Garland Technology

EdgeSafe™: 40G Bypass Modular Network TAP

User Guide

M40G1AC, M40GMSBP, M40GSSBP, M10GMS2BP, M10GSS2BP

GARLAND
TECHNOLOGY
See every bit, byte, and packet®

New York | Texas | Germany | Australia
Office: 716-242-8500
support@garlandtechnology.com
garlandtechnology.com

REVISION HISTORY

Revision	Date	Change description
1.0	15-Jun-13	M40GBP guide – Initial version
1.1	4-Mar-14	Adding info for 10G modules
1.2	18-Aug-14	Add support for Dual rate 10G/1G bypass segment
1.3	11-Feb-15	Update LED specification
1.4	3-Apr-16	FW -1.0.3
1.5	16-Nov-16	FW-1.0.5
1.6	2-Jul-17	FW-1.2.6

Table of Contents

1 INTRODUCTION 9
1.1 TARGET RELEASE 9
2 FEATURES 11
2.1 GENERAL 11
2.2 BYPASS MODES 12
2.3 APPLICATION FAILURE (HEARTBEAT) 13
2.4 MONITOR LINK FAILURE 14
2.5 POWER FAILURE 14
2.6 TAP MODE 15
2.7 TAPI12 MODE 16
2.8 TAPA MODE 17
2.9 TAPAI1 MODE 18
2.10 TAPAI2 MODE 19
2.11 TAPAI12 MODE 20
2.12 LINKDROP MODE 21
2.13 TWO PORT LINK (2PL) 22
2.14 RESTORE FROM ACTIVE EXPIRE STATE 22
2.15 HEARTBEAT ACTIVE MODE 22
3 FRONT PANELS 23
3.1 M40G1AC – M40G1AC WITH 3 EDGESAFE 40G MODULES 23
3.2 M40G1AC – MANAGEMENT PANEL 23
3.2.1 Bypass Switch 1U Host System LEDs & Switches Specifications 23
3.3 M40GBP MODULE 25
3.3.1 M40GMSBP4/ M40GSSBP4: LED and Connector Specifications 25
3.4 M40GBP MODULE 26
3.4.1 M10GMS2BP/ M10GSS2BP: LED and Connector Specifications 26
4 REAR PANELS 27
4.1 M40G1AC - M40G1AC – REAR PANEL 27
5 GARLAND TECHNOLOGY INTELLIGENT BYPASS SWITCH INSTALLATION 28
5.1 RACK MOUNT THE M40GBP 28
5.2 CONNECTING POWER TO THE 220V/110V M40GBP UNIT 28
5.2.1 Connect two power cables to the power supplies on to the back of the M40GBP. The PWR led's on the front panel of the M40GBP will illuminate when switching on the power switch power. 28
5.3 CONNECTING POWER TO THE -48VDC M40GBP UNIT 28
5.3.1 Verify that the power is OFF on the DC power source 28
5.3.2 Verify that the power switch on the M40GBP unit is OFF 28
5.3.3 Connect the DC input wires to the DC input terminal on the M40GBP as follows: 28
5.4 CONNECTING THE RS232 DB9 MANAGEMENT CABLE 29
5.5 CONNECTING THE ETHERNET MANAGEMENT PORT 29
6 COMMAND LINE INTERFACE (CLI) 30
6.1 MAIN MENU 30
6.2 COMMANDS LIST 31
6.3 GET DEVICE PROPERTIES (GET_DEV_PROP) 32
6.4 GET/SET SEGMENT (GET/SET_SEG) 32
6.5 HEARTBEAT ACTIVE MODE. (HB_ACT_MODE) 33
6.6 ACTIVE BYPASS MODE 34
6.7 TWO PORT LINK (2PL) 35
6.8 MONITOR PORTS TWO PORT LINK (M2M) 35

6.9 HB_INTERVAL (HB_INTERVAL) 36
6.10 HB_HOLDTIME (HB_HOLDTIME) 37
6.11 KEEP HEARTBEAT ACTIVE MODE (KEEP_HB_ACT_MODE) 37
6.12 HEARTBEAT EXPIRATION STATE (HB_EXP_STATE) 38
6.13 RESTORE FROM HEARTBEAT EXPIRATION EVENT (EN_ACT_HB_RESTORE) 39
6.14 CHANGE BYPASS STATE ON RX/TX ERROR DETECTION (RX_TX_ERR_MODE) 40
6.15 LAG CONFIGURATION 41
CONFIGURING THE LAGS 42
6.15.1 Get lag (get_lag) 42
6.15.1 Add lag Get lag (add_lag_member) 42
6.15.2 Set minimum lag working members (set_lag_min_work_members) 43
6.15.1 Delete lag members (del_lag_members) 44
6.15.2 Delete lag (del_lag) 44
6.16 SELECTIVE BYPASS FILTERS 45
6.16.1 White list – redirect 46
6.16.2 Black list – redirect 47
6.16.3 Black list – drop 48
6.16.4 Defune the selective bypass mode (set_slct_bypass_mode) 49
6.16.5 Add selective bypass rule (add_slct_bypass) 49
6.16.6 Delete skective bypass filter (del_slct_bypass) 50
6.16.7 Set selective bypass on/off (set_slct_bypass on/off) 50
6.16.8 Get selective bypass on/off (set_slct_bypass on/off) 50
6.16.9 Get selective bypass rule list (get_slct_bypass rule_list) 50
6.16.10 Get selective bypass filter (get_slct_bypass filter) 50
6.16.11 get_slct_bypass x_range (get_slct_bypass x_range first last [on|off] [group]) 51
6.17 ETHERNET MANAGEMENT PORT IP ADDRESS 52
6.18 ETHERNET MANAGEMENT PORT NET MASK ADDRESS 52
6.19 ETHERNET MANAGEMENT PORT GATEWAY IP ADDRESS 53
6.20 TIME 53
6.21 SYSTEM USER (SET_USER) 54
6.22 SYSTEM PASSWORD (SET_PSW) 54
6.23 UNIT NAME. 54
6.24 WHO AM I (WHOAMI) 55
6.25 DISPLAY EDGESAFE 40G VERSIONS (GET_VER) 55
6.26 DISPLAY EDGESAFE 40G PARