoring tools.

8.1.6 M1GMCF Configuration

Once you have selected the Slot that has the M1G MCF module that you want to configure (in this case the M1G MCF TAP we want to configure is in Slot 2).

```
=====
Slot 2 Status:
=====
Link State:  Port A      Port B      Port C      Port D
Speed:       1G         1G         1G         1G
Duplex:      Full       Full       Full       Full
Media Type:  MMF        MMF        RJ45       RJ45
Serial Number: 21270020410
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 2 Select Option:
=====
Press
TAPs with Fiber Network ports have network ports set to 1Gps
2. Set Monitor Ports Speed (Forced Gbit Full Duplex)
TAPs with Fiber Network ports always have LFP ON.
b: Restore Default TAP settings
c: Port Utilization
Press Enter to refresh this Status screen
0. Exit
```

Figure 82: Slot 2 Status screen

8.1.6.1 Slot '2' Status screen

Press '2' to bring up the 'Slot 2' Status's screen for the M1G MCF module. This screen will provide the status of the module that is installed in 'Slot 2' of row 1 of the chassis. The link state of all the ports is 'Up'. The speed of all the links is '1Gbps'. The Duplex is set for 'Full'. As it states on the Slot 3 Status screen, TAPs with Fiber Network Ports have their ports fixed at 1G bps. This screen also provides you with the serial number of the module and the software version that is installed. The Because the Monitor ports' media is copper, you can set the monitor ports' speed to 1G bps, Full Duplex or 100Mbps Autonegotiate.

8.1.6.2 Monitor Speed Configuration

Pressing '2' to bring up the Slot 2 Monitor Speed Configuration screen. **Pressing '1'** will set the monitor ports to Forced Gbit Full Duplex and **Pressing '2'** will set monitor ports to Autonegotiate 100Mbps. **Press '0'** to apply and Return.

```
=====
Slot 3 Monitor Speed Configuration
=====

Original Monitor speed: Forced Gbit Full Duplex
New Monitor speed: Forced Gbit Full Duplex
1: 1G
2: 100M
0. Return and Apply
```

Figure 83: Monitor Sp . Co nf.

8.1.6.3 Restore Default TAP settings

Back on the Slot 2 Status Screen, **pressing 'b'** will bring up the **"Restore Defaults"** screen to allow you to reset the TAP module to its default values.

```
=====
Slot 1 Restore Defaults
=====

1. Restore defaults
0. Exit without restore
```

Figure 84: Restore Defaults Screen

8.1.6.4 Port Utilization Module screen.

Pressing 'c' will bring up the **'Port Utilization Module 2'** screen to allow you to see port utilization and number of packets. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane stats.

```
Port Utilization Module 2

xmt packets      PORT A      PORT B      PORT C      PORT D
rcv packets      0          0          0          0
xmt bytes        0          0          0          0
rcv bytes        0          0          0          0
xmt util         0%         0%         0%         0%
xmt max util     0%         0%         0%         0%
xmt threshold    100%      100%      100%      100%
rcv util         0%         0%         0%         0%
rcv max util     0%         0%         0%         0%
rcv threshold    100%      100%      100%      100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

select:
```

Figure 85: Port Utilization Module Screen for Module 1

8.1.6.5 Set Max Receive threshold.

From the Port Utilization Module Screen **press '1'** to **'set max receive threshold'**. This will place a **'1'** on the select line at the bottom of the screen and add a new line that is **'Port (A-D):'**. Select which port that you want to set for the max receive threshold.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:1				
Port (A-D):				

Figure 86: Set max receive thres hold

For example, setting the 'set max receive thres hold' for Port A receive to 53%, will cause a syslog and/or snmp trap to be sent if the receive traffic on port A exceeds 53%. **Press 'ENTER'** to save.

8.1.6.6 Set Max Transmit Thres hold.

From the Port Utilization Module Screen **press '2'** to set max transmit threshold. This will place a **'2'** on the select line at the bottom of the screen which will add a new line that is **'Port (A-D):'**. Select the port that you want to set.

For example, we want to set the max transmit threshold for Port C to 90%. When we **press 'c'**, a new line will be inserted at the left bottom of the screen **'Enter new max transmit threshold (0-100):'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Port C'**, a syslog and/or snmp trap will be sent.

Port Utilization Module 2				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	90%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:2				
Port (A-D):c				
Enter new max transmit threshold (0-100):90				

Figure 87: Set max transmit thres hold

8.1.6.7 Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **xmt/rcv max util counters**.

8.1.6.8 Error Menu screen.

Next, **pressing '5'** will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. **Press '0'** to return to the **Port Utilization Module screen**.


```
Garland Technology M1G1ACE

Port Errors Module 1

      crc      PORT A      PORT B      PORT C      PORT D
      frame    0          0          0          0
      jabber    0          0          0          0
      undersize 0          0          0          0
      oversize  0          0          0          0
      fragments 0          0          0          0
      rcv overrun 0        0          0          0

      1.clear errors
      0.exit

select:
```

Figure 88: Port Errors screen for module 3

8.1.6.9 Backplane.

The last thing we can review on the Port Utilization Modules screen is the traffic that goes from module 1 to the modules 2, 3 and 4 via the Backplane. **Press '6'** to bring up the **Port Utilization Module** for the Backplane.

8.1.6.10 Setting Backplane Max Receive Threshold

To set the max receive threshold, **press '1'** this will add a **'1'** on the **select:** line at the bottom left side of the screen and add the line **'bp* port (0-2):'**. **Pressing '2'** will let you set the **column 1** receive threshold, **pressing '1'** will let you set the **column 2** receive threshold, and **pressing '0'** will let you set the **column 3** receive threshold.

```
Port Utilization Module 2

      Module 1      Module 3      Module 4
      rcv bytes      0          0          0
      xmt bytes      0          0          0
      rcv packets    0          0          0
      xmt packets    0          0          0
      rcv util       0%         0%         0%
      xmt util       0%         0%         0%
      rcv max util   0%         0%         0%
      xmt max util   0%         0%         0%
      rcv threshold  100%       100%       95%
      xmt threshold  100%       100%       90%

      1.set max receive threshold
      2.set max transmit threshold
      3.clear counts
      4.clear max util
      5.errors
      0.exit

select:1
bp port(0-2):0
enter new max receive threshold(0-100):95
```

Figure 89: Set max receive threshold

For example, we want to set the max receive threshold for module 4 (column 3) to 90%. When we **press '0'**, a new line will be inserted at the left bottom of the screen **'Enter new max receive threshold (0-100):'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Module 4'** backplane, a syslog and/or snmp trap will be sent.

*"bp" stands for Backplane

8.1.6.11 Setting Backplane Max Transmit Threshold

To set the max transmit threshold, **press '2'** this will add a **'2'** on the **select:** line at the bottom left side of the screen and add the line **'bp port (0-2):'**. **Pressing '2'** will let you set the **column 1** transmit threshold, **pressing '1'** will let you set the **column 2** transmit threshold, and **pressing '0'** will let you set the **column 3** transmit threshold.

```

Port Utilization Module 2

      Module 1      Module 3      Module 4
rcv bytes      0      0      0
xmt bytes      0      0      0
rcv packets    0      0      0
xmt packets    0      0      0
rcv util       0%     0%     0%
xmt util       0%     0%     0%
rcv max util   0%     0%     0%
xmt max util   0%     0%     0%
rcv threshold 100%   100%   95%
xmt threshold 100%   100%   90%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.errors
0.exit

select:2
bp port(0-2):0
enter new max transmit threshold(0-100):90

```

Figure 90: Set max transmit threshold

8.1.6.12 Clear Counts/Clear max utility on Backplane.

Pressing '3' will clear the **xmt/rcv packet counter** and pressing '4' will clear the **xmt/rcv max util counters**.

8.1.6.13 Error Menu screen for Backplane.

Next, pressing '5' will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. Press '0' to return to the **Port Utilization Module screen**.

```

Garland Technology M1G1ACE

Port Errors Module 1

      PORT A      PORT B      PORT C      PORT D
crc      0      0      0      0
frame    0      0      0      0
jabber   0      0      0      0
undersize 0      0      0      0
oversize 0      0      0      0
fragments 0      0      0      0
rcv overrun 0      0      0      0

1.clear errors
0.exit

select:

```

Figure 91: Port Errors screen for module 3

8.1.7 CM1GMSF Module

1000M Filtering TAP Module: Two (2) Multi-Mode Passive Fiber LC Network Ports with two (2) SFP Monitoring Ports.

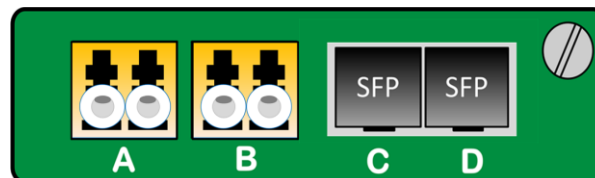


Figure 92: Front View of M1GMSF

The Multi-Mode 1G bps Fiber Network ports to 1G bps SFP Monitor Ports Modules can operate at 1000Mbps speeds. Can be used to connect to a Multi-Mode Monitoring device or convert the media from Multi-Mode Fiber to Single mode fiber.

8.1.8 M1G MS F Co nfiguration

From the Once you have sel ected the S lot that has the M1GMS F m odule that you want to configure (in this case the M1GMS F T AP we want to con figure is in S lot 3).

```
=====
Slot 3 Status:
=====
Link State:      Port A      Port B      Port C      Port D
Speed:          1G          1G          1G          1G
Duplex:         Full        Full        Full        Full
Media Type      MMF         MMF         SFP         SFP
Serial Number:   2127000000
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 3 Select Option:
=====
Press
Taps with Fiber Network ports have network ports set to 1Gbps
Taps with Fiber Monitor ports have monitor ports set to 1Gbps
Taps with Fiber Network ports always have LFP ON.
C: Port Utilization
Press 'Enter' to refresh this status screen
0. Exit
█
```

Figure 93: S lot 3 S tatus s creen

8.1.8.1 Slot '3' S tatus s creen

Press '3' to bring up the **'Slot 3'** S tatus 's screen. This screen will provide the s tatus of the M1GMS F module that is installed in S lot 3 of row 1 of the chassis. In this case, the link state of all the ports is **'Up'**. The speed of all the links is **'1Gbps'**. The Duplex is **'Full'**. This screen also provides you with the serial number of the module and the software version that is installed.

Because the network ports are fiber and the monitor ports are S F P, all the ports on the TAP will be set to 1G bps speed and the Duplex will be Full and the L F P will be set for ON.

The only thing that can be seen or changed is the **'Port Utilization'**.

8.1.8.2 Port Utilization Module s creen.

Pressing 'c' will bring up the **'Port Utilization Module 3'** screen to allow you to see port utilization and number of packets. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane s tats.

```
Port Utilization Module 3
PORT A      PORT B      PORT C      Port D
xmt packets  0          0          0          0
rcv packets  0          0          0          0
xmt bytes    0          0          0          0
xmt util     0%         0%         0%         0%
xmt max util 0%         0%         0%         0%
xmt threshold 100%      100%      100%      100%
rcv util     0%         0%         0%         0%
rcv max util 0%         0%         0%         0%
Rcv threshold 100%      100%      100%      100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

select:█
```

Figure 94: Port Utilization Module S creen

8.1.8.3 Set Max Receive threshold.

From the Port Utilization Module Screen **press '1'** to **'set max receive threshold'**. This will place a **'1'** on the select line at the bottom left of the screen and add a new line **'Port (A-D)'**. Select the port that you want to set.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:1				
Port (A-D): █				

Figure 95: Set max receive threshold

For example, setting the max utilization threshold for Port A receive to 53%, will cause a syslog and/or snmp trap to be sent if the receive traffic on port A exceeds 53%.

8.1.8.4 Set Max Transmit Threshold.

From the Port Utilization Module Screen **press '2'** to set max transmit threshold. This will place a **'2'** on the select line at the bottom of the screen which will add a new line that is **'Port (A-D)'**. Select the port that you want to set. For example, we want to set the max transmit threshold for Port C to 90%. When we **press 'c'**, a new line will be inserted at the bottom of the screen **'Enter new max transmit threshold (0-100)'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Port C'**, a syslog and/or snmp trap will be sent.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:2				
Port (A-D): █				

Figure 96: Set max transmit threshold

8.1.8.5 Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and pressing '4' will clear the **xmt/rcv max util counters**.

8.1.8.6 Port Errors Menu screen.

Pressing '5' will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. Press '0' to return to the **Port Utilization Module screen**.

```
Garland Technology M1G1ACE

Port Errors Module 3
```

	Port A	Port B	Port C	Port D
crc	0	0	0	0
frame	0	0	0	0
jabber	0	0	0	0
undersize	0	0	0	0
oversize	0	0	0	0
fragments	0	0	0	0
rcv overrun	0	0	0	0
1.clear errors				
0.exit				

Select: █

Figure 97: Port Errors Module screen

8.1.8.7 Backplane.

The last thing we can review on the Port Utilization Module screen is the traffic that goes from module 3 to the modules 1, 2 and 4 via the Backplane. Press '6' to bring up the **Port Utilization Module** for the Backplane. To set the max receive threshold, press '1' this will add a '1' on the select: line at the bottom left side of the screen and add the line **'bp port (0-2):'**. Thresholds for intermodule (or backplane) ports work just like the thresholds for the module ports. If traffic exceeds threshold settings, a syslog and/or snmp event will be issued.

```
Garland Technology M1G1ACE

Port Utilization Module 3
```

	Module 1	Module 2	Module 4
rcv bytes	0	0	0
xmt bytes	0	0	0
rcv packets	0	0	0
xmt packets	0	0	0
rcv util	0%	0%	0%
xmt util	0%	0%	0%
rcv max util	0%	0%	0%
xmt max util	0%	0%	0%
rcv threshold	95%	95%	0%
xmt threshold	95%	95%	0%
1.set max receive threshold			
2.set max transmit threshold			
3.clear counts			
4.clear max util			
5.errors			
0.exit			

select:3

Bp port(0-2): █

Figure 98: Set max transmit threshold

8.1.9 M1GSCF Module

1000M Filtering TAP Module: Two (2) Single Mode Passive Fiber LC Network Ports with two (2) Copper 1000M RJ-45 Monitoring Ports.

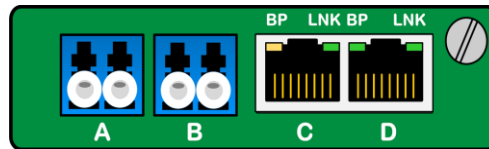


Figure 99: Front View of M1G SCF

The Single-Mode 1G bps Fiber Network ports to 1G bps Copper Monitor Port Modules can operate at 1000Mbps speeds. Allows you to convert the Single-Mode network media to connect to Copper Monitoring tools.

8.1.10 M1GSCF Configuration

The Slot that has the M1GSCF module that we want to configure is in Slot 2. It doesn't matter what slot the TAP is in, they will work the same in any slot.

```

=====
Slot 3 Status:
=====
          Port A      Port B      Port C      Port D
Link State: Up        UP          UP          UP
Speed:      1G        1G          1G          1G
Duplex:     Full      Full        Full        Full
Media Type: MMF       MMF         RJ45       RJ45
Serial Number: 21270020410
Software Version: Boot:1.2.2   App:1.2.54
=====
Slot 3 Select Option:
=====
Press
Taps with Fiber Network ports have network ports set to 1Gps
2. Set Monitor Ports Speed (Forced Gbit Full Duplex)
TAPS with Fiber Network ports always have LFP ON.
b: Restore Default TAP settings
c: Port Utilization
Press Enter to refresh this status screen
0. Exit

```

Figure 100: Slot 1 Status Screen

8.1.10.1 Slot '2' Status screen

Press '2' to bring up the 'Slot 2 Status' screen. This screen will provide the status of the M1GSCF module that is installed in Slot 2 of row 1 of the chassis. The link state of all the ports is 'Up'. The speed of all the links is 1Gbps. The Duplex is set for 'Full'. This screen also provides you with the serial number of the module and the software version that is installed.

```

=====
Slot 2 Monitor Speed Configuration
=====

Original Monitor Speed: Forced Gbit Full Duplex
New Monitor Speed: Forced Gbit Full Duplex
1: 1G
2: 100M
0: Return and apply

```

Figure 101: Slot 2 Monitor Speed Configuration screen

The Network Ports on this TAP are Fiber. The speed of fiber media is always 1Gbps.

8.1.10.2 Monitor Speed Configuration

Pressing '2' to bring up the Slot 3 Monitor Speed Configuration screen. **Pressing '1'** will set the monitor ports to Forced Gbit Full Duplex and **Pressing '2'** will set monitor ports to Autonegotiate 100Mbps. **Press '0'** to apply and Return.

```
=====
Slot 3 Monitor Speed Configuration
=====

Original Monitor speed: Forced Gbit Full Duplex
New Monitor speed: Forced Gbit Full Duplex
1: 1G
2: 100M
0. Return and Apply
```

Figure 102: Monitor S p. C onf.

8.1.10.3 Restore Default TAP settings

Back on the Slot 3 Status Screen, **pressing 'b'** will bring up the **"Restore Defaults"** screen to allow you to reset the TAP module to its default values.

```
=====
Slot 3 Restore Defaults
=====

1. Restore defaults
0. Exit without restore
```

Figure 103: Restore Defaults Screen

8.1.10.4 Port Utilization Module screen.

Pressing 'c' will bring up the "Port Utilization Module 1" screen to allow you to see port utilization and number of packets. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane stats.

```
Port Utilization Module 3

      Port A      Port B      Port C      Port D
xmt packets      0          0          0          0
rcv packets      0          0          0          0
xmt bytes        0          0          0          0
rcv bytes        0          0          0          0
xmt util         0%        0%        0%        0%
xmt max util     0%        0%        0%        0%
xmt threshold    100%     100%     100%     100%
rcv util         0%        0%        0%        0%
rcv max util     0%        0%        0%        0%
rcv threshold    100%     100%     100%     100%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.error menu
6.backplane
0.exit

Select:
```

Figure 104: Port Utilization Module Screen for Module 1

8.1.10.5 Set Max Receive threshold.

From the Port Utilization Module Screen **press '1'** to **'set max receive threshold'**. This will place a **'1'** on the select line at the bottom of the screen and add a new line that is **Port (A-D)**: so you can set the threshold.

Port Utilization Module 3				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:	1			

Figure 105: Set max receive threshold

For example, setting the 'set max receive threshold' for Port A receive to 53%, will cause a syslog and/or snmp trap to be sent if the receive traffic on port A exceeds 53%. **Press 'ENTER'** to save.

8.1.10.6 Set Max Transmit Threshold.

From the Port Utilization Module Screen **press '2'** to set max transmit threshold. This will place a **'2'** on the select line at the bottom of the screen which will add a new line that is **'Port (A-D)'**. Select the port that you want to set. For example, we want to set the max transmit threshold for Port C to 90%. When we **press 'c'** a new line will be inserted at the bottom of the screen **'Enter new max transmit threshold (0-100)'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Port C'**, a syslog and/or snmp trap will be sent.

Port Utilization Module 3				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	90%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	53%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:	2			
Port (A-D):	c			
Enter new max transmit threshold(0-100):	90			

Figure 106: Set max transmit threshold

For example, we will set the max transmit threshold for Port C to 90%. When we **press 'c'** a new line will be inserted at the bottom of the screen **'Enter new max transmit threshold (0-100):'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Port C'**, a syslog and/or snmp trap to be sent.

8.1.10.7 Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **xmt/rcv max util counters**.

```
Garland Technology M1G1ACE

Port Errors Module 1

      PORT A      PORT B      PORT C      PORT D
      crc          0          0          0          0
      frame        0          0          0          0
      jabber        0          0          0          0
      undersize     0          0          0          0
      oversize      0          0          0          0
      fragments     0          0          0          0
      rcv overrun   0          0          0          0

      1.clear errors
      0.exit

select:
```

Figure 107: Port Errors screen for module 3

8.1.10.8 Error Menu screen.

Next, **pressing '5'** will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. **Press '0'** to return to the **Port Utilization Module screen**.

8.1.10.9 Backplane.

The last thing we can review on the Port Utilization Module screen is the traffic that goes from module 1 to the modules 2, 3 and 4 via the Backplane. **Press '6'** to bring up the **Port Utilization Module** for the Backplane. To set the max receive threshold, **press '1'** this will add a **'1'** on the select: line at the bottom left side of the screen and add the line **'bp port (0-2) : Thresholds for intermodule (or backplane) ports work just like the thresholds for the module ports. If traffic exceeds threshold settings, a syslog and/or snmp event will be issued.**

```
Port Utilization Module 1

      Module 2      Module 3      Module 4
      rcv bytes      0          0          0
      xmt bytes      0          0          0
      rcv packets    0          0          0
      xmt packets    0          0          0
      rcv util       0%         0%         0%
      xmt util       0%         0%         0%
      rcv max util   0%         0%         0%
      xmt max util   0%         0%         0%
      rcv threshold  95%         95%         0%
      xmt threshold  95%         95%         7%

      1.set max receive threshold
      2.set max transmit threshold
      3.clear counts
      4.clear max util
      5.errors
      0.exit

select:1
bp port (0-2):
```

Figure 108: Set max transmit threshold

8.1.11 M1GSSF Module

1000M Aggregating TAP Module: Two (2) Single Mode Passive Fiber LC Tap Ports with two (2) SFP Monitoring Ports,

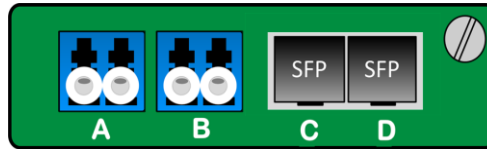


Figure 109: Front View of M1GSSF

The Single-Mode 1G bps Fiber Network ports to 1G bps SFP Monitor Ports Modules can operate at 1000Mbps speeds. Can be used to connect to a Single-Mode Monitoring device or convert the media from Single-Mode Fiber to Multi-Mode fiber.

8.1.12 M1GSSF Configuration

Once you have selected the Slot that has the M1GSSF module that you want to configure (in this case the M1GSSF TAP we want to configure is in Slot 1).

```

=====
Slot 1 Status:
=====
Link State:   Port A      Port B      Port C      Port D
Speed:        unknown    unknown    1G          unknown
Duplex:                Full
Media Type:    SMF        SMF        SFP         SFP
Serial Number: 00000
Software Version: Boot:1.2.2 App:1.2.54
=====
Slot 1 Select Option:
=====
Press
Taps with Fiber Network ports have network ports set to 1Gbps
Taps with Fiber Monitor ports have monitor ports set to 1Gbps
Taps with Fiber Network ports always have LFP ON.
c: Port Utilization
Press Enter to refresh this status screen
0. Exit

```

Figure 110: Network Port Speed Configuration

8.1.12.1 Slot '1' Status screen

Press '1' to bring up the 'Slot 1 Status' screen. This screen will provide the status of the M1GSSF module that is installed in Slot 1 of row 1 of the chassis. In this case, the link state of the network ports is 'Up'. The link state of the monitor ports is down as they have not been connected yet. There is nothing more to configure because the network ports of the M1GSSF are fiber the speed is always set for 1G bps and the Duplex is always set for 'Full'. This screen also provides you with the serial number of the module and the software version that is installed.

8.1.12.2 Port Utilization Module screen.

Pressing 'c' will bring up the 'Port Utilization Module 3' screen to allow you to see port utilization and number of packets. You can also set the TAP's max receive threshold, max transmit threshold, you can clear the packet counters to begin a new count, clear max utilization, bring up the error menu and see the backplane stats.

Port Utilization Module 3				
	PORT A	PORT B	PORT C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
Rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
select:				

Figure 111: Port Utilization Module Screen for Module 3

8.1.12.3 Set Max Receive threshold.

From the Port Utilization Module Screen press '1' to 'set max receive threshold'. This will place a '1' on the select line at the bottom of the screen and add a new line that is **Port (A-D)**: so you can set the threshold.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:1				
Port (A-D):				

Figure 112: Set max receive threshold

For example, setting the max utilization threshold for Port A receive to 53%, will cause a syslog and/or snmp trap to be sent if the receive traffic on port A exceeds 53%.

8.1.12.4 Set Max Transmit Threshold.

From the Port Utilization Module Screen **press '2'** to set max transmit threshold. This will place a **'2'** on the select line at the bottom of the screen and add a new line that is **Port (A-D):** so you can set the threshold for that port.

Port Utilization Module 1				
	Port A	Port B	Port C	Port D
xmt packets	0	0	0	0
rcv packets	0	0	0	0
xmt bytes	0	0	0	0
rcv bytes	0	0	0	0
xmt util	0%	0%	0%	0%
xmt max util	0%	0%	0%	0%
xmt threshold	100%	100%	100%	100%
rcv util	0%	0%	0%	0%
rcv max util	0%	0%	0%	0%
rcv threshold	100%	100%	100%	100%
1.set max receive threshold 2.set max transmit threshold 3.clear counts 4.clear max util 5.error menu 6.backplane 0.exit				
Select:2				
Port (A-D): █				

Figure 113: Set max transmit threshold

For example, we will set the max transmit threshold for Port C to 90%. When we press 'c' a new line will be inserted at the bottom of the screen 'Enter new max transmit threshold (0-100):'. This is where we enter 90 and press 'ENTER'. Now, whenever the traffic exceeds 90% on 'Port C', a syslog and/or snmp trap will be sent. Clear Counts/Clear max util.

8.1.12.5 Clear Counts/Clear max util.

Pressing '3' will clear the **xmt/rcv packet counter** and **pressing '4'** will clear the **xmt/rcv max util counters**.

8.1.12.6 Port Errors Menu screen.

Pressing '5' will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. **Press '0'** to return to the **Port Utilization Module screen**.

Garland Technology M1G1ACE				
Port Errors Module 3				
	Port A	Port B	Port C	Port D
crc	0	0	0	0
frame	0	0	0	0
jabber	0	0	0	0
undersize	0	0	0	0
oversize	0	0	0	0
fragments	0	0	0	0
rcv overrun	0	0	0	0
1.clear errors 0.exit				
Select:█				

Figure 114: Port Errors Module screen

8.1.12.7 Backplane.

The last thing we can review on the Port Utilization Module screen is the traffic that goes from module 4 to the modules 1, 2 and 3 via the Backplane. **Press '6'** to bring up the **Port Utilization Module** for the Backplane.

8.1.12.8 Setting Backplane Max Receive Threshold

To set the max receive threshold, **press '1'** this will add a **'1'** on the **select:** line at the bottom left side of the screen and add the line **'bp* port (0-2):'**. **Pressing '2'** will let you set the **column 1** receive threshold, **pressing '1'** will let you set the **column 2** receive threshold, and **pressing '0'** will let you set the **column 3** receive threshold.

Port Utilization Module 2			
	Module 1	Module 3	Module 4
rcv bytes	0	0	0
xmt bytes	0	0	0
rcv packets	0	0	0
xmt packets	0	0	0
rcv util	0%	0%	0%
xmt util	0%	0%	0%
rcv max util	0%	0%	0%
xmt max util	0%	0%	0%
rcv threshold	100%	100%	95%
xmt threshold	100%	100%	90%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.errors
0.exit


```

select:1
bp port(0-2):0
enter new max receive threshold(0-100):95

```

Figure 115: Set max receive threshold

For example, we want to set the max receive threshold for module 4 (column 3) to 90%. When we **press '0'**, a new line will be inserted at the left bottom of the screen **'Enter new max receive threshold (0-100):'**. This is where we enter **90** and **press 'ENTER'**. Now, whenever the traffic exceeds 90% on **'Module 4'** backplane, a syslog and/or snmp trap will be sent.

"bp" stands for Backplane

8.1.12.9 Setting Backplane Max Transmit Threshold

To set the max transmit threshold, **press '2'** this will add a **'2'** on the **select:** line at the bottom left side of the screen and add the line **'bp* port (0-2):'**. **Pressing '2'** will let you set the **column 1** transmit threshold, **pressing '1'** will let you set the **column 2** transmit threshold, and **pressing '0'** will let you set the **column 3** transmit threshold.

```

Port Utilization Module 2
      Module 1      Module 3      Module 4
rcv bytes      0      0      0
xmt bytes      0      0      0
rcv packets    0      0      0
xmt packets    0      0      0
rcv util       0%     0%     0%
xmt util       0%     0%     0%
rcv max util   0%     0%     0%
xmt max util   0%     0%     0%
rcv threshold  100%   100%   95%
xmt threshold  100%   100%   90%

1.set max receive threshold
2.set max transmit threshold
3.clear counts
4.clear max util
5.errors
0.exit

select:2
bp port(0-2):0
enter new max transmit threshold(0-100):90

```

Figure 116: Set max transmit threshold

8.1.12.10 Clear Counts/Clear max utility on Backplane.

Pressing '3' will clear the **xmt/rcv packet counter** and pressing '4' will clear the **xmt/rcv max util counters**.

8.1.12.11 Error Menu screen for Backplane.

Next, pressing '5' will bring up the **Port Errors module screen** where you can get a report on the various errors that may have occurred while monitoring the traffic passing through the TAP module. This screen gives you the option to clear the errors. Press '0' to return to the **Port Utilization Module screen**.

```

Garland Technology M1G1ACE
Port Errors Module 1
      PORT A      PORT B      PORT C      PORT D
crc      0      0      0      0
frame    0      0      0      0
jabber   0      0      0      0
undersize 0      0      0      0
oversize 0      0      0      0
fragments 0      0      0      0
rcv overrun 0      0      0      0

1.clear errors
0.exit

select:

```

Figure 117: Port Errors screen for module 3

The last thing we can review on the Port Utilization Module screen is the traffic that goes from module 3 to the modules 1, 2 and 4 via the Backplane. Press '6' to bring up the **Port Utilization Module** for the Backplane. To set the max receive threshold, press '1' this will add a '1' on the select: line at the bottom left side of the screen and add the line 'bp port (0-2):'. Thresholds for intermodule (or backplane) ports work just like the thresholds for the module ports. If traffic exceeds threshold settings, a syslog and/or snmp event will be issued.

```
Garland Technology M1G1ACE

Port Utilization Module 3

      rcv bytes      Module 1      Module 2      Module 4
      xmt bytes      0              0              0
      rcv packets    0              0              0
      xmt packets    0              0              0
      rcv util       0%            0%            0%
      xmt util       0%            0%            0%
      rcv max util   0%            0%            0%
      xmt max util   0%            0%            0%
      rcv threshold  95%          95%            0%
      xmt threshold  95%          95%            0%

      1.set max receive threshold
      2.set max transmit threshold
      3.clear counts
      4.clear max util
      5.errors
      0.exit

select:3
Bp port(0-2):
```

Figure 118: Set max transmit threshold

8.2 Filter Configuration

Pressing '2' on the Main Menu Screen, will begin the Filtering setup process.

```
Garland Technology M1G2ACE

Select Row

1:      M1GMSF      M1GCSF      M1GCSF      M1GCSF
2:      M1GCCBP     M1GCCA     M1GCSF     M1GCSF
3:      M1GSSF      M1GSCF     M1GCCBP     M1GCCA
0: Back
```

Figure 119: TAP Control M1G2ACE Chassis

We will set up filters for Layer 2, Layer 3 and Layer 4

The Chassis in the screen shot above shows the screen shot for a 2U chassis. The 2U chassis has 3 rows of four TAPs. If it were a 1U chassis it would have only one row of TAPS. Then you would not need to select the row that you want to set up.

Pressing '1' would bring up the Row 1 Filters screen.

```
TAP Control M1G1ACE

Row 1 Filters

No Filters defined for row 1.

u:cursor up  d:cursor down  v:view      c:clear count
a:add        e:edit        i:insert    x:delete
t:filter up  g:filter down  r:reset     h:help
0:exit
select:
```

Figure 120: Row 1 Filters screen

8.2.1 Layer 2 Filter setup

We will begin by setting up a Layer 2 Filter. Layer 2 filtering allows filtering on the source MAC address, the destination MAC address or the VLAN ID. These may be used in any combination

with each other or any other filter field.

Press 'a' to begin the process of adding and defining a layer 2 filter. This will bring up the Edit Filter menu.

```

Edit filter:
1.Name                : FILTER
2.Ports               : [   |   |   |   ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:
  
```

Figure 121: Edit Filter Screen

The program has provided the default name 'Filter' for the Filter. **Press '1'** to change the filter's name.

```

Edit filter:
1.Name                : FILTER
2.Ports               : [   |   |   |   ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:1
Filter Name: FILTER
  
```

Figure 122: Changing the filter name

Pressing '1' causes the program to add a line '**Filter Name: FILTER**' at the bottom of the menu. Using the Backspace Key, erase the word FILTER and enter the new name 'case 432A'. Press the **RETURN Key** and the new filter name replaces the default filter name on the name line of the edit filter screen.

```

Edit filter:
1.Name                : Case 432A
2.Ports               : [   |   |   |   ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:
  
```

Figure 123: Filter has a new name

The next step is to define the Ingress port(s) for this filter. **Press '2'** to bring up the 'Select Ingress Port(s)' screen.


```
TAP Control M1G1ACE

Select Ingress Port(s)

map: [   |   |   |   ]

Slot 1 - M1GSSF:
1: A1 [ ]
2: B1 [ ]
Slot 2 - M1GSCF:
3: A2 [ ]
4: B2 [ ]
Slot 3 - M1GMCf:
5: A3 [ ]
6: B3 [ ]
Slot 4 - M1GCSF:
7: A4 [ ]
8: B4 [ ]
e: Egress Ports Menu
0: Exit
```

```
TAP Control M1G1ACE

Select Ingress Port(s)

map: [   | i |   | i ]

Slot 1 - M1GSSF:
1: A1 [ ]
2: B1 [ ]
Slot 2 - M1GSCF:
3: A2 [ ]
4: B2 [*]
Slot 3 - M1GMCf:
5: A3 [ ]
6: B3 [ ]
Slot 4 - M1GCSF:
7: A4 [*]
8: B4 [ ]
e: Egress Ports Menu
0: Exit
```

Figure 124: Select Ingress Port(s) Screen and **Figure 125:** Ingress port(s) selected

Pressing ‘2’ takes you directly to the ‘Select Ingress Port(s)’ menu. **Press ‘4’ and ‘7’.** This inserts an asterisk ‘*’ in the Brackets of port B2 and port A4 as well as placing ‘i’s in their respective positions on the ports map.

```
TAP Control M1G1ACE

Select Egress Port(s)

map: [   | i |   | i ]

Slot 1 - M1GSSF:
1: C1 [ ]
2: D1 [ ]
Slot 2 - M1GSCF:
3: C2 [ ]
4: D2 [ ]
Slot 3 - M1GMCf:
5: C3 [ ]
6: D3 [ ]
Slot 4 - M1GCSF:
7: C4 [ ]
8: D4 [ ]
i: Ingress Ports Menu
0: Exit
```

```
TAP Control M1G1ACE

Select Egress Port(s)

map: [   | i |   | i o ]

Slot 1 - M1GSSF:
1: C1 [ ]
2: D1 [ ]
Slot 2 - M1GSCF:
3: C2 [ ]
4: D2 [ ]
Slot 3 - M1GMCf:
5: C3 [ ]
6: D3 [ ]
Slot 4 - M1GCSF:
7: C4 [ ]
8: D4 [*]
i: Ingress Ports Menu
0: Exit
```

Figure 126: Select Egress port(s) screen and **Figure 127:** Egress port(s) selected

You can go directly to the ‘Select Egress Port(s)’ menu to setup the egress port(s) by **pressing ‘e’**. When you see the Select Egress Ports screen, **Press ‘8’** to select the egress port at port D4. **Press ‘0’** to return to the Edit Filter Screen. We now have ‘i’s in the B2 and A4 positions of the ports map and an ‘o’ in the D4 position of the ports map line.

```
Edit filter:
1.Name           : Case 432A
2.Ports          : [   | i |   | i o ]
3.Counter used   : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID       :
7.Layer 3       :
0:Exit
Enter menu selection:
```

Figure 128: Back to Edit Filter Screen

Press '0' to return to the Row 1 Filters Screen. As you can see, we now have a 'case 432A' filter which can send traffic from ports B2 and A4 to port D4 (slot 2 port B and slot 4 port A to slot 4 port D). At this point, ALL traffic will be sent as there are no filters defined yet. Note the presence of the '**s**' in the menu. This indicates that the filter has not been saved in flash memory or downloaded to the modules yet. **Press 's'** now.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

  #: Name      Ports      Count
-> 1: case 432A [ | 1 | | 1 o] 0

u:cursor up d:cursor down v:view      c:clear count
a:add       e:edit        i:insert   x:delete
t:filter up g:filter down r:reset    h:help
0:exit     *** s:SAVE AND APPLY FILTERS ***
select: █
```

Figure 129: Row 1 Filters Screen

Figure 130 below is what the screen looks like while the program is saving the filter to the flash and downloading to the modules.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

  #: Name      Ports      Count
-> 1: Case 432A [unav| i | | i o] 0
   1: Case 432A [unav| i | | i o] 0

u:cursor up d:cursor down t:filter up g:filter down
a:add       e:edit        i:insert   x:delete
v:view      c:clear count r:reset    h:help
0:exit     *** s:SAVE AND APPLY FILTERS ***
Select:

Updating filters in modules in row 1, slot 1, 2, 3, 4 ...
```

Figure 130: Row 1 Filters Screen

Once the save is completed, the Row 1 Filters Screen will look like Figure 79. Notice the '**s**' selection is gone. Next, we want to copy the case 432A filter name, then edit it, to filter on the destination MAC addresses.

```
TAP Control M1G1ACE

Row 1 Filters

  #: Name      Ports      Count
-> 1: case 432A [ | i | | i o] 0

u:cursor up d:cursor down v:view      c:clear count
a:add       e:edit        i:insert   x:delete
t:filter up g:filter down r:reset    h:help
0:exit
select: █
```

Figure 131: Row 1 Filters Screen with case 432A in progress

We can copy the case 432A filter by **pressing the 'F1' function key**. The copied filter will appear on the Row 1 Filters screen in the number 1 position. The **'F1'** function key is the only function key that is used in the program and its only purpose is to copy a filter, so you can modify it without having to start from scratch.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

# Name Ports Count
-> 1: case 432A [ | i | |i o] 0
   2: case 432A [ | i | |i o] 0

u:cursor up d:cursor down v:view c:clear count
a:add e:edit i:insert x:delete
t:filter up g:filter down r:reset h:help
0:exit *** s:SAVE AND APPLY FILTERS ***
select: █
```

Figure 132: Row 1 Filters screen with new filter in 1st position

Now we can edit the new filter by **pressing 'e'**. Next, we want to create a new name for the filter. In this case, we want to add to the current name 'case 432A'. We will add 'dmac' to the end of the current name. Press **<enter>** to save the new name on the name line of the screen.

```
Edit filter:
1.Name : case 432A dmac
2.Ports : [ | i | |i o]
3.Counter used : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID :
7.Layer 3 :
0:Exit
Enter menu selection: █
```

Figure 133: New Filter Name 'case 432A dmac'

Next, we want to set up a filter for the **'destination MAC address'** so we will **press '5'**.

```
Edit filter:
1.Name : case 432A dmac
2.Ports : [ | i | |i o]
3.Counter used : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID :
7.Layer 3 :
0:Exit
Enter menu selection:5

filter on DESTINATION mac address?[N]: █
```

Figure 134: Filter on destination MAC address

The program will add the line **'filter on DESTINATION mac address? [N:]'** at the bottom of the menu. Press **'y'** to add the address.

Note: The name of the filter is for User's convenience only and does not affect the operation. So, multiple filters with the same name are allowed.

```

Edit filter:
1.Name           : case 432A dmac
2.Ports          : [   | i |   |i o]
3.Counter used   : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID        :
7.Layer 3        :
0:Exit
Enter menu selection:5

filter on DESTINATION mac address?[N]:y
Enter DESTINATION mac address(hex):

```

Figure 135: Enter the destination MAC address (in hex)

The program will add a second line to the bottom of the screen 'Enter DESTINATION MAC address?' (hex). At this point, the controller expects the user to enter 6 hex numbers. The ':' delimiting colons are added automatically for convenience. Hex numbers expected are two digits each with the digits being 0-9 or a-f. So, we will enter 'c', '8', '2', '0'. Now if we enter 'g' instead of 'f' the program will alert the user by posting a warning message. For example, **pressing 'g'** will warn of an **INVALID CHARACTER** but not allow the character to be entered.

```

Edit filter:
1.Name           : case 432A dmac
2.Ports          : [   | i |   |i o]
3.Counter used   : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID        :
7.Layer 3        :
0:Exit
Enter menu selection:5

filter on DESTINATION mac address?[N]:y
!INVALID CHARACTER! Enter DESTINATION mac address(hex): c8:20:

```

Figure 136: Edit Filter screen showing INVALID CHARACTER entered

Now we will enter the remainder of the Destination MAC address, 'f', '1', '5', '7', '3', 'a', '4', '2' and if the numbers are entered correctly, the program will announce that the a 'valid MAC address' was entered. Press 'ENTER' to accept the MAC address.

```

Edit filter:
1.Name           : case 432A dmac
2.Ports          : [   | i |   |i o]
3.Counter used   : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID        :
7.Layer 3        :
0:Exit
Enter menu selection:5

filter on DESTINATION mac address?[N]:y
valid mac address Enter DESTINATION mac address(hex): c8:20:f1:57:3a:42

```

Figure 137: The Destination MAC is entered

```

Edit filter:
1.Name           : case 432A dmac
2.Ports          : [   | i |   |i o]
3.Counter used   : YES
4.Source MAC address :
5.Destination MAC address : c8:20:f1:57:3a:42
6.VLAN ID        :
7.Layer 3        :
0:Exit
Enter menu selection:

```

Figure 138: The Destination MAC is entered

Please note that entering the SOURCE MAC address is operationally the same as entering the DESTINATION MAC address. If a SOURCE MAC address is entered at this point, the filter would require a packet to match both criteria before passing that packet. **Press '0'** to return to the **'Row 1 Filter'** screen.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

# : Name          Ports          Count
-> 1: Case 432A dmac [unav| i | |i o] 0
   1: Case 432A    [unav| i | |i o] 0

u:cursor up  d:cursor down  t:filter up  g:filter down
a:add        e:edit         i:insert     x:delete
v:view       c:clear count  r:reset     h:help
0:exit      *** s:SAVE AND APPLY FILTERS ***
Select:
```

Figure 139: Back to the Row 1 Filters Screen

Back to the Row 1 Filter screen and we will **press 's'** to save and apply the filters as we did before.

```
TAP Control M1G1ACE

Row 1 Filters

# : Name          Ports          Count
-> 1: Case 432A dmac [unav| i | |i o] 0
   1: Case 432A    [unav| i | |i o] 0

u:cursor up  d:cursor down  t:filter up  g:filter down
a:add        e:edit         i:insert     x:delete
v:view       c:clear count  r:reset     h:help
0:exit
Select:
```

Figure 140: The case 432A dmac is saved

Now we want to create a filter 'abc'. This filter will look for packets with a VLAN 768 from port A on slot 2 and send them to port C on slot 3. So, we will **press 'a'** to add the new filter. Remember how we have done it before. Now we tell the filter what the ingress and egress ports are.

```
Edit filter:
1.Name          : abc
2.Ports         : [ | | | | ]
3.Counter used  : YES
4.Source MAC address :
5.Destination MAC address :
6.VLAN ID       :
7.Layer 3       :
0:Exit
Enter menu selection:
```

Figure 141: The new Filter has a name

Press '3' to select slot 2 port 'A' this will cause an asterisk '*' to be placed in the A2 brackets and an 'i' to be placed in the slot 2, port A position on the map line. Now we will set up the egress port. **Pressing 'e'** will bring up the **'Egress port(s)'** screen.

```
TAP Control M1G1ACE
Select Ingress Port(s)

map: [   |   |   |   ]

Slot 1 - M1GSSF:
1: A1 [ ]
2: B1 [ ]
Slot 2 - M1GSCF:
3: A2 [ ]
4: B2 [ ]
Slot 3 - M1GMCF:
5: A3 [ ]
6: B3 [ ]
Slot 4 - M1GCSF:
7: A4 [ ]
8: B4 [ ]
e: Egress Ports Menu
0: Exit
```

```
TAP Control M1G1ACE
Select Ingress Port(s)

map: [   |i |   |   ]

Slot 1 - M1GSSF:
1: A1 [ ]
2: B1 [ ]
Slot 2 - M1GSCF:
3: A2 [*]
4: B2 [ ]
Slot 3 - M1GMCF:
5: A3 [ ]
6: B3 [ ]
Slot 4 - M1GCSF:
7: A4 [ ]
8: B4 [ ]
e: Egress Ports Menu
0: Exit
```

Figure 142: Select Ingress Port(s) Screen and **Figure 143:** Ingress port(s) selected

Press '5' to select slot 3 port 'C'. This will place a n asterisk (*) in C3 brackets and an 'o' in the slot 3 port 'C' position of the map line. Press '0' to return to the 'Edit filter screen' figure '81'. The filter has a name and the ingress and egress ports are defined.

```
TAP Control M1G1ACE
Select Egress Port(s)

map: [   |i |   |   ]

Slot 1 - M1GSSF:
1: C1 [ ]
2: D1 [ ]
Slot 2 - M1GSCF:
3: C2 [ ]
4: D2 [ ]
Slot 3 - M1GMCF:
5: C3 [ ]
6: D3 [ ]
Slot 4 - M1GCSF:
7: C4 [ ]
8: D4 [ ]
i: Ingress Ports Menu
0: Exit
```

```
TAP Control M1G1ACE
Select Egress Port(s)

map: [   |i | o |   ]

Slot 1 - M1GSSF:
1: C1 [ ]
2: D1 [ ]
Slot 2 - M1GSCF:
3: C2 [ ]
4: D2 [ ]
Slot 3 - M1GMCF:
5: C3 [*]
6: D3 [ ]
Slot 4 - M1GCSF:
7: C4 [ ]
8: D4 [ ]
i: Ingress Ports Menu
0: Exit
```

Figure 144: Select Egress Port(s) Screen and **Figure 145:** Egress port(s) selected

```
Edit filter:
1.Name                : abc
2.Ports               : [   |i | o |   ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:
```

Figure 146: Ingress and egress ports defined

```
Edit filter:
1.Name                : abc
2.Ports               : [   |i | o |   ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:6

filter on vlan id?[N]:y
Enter vlan id(decimal):
```

Figure 147: Creating VL AN ID

Now we want to define the VLAN ID s o **press '6'**. T he program will enter a line at the bottom **“filter on VLAN ID [N]:”, press 'y'**. A second line will appear asking for the VLAN ID in decimal form. E nter '7', '6', '8' for the VLAN ID then press **'ENTER'** next **press '0'** to return to the Ro w 1 Fi lters S creen.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

#  Name      Ports      Count
1: Case 432A dmac [unav] i | |i o] 0
-> 2: Case 432A [unav] i | |i o] 0
3: abc [unav] i | o | ] 0
u:cursor up d:cursor down t:filter up g:filter down
a:add e:edit i:insert x:delete
v:view c:clear count r:reset h:help
0:exit *** s:SAVE AND APPLY FILTERS ***
Select:
```

Figure 148: VL AN ID c reated

Next, we want to move the cursor up f rom filter 3 to filter 2 s o we can move the filter cas e 432A up to the first position. **Press 'u'** to move the cursor up o ne position

```
TAP Control M1G1ACE

Row 1 Filters

#  Name      Ports      Count
-> 1: Case 432A [unav] i | |i o] 0
2: Case 432A dmac [unav] i | |i o] 0
3: abc [unav] i | o | ] 0
u:cursor up d:cursor down t:filter up g:filter down
a:add e:edit i:insert x:delete
v:view c:clear count r:reset h:help
0:exit
Select:
```

Figure 149: Filter case432A is now in first position

Press 't' to move the filter 'cas e 432A' up one position.

Press 's' to save the Ro w 1 Filters screen

```
TAP Control M1G1ACE

Row 1 Filters

#  Name      Ports      Count
1: 432A [ i | |i o] ] 0
2: 432A dmac [ i | |i o] ] 0
-> 3: abc [ |i | o | ] 0
u:cursor up d:cursor down v:view c:clear count
a:add e:edit i:insert x:delete
t:filter up g:filter down r:reset h:help
0:exit
select: █
```

Figure 150: Filter case **432A** is now in first position

8.2.2 Layer 3 Filter set up

La yer 3 filtering can target all IP messages or a ll non-IP messages. When IP is selected, the other layer 3 filter fields appear on the menu, these are s ource IP address, destination IP address, and DS CP. These may be used in any combination with each other or any other filter if IP messaging has been selected. **Press 'a'** to bring up **'Edit Filter Screen'**

```

Edit filter:
1.Name                : src IP fltA
2.Ports               : [  |i  o|  |  ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             :
0:Exit
Enter menu selection:7
  
```

Figure 151: New filter src IP fltA

Using the menu system as previously described, we will create a filter named 'src IP fltA'. This filter will filter on packets with source IP address 192.168.1.102. We now **press '7' then 'i'**. The Edit Filter menu changes. **Press '8'** then enter the IP address 192.168.1.102. The program will enter the source IP mask and provides the opportunity to edit it if necessary. Then press <enter>.

```

Edit filter:
1.Name                : src IP fltA
2.Ports               : [  |i  o|  |  ]
3.Counter used        : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             : IP
8.Source IP address    : 192.168.1.102 mask:255.255.255.255
9.Destination IP address :
a.DSCP                :
b.Layer 4             :
0:Exit
Enter menu selection:
  
```

Figure 152: The source IP address and mask is set

```

TAP Control M1G1ACE

Row 1 Filters  ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

# Name          Ports          Count
1: Case 432A    [ i |  |i  o|  ] 0
2: Case 432A dmac [ i |  |i  o|  ] 0
3: abc         [  |i  | o|  ] 0
-> 4: src IP fltA [  |i  o|  |  ] 0
u:cursor up  d:cursor down  t:filter up   g:filter down
a:add        e:edit       i:insert      x:delete
v:view       c:clear count r:reset       h:help
0:exit      *** s:SAVE AND APPLY FILTERS ***
Select:
  
```

Figure 153: Save the source IP filter

Next move Filter '4' up to the #1 position. **Press 's'** to save the Source IP Filter 'src IP fltA'.

Next, we will create another layer 3 filter named 'DSCP=21'. **Press 'a'** to add the new filter. **Press '1'** to name it 'DSCP=21' and **press <enter>**. Next **press '2'** to set up the ports. **Press '7'** to select ingress port 'a4' next **press 'e'** to bring up the Egress port screen then **press '7'** to select egress port 'c4'.


```

Edit filter:
1.Name                : DSCP=21
2.Ports               : [   |   |   |i o ]
3.Counter used       : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID            :
7.Layer 3             : IP
8.Source IP address   :
9.Destination IP address :
a.DSCP               : 21
b.Layer 4            :
0:Exit
Enter menu selection:
  
```

Figure 154: DSC P=21 is named and set to be defined

Next **press '7'** to set up the Layer 3 DSCP parameters, **press 'a'** to define the DSCP value. **Press '21'** **<enter>** to enter 21 on line 'a'. Filter DSCP=21 is now complete.

```

TAP Control M1G1ACE
Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

  #: Name                Ports                Count
-> 1: src IP fltA        [   |i o|   |   ]    0
   2: 432A               [ i |   |i o|   ]    0
   3: 432A dmac          [ i |   |i o|   ]    0
   4: abc                [   |i | o |   ]    0
   5: DSCP=21            [   |   |   |i o ]    0

u:cursor up  d:cursor down  v:view        c:clear count
a:add        e:edit         i:insert       x:delete
t:filter up  g:filter down  r:reset       h:help
0:exit      *** s:SAVE AND APPLY FILTERS ***
select:
  
```

Figure 155: Save the DSCP=21 filter

Filter DSCP=21 is complete. **Press 's'** to save.

```

TAP Control M1G1ACE
Row 1 Filters

  #: Name                Ports                Count
-> 1: src IP fltA        [   |i o|   |   ]    0
   2: 432A               [ i |   |i o|   ]    0
   3: 432A dmac          [ i |   |i o|   ]    0
   4: abc                [   |i | o |   ]    0
   5: DSCP=21            [   |   |   |i o ]    0

u:cursor up  d:cursor down  v:view        c:clear count
a:add        e:edit         i:insert       x:delete
t:filter up  g:filter down  r:reset       h:help
0:exit
select:
  
```

Figure 156: Filter DSCP=21 is saved

Press '0' to return to the Row 1 Filters screen. Next **press 'a'** to add a **layer 4** filter.

8.2.3 Layer 4 Filter set up

Layer 4 filtering captures protocols riding on layer 3 IP. Specifically, the IP port number, 0-255, which identifies the Layer 4 protocol in the packet. Two of the protocols, TCP=6, and UDP=17, contain source and destination ports which can also be used as keys for filters.

ICMP is identified as IP protocol=1. Using previously explained commands, we create a new filter named 'ICMP', B2->C3...

Next, we will create layer 4 filter named **'ICMP'**. Press **'a'** to begin the process to add the new filter.

Press **'1'** to name it **'ICMP'** and press **<enter>**.

Press **'2'** to set up the ports. Press **'4'** to select ingress port **'b2'**

Press **'e'** to bring up the Egress port screen then press **'5'** to select egress port **'c3'**

Press **'0'** to return to the **'Edit Filter Screen'**.

Press **'7'** to select the Layer 3 function then press **'i'** to select **'IP'** then press **'b'** to select Layer 4 this will bring up more selections at the bottom of the screen.

Press **'h'** and enter **'1'** so we can filter on **'ICMP IP protocol =1'**. IP protocol can be a decimal number 0-255.

```

Edit filter:
1.Name                : ICMP
2.Ports               : [   | i | o |   ]
3.Counter used       : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             : IP
8.Source IP address   :
9.Destination IP address :
a.DSCP                :
b.Layer 4             :
0:Exit
Enter menu selection:b

filter on layer 4(IP protocol)?[N]:y
t.tcp:
u.udp
h.other
any other key.no change
ip protocol[0]:
  
```

Figure 157: Filter ICMP filter is almost done

```

Edit filter:
1.Name                : ICMP
2.Ports               : [   | i | o |   ]
3.Counter used       : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             : IP
8.Source IP address   :
9.Destination IP address :
a.DSCP                :
b.Layer 4             : 1
0:Exit
Enter menu selection:
  
```

Figure 158: Filter ICMP filter is complete

Press **'0'** to return to the Row 1 filter screen.

```
TAP Control M1G1ACE

Row 1 Filters ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

# Name Ports Count
1: src IP fltA [ |i o| | ] 0
2: 432A [ i | |i o| ] 0
3: 432A dmac [ i | |i o| ] 0
4: abc [ |i | o | ] 0
5: DSCP=21 [ | | |i o ] 0
-> 6: ICMP [ | i | o | ] 0

u:cursor up d:cursor down v:view c:clear count
a:add e:edit i:insert x:delete
t:filter up g:filter down r:reset h:help
0:exit *** s:SAVE AND APPLY FILTERS ***
select: █
```

Figure 159: Filter ICMP filter is ready to be saved

Press **'s'** to save the filter.

```
TAP Control M1G1ACE

Row 1 Filters

# Name Ports Count
1: src IP fltA [ |i o| | ] 0
2: 432A [ i | |i o| ] 0
3: 432A dmac [ i | |i o| ] 0
4: abc [ |i | o | ] 0
5: DSCP=21 [ | | |i o ] 0
-> 6: ICMP [ | i | o | ] 0

u:cursor up d:cursor down v:view c:clear count
a:add e:edit i:insert x:delete
t:filter up g:filter down r:reset h:help
0:exit
select: █
```

Figure 160: Now have 6 filters completed

We will add one more filter to our set of examples. We will create a filter named **'Email send'** capture filter and send them to a monitor port.

So, for the last filter, we will create a layer 4 filter named **'email send'**.

Press **'a'** to add the new filter. Press **'1'** to name it **'email send'** and press **<enter>**.

Next press **'2'** to set up the ingress port.

Press **'3'** to select ingress port **'a2'**

Next press **'e'** to bring up the Egress port screen then press **'3'** to select egress port **'c2'**.

Press **'0'** to return to the **'Edit Filter'** screen.

Press **'7'** to display the Layer 3 functions, then press **'i'**, to select **'IP'** then press **'b'** to select Layer 4.

A question will display at the bottom of the screen asking if you want to filter on layer 4 (IP protocol) press **'y'**. This will bring up more selections at the bottom of the screen. We will press **'t'** to select **'tcp'**.

Now we want to define the **DESTINATION port**, press **'d'** and the program will add a new question line to the bottom of the menu – **'filter on DESTINATION port? [N]'**.

Press **'y'** and the program will add another line to allow the entry of the Destination port. Enter the number **'587'**.

```

Edit filter:
1.Name                : email send
2.Ports               : [   |i o|   |   ]
3.Counter used       : YES
4.Source MAC address  :
5.Destination MAC address :
6.VLAN ID             :
7.Layer 3             : IP
8.Source IP address   :
9.Destination IP address :
a.DSCP                :
b.Layer 4             : 6 (TCP)
c.Source Port         :
d.Destination Port    : 587
0:Exit
Enter menu selection:
  
```

Figure 161: The 'email send' is complete

Press '0' to return to the Row 1 Filters screen. The TCP source port, and UDP source and destination entries are similar.

```

TAP Control M1G1ACE

Row 1 Filters  ***FILTER CONFIGURATION NOT SAVED OR APPLIED***

# : Name                Ports                Count
1: src IP fltA          [   |i o|   |   ]      0
2: 432A                 [ i |   |i o|   ]      0
3: 432A dmac            [ i |   |i o|   ]      0
4: abc                  [   |i | o |   ]      0
5: DSCP=21              [   |   |   |i o|   ]    0
6: ICMP                 [   | i | o |   ]      0
-> 7: email send         [   |i o|   |   ]      0

u:cursor up  d:cursor down  v:view       c:clear count
a:add        e:edit         i:insert     x:delete
t:filter up  g:filter down  r:reset     h:help
0:exit      *** s:SAVE AND APPLY FILTERS ***
select:
  
```

Figure 162: The filters are ready to be saved

Always remember to **press 'S'** to save your work when you finish entering your filters or they won't be there when you try to use them.

```

TAP Control M1G1ACE

Row 1 Filters

# : Name                Ports                Count
1: src IP fltA          [   |i o|   |   ]      0
2: 432A                 [ i |   |i o|   ]      0
3: 432A dmac            [ i |   |i o|   ]      0
4: abc                  [   |i | o |   ]      0
5: DSCP=21              [   |   |   |i o|   ]    0
6: ICMP                 [   | i | o |   ]      0
-> 7: email send         [   |i o|   |   ]      0

u:cursor up  d:cursor down  v:view       c:clear count
a:add        e:edit         i:insert     x:delete
t:filter up  g:filter down  r:reset     h:help
0:exit
select:
  
```

Figure 163: The 'email send' filter is now complete

Press '0' to return to the main menu.

```
Garland Technology M1G1ACE (Code Version: 1.0.50j)

Main Menu

Select:

1. Change/View Module Configuration
2. Filtering
3. Username/Password
4. Settings
5. Users
0. Logout
Select:█
```

Figure 164: Main Menu Screen

This concludes the demonstration of the various types of filters that can be set up to manage the traffic flow that will go out to the monitor ports.

You will find this product to be a big help to monitor all that is happening on your 1G bps network.

9 M1GXX BP Module Series TAPs

The M1GXX BP TAP module series is ideal for 100/1000Mbps copper or fiber network monitoring. Their innovative design allows these TAPs to be easily installed into any copper or fiber 100/1000Mbps network segment.

Once installed in your network, the 100/1000Mbps network TAP will enable you to monitor your network segments quickly and effectively using a network analyzer, security devices or any monitoring appliance. These 100/1000Mbps allow you to process full-duplex traffic without dropping any packets and can handle SPAN traffic as well. The SPAN traffic can be replicated out to ports B, C and D. The Bypass TAP provides a safe way to install your In-Line Appliances directly in line of your critical links without introducing a "Point of Failure".

From the Main Menu, **press '1'** to bring up the **'Select the slot number to view/modify'** screen. This screen will provide information about the Packet Broker chassis like the serial number of the chassis, the serial number of the management controller if one is present and the part number of the modules that are installed in the slots and their current states.

```

Select slot number to view/modify
Chassis Serial Number: 21870020103 Controller Serial Number: 21910020100

Power Supply 1: Down
Power Supply 2: Up

# : Module Type
Operating Mode (Current State)
-----
1: M1GCCBP      2: M1GMSBP      3: Slot Empty    4: Slot Empty
   Bypass(Inline)  Bypass(Bypass)

Press
1: Select Slot 1  2: Select Slot 2  3: Select Slot 3  4: Select Slot 4
0: Exit

```

Figure 165: Select slot number to view/modify screen

Next **press '1'** again to bring up the **'Slot 1 Status'** screen where a M1GCC BP module is installed. This screen will show how the module is currently set and provide you the buttons you need to change the speed, the duplex mode, the LFP mode or restore the default settings of the modules.

In the case of a TAP with fiber network ports, there is no selection for setting the speed and no selection for setting the LFP mode, because TAPs with fiber network ports are always set for **1Gbps** speed and the LFP mode is always **'ON'**. But, because the TAP in slot 1 is a copper TAP, there are options to change the speed and the LFP modes. Once you get to the screen pertinent to each type of module, the screen is self-explanatory.

```

=====
Slot 1 Status:
=====
Current Bypass State: Inline

Link State:   Port A   Port B   Port C   Port D
Duplex:       auto    auto    auto    auto
Media Type:   RJ45    RJ45    RJ45    RJ45
Serial Number: 2076-0020455
=====
Slot 1 Select Option:
=====
Press
1: Set Operating Mode (Bypass)
2: Set Speed(1G)
3: Set LFP Mode (OFF)
4: Set Duplex Mode
5: Set Reverse Bypass Mode (OFF)
6: Set Forced Bypass Mode (OFF)
D: Restore Defaults
Press Enter to refresh this status screen
0: Exit

```

Figure 166: Slot 1 Status screen

10 M1GXXA Modular TAP Series

The M1GXXA TAP module series is ideal for 100/1000Mbps copper or fiber network monitoring. Their innovative design allows these TAPs to be easily installed into any copper or fiber 100/1000Mbps network segment.

Once installed in your network, the 100/1000Mbps network TAP will enable you to monitor your network segments quickly and effectively using a network analyzer, security devices or any monitoring appliance. These 100/1000Mbps allow you to process full-duplex traffic without dropping any packets and can handle SPAN traffic as well. The SPAN traffic can be replicated out to ports B, C and D. The Bypass TAP provides a safe way to install your In-Line Appliances directly in line of your critical links without introducing a "Point of Failure".

From the Main Menu, **press '1'** to bring up the **'Select the slot number to view/modify'** screen. This screen will provide information about the Packet Broker chassis like the serial number of the chassis, the serial number of the management controller if one is present and the part number of the modules that are installed and their current state.

11 Part Numbers and Descriptions

11.1 1U and 2U Packet Broker Chassis

Part Number	Description
M1G1ACE	1U modular chassis with dual internal AC power supplies, supports up to four TAP modules. Backplane feature can be used with all of Garland Technology's 1Gbps modular TAPs that end with a letter "F".
M1G1DCE	1U modular chassis with dual internal DC power supplies, supports up to four TAP modules. Backplane feature can be used with all of Garland Technology's 1Gbps modular TAPs that end with a letter "F".
M1G2ACE	2U modular chassis with dual internal AC power supplies, supports up to twelve TAP modules. Backplane feature can be used with all of Garland Technology's 1Gbps modular TAPs that end with a letter "F".
M1G2DCE	2U modular chassis with dual internal DC power supplies, supports up to twelve TAP modules. Backplane feature can be used with all of Garland Technology's 1Gbps modular TAPs that end with a letter "F".
M1GC	Management card: Ethernet/GUI and Serial/CLI for M1GXXE
TRAY-BG	Blanking Tray for management slot when the management card is not required

11.2 Modular TAPs designed to operate with the filtering and aggregating backplane.

Part Number	Description	Filter TAP Modules
M1GCCF	10/100/1000Mbps network Speed, Copper network ports to copper, aggregating, L2-L4 filtering monitor ports module.	
M1GCSF	Copper network ports to SFP, aggregating, filtering monitor ports module.	
M1GMCf	Multi-mode fiber network ports to copper, aggregating, filtering monitor ports module.	
M1GMSF	Multi-mode fiber network ports to SFP, aggregating, filtering monitor ports module.	
M1GSCF	Single-mode fiber network ports to Copper, aggregating, filtering monitor ports module.	
M1GSSF	Single-mode fiber network ports to SFP, Aggregating, Filtering monitor ports module.	

Note: All Garland Technology 1Gbps TAP Modules can be used on the Packet Broker Chassis. (see lists below)

11.3 Bypass TAP Modules

Modules that can be deployed in the Packet Broker Chassis.

Part Number	Description
M1GCCBP	100/1000M Aggregating Tap Module: Two (2) Copper 100/1000M RJ-45 Tap Ports with two (2) Copper 100/1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support
M1GCSBP	100/1000M Aggregating Tap Module: Two (2) Copper 100/1000M RJ-45 Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support
M1GMCBP	1000M Aggregating Tap Module: Two (2) Multi-Mode Fiber LC Tap Ports with two (2) Copper 1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support
M1GMSBP	1000M Aggregating Tap Module: Two (2) Multi-Mode Fiber LC Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support
M1GSCBP	1000M Aggregating Tap Module: Two (2) Single Mode Fiber LC Tap Ports with two (2) Copper 1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support
M1GSSBP	1000M Aggregating Tap Module: Two (2) Single Mode Fiber LC Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support

11.4 Legacy TAP Modules

Part Number	Description	Aggregation TAP Modules
M1GCCA is now M1GCCBP	100/1000M Aggregating Tap Module: Two (2) Copper 100/1000M RJ-45 Tap Ports with two (2) Copper 100/1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support	
M1GCSA is now M1GCSBP	100/1000M Aggregating Tap Module: Two (2) Copper 100/1000M RJ-45 Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and Bypass Mode with Packet Injection support	
M1GMCA	1000M Aggregating Tap Module: Two (2) Multi-Mode Passive Fiber LC Tap Ports with two (2) Copper 1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and SPAN Mode	
M1GMSA	1000M Aggregating Tap Module: Two (2) Multi-Mode Passive Fiber LC Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and SPAN Mode	
M1GSCA	1000M Aggregating Tap Module: Two (2) Single Mode Passive Fiber LC Tap Ports with two (2) Copper 1000M RJ-45 Monitoring Ports, supports Breakout Mode, Aggregation Mode, and SPAN Mode	
M1GSSA	1000M Aggregating Tap Module: Two (2) Single Mode Passive Fiber LC Tap Ports with two (2) SFP Monitoring Ports, supports Breakout Mode, Aggregation Mode, and SPAN Mode	

Part Number	Description	Breakout TAP Modules
M100CCB	10/100 Passive Breakout Tap Module: Two (2) Copper 10/100M RJ-45 Tap Ports with two (2) Copper 10/100M RJ-45 Monitoring Ports, support Breakout Mode and passes physical layer errors, Plug-n-Play no configuration	
M1GCCB	10/100/1000M Breakout Tap Module: Two (2) Copper 10/100/1000M RJ-45 Tap Ports with two (2) Copper 10/100/1000M RJ-45 Monitoring Ports, supports breakout Mode (unique GT Features: link speed synchronization, passes data-link layer errors, easily deployed)	

12 Technical Specifications

Chassis Specifications						
Model #	Chassis/TAPs*	Power Supplies	Voltage	Current (Max)	Consumption (Max)	Dimensions
M1G1 ACE	1U; up to 4 TAP s	Dua l Internal AC	100-240VAC	.75 Amps @ 115VAC	86.25 Watts	17.40" x 1.75" x 13.45" 441.96mm x 44.45mm x 341.63mm
M1G1 ADE	1U; up to 4 TAP s	Dua l Internal DC	36-60VDC	1 Amp @ 48VDC	48 Watts	
M1G2 ACE	2U; up to 12 TAP s	Dua l Internal AC	100-240VAC	1 Amp @ 115VAC	115 Watts	17.40" x 1.75" x 13.45" 441.96mm x 88.14mm x 341.63mm
M1G2 ADE	2U; up to 12 TAP s	Dua l Internal DC	36-60VDC	.8 Amps @ 48VDC	134 Watts	
M1GC*	Management card: E ternet/GUI -and- Serial/CLI for M1Gx xxE					
*Blanking plates are used if the management card is n ot required or if not all the TAP slots are not all populated.						

Caution: This unit may have up to 2 power supply connections. Disconnect all power supply cords before servicing to prevent electrical shock or equipment damage.

Caution: For the AC powered chassis: for continued protection, only replace fuse with a 2Amp slow blow 5x20mm fuse. (Cooper Bussmann # S56 0-800-R or equiv.)

M1GXXF Filtering TAP Specifications									
Model #	Network Speed	Media		Modes					Link Speed Synchronization
		Network	Monitor	Breakout	Aggregation	SPAN/Regen	Filtering	Bypass	
M1GCCF	10/100/1000M	2 Copper-RJ -45	2 Copper RJ -45 conn	X	X	X	X	N/A	Yes
M1GCS F	10/100/1000M	2 Copper-RJ -45	2 SFP Transceivers	X	X	X	X	N/A	Yes
M1GMC F	1G	2 S X M/M, Passive LC Fiber	2 Copper RJ -45 conn	X	X	X	X	N/A	N/A
M1GMS F	1G	2 S X M/M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A
M1GSC F	1G	2 LX S /M, Passive LC Fiber	2 Copper RJ -45 conn	X	X	X	X	N/A	N/A
M1GSS F	1G	2 LX S /M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A

M1GXXA - Breakout, Aggregation, and SPAN/Regeneration TAP Specifications									
Model #	Network Speed	Media		Modes					Link Speed Synchronization
		Network	Monitor	Breakout	Aggregation	SPAN/Regen	Filtering	Bypass	
M1GCC A	10/100/1000M	2 Copper-RJ -45	2 Copper-RJ -45 conn	X	X	X	X	N/A	Yes
M1GCS A	10/100/1000M	2 Copper-RJ -45	2 SFP Transceivers	X	X	X	X	N/A	Yes
M1GMCA	1G	2 S X M/M, Passive LC Fiber	2 Copper RJ -45 conn	X	X	X	X	N/A	N/A
M1GMS A	1G	2 S X M/M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A
M1GSC A	1G	2 LX S /M, Passive LC Fiber	2 Copper RJ -45conn	X	X	X	X	N/A	N/A
M1GSA	1G	2 LX S /M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A

M1GXXBP – Breakout, Aggregation, SPAN/Regeneration, and Bypass TAP Specifications									
Model #	Network Speed	Media		Modes					Link Speed Synchronization
		Network	Monitor	Breakout	Aggregation	SPAN/Regen	Filtering	Bypass	
M1GCCB P	10/100/1000M	2 Copper-RJ -45	2 Copper-RJ -45 Conn	X	X	X	X	N/A	Yes
M1GCS BP	10/100/1000M	2 Copper-RJ -45	2 SFP Transceivers	X	X	X	X	N/A	Yes
M1GMCB P	1G	2 S X M/M, Passive LC Fiber	2 Copper RJ -45 conn	X	X	X	X	N/A	N/A
M1GMS BP	1G	2 S X M/M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A
M1GSCB P	1G	2 LX S /M, Passive LC Fiber	2 Copper RJ -45 conn	X	X	X	X	N/A	N/A
M1GSSBP	1G	2 LX S /M, Passive LC Fiber	2 SFP Transceivers	X	X	X	X	N/A	N/A

13 Definitions and Help

Definitions:

S MF	Singlemode Fi ber Network Ports
MMF	Multimode Fi ber Network Ports
RJ -45	Copper Port
S FP	Transce iver Port – 1Gbp s
LFP	Link Fa ilure Propagation - LF P is use d mostly for HA de signed networks. When turned on, it can sen se a network failure and reflect the failure to the adjacent port of the live network allowing the network’s failover mechanism to switch ov er to the seco ndary network path.
Reverse Bypass	Disab les li nk on both live network ports if all inline appliances lo se li nk or cannot pass traffic. Disab led by default.
Forced Bypass	Allows the In-line appliance to be bypassed whenever firmware or software upgrades nee d to be installed.

Help:

Pressing ‘h’ on Filtering Menu will bring up the help Screen

```

----- CURSOR MOVEMENT -----
<home>.....Place cursor at the beginning of the filter list
<end>.....Place cursor at the end of the filter list
<pg up>.....Move cursor forward a page in the filter list
<pg dn>.....Move cursor backward a page in the filter list
U,u,<up arrow>.....Move cursor up one position in the filter list
D,d,<down arrow>.....Move cursor down one position in the filter list

----- FILTER MOVEMENT -----
T,t.....Move selected filter on the list (increases priority)
G,g.....Move selected filter down on the list(decreases priority)

----- FILTER MODIFICATION -----
E,e.....Edit selected filter
A,a.....Add a new filter to the end of the list
<F1>.....Copy a selected filter
I,i,<insert>.....Insert a new filter above selected filter
X,x,<delete>.....Delete selected filter
V,v.....View details on selected filter
c.....Clear count on selected filter

----- CONTROL -----
O.....Exit row filtering menu
C.....Clear counts on all filters this row
R,r.....Reset filters to factory default, deletes all filters
this row
S,s.....Save this row’s filter list to flash, and apply it to
modules

```

Figure 167: Help Sc reen for the F iltering Menu

14 Console Cable for M1GXX C E Serial Mgt. port

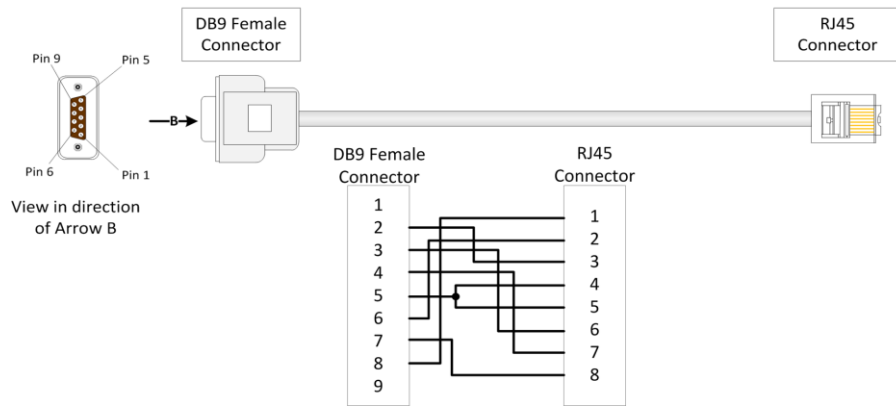


Figure 168: Serial Cable Pinout

For questions, please contact Garland Technology Support at:

Technical Support:

8AM-9PM (CST) Monday – Friday (except for observed US Holidays)

Tel: 716.242.8500

Email Address: support@garlandtechnology.com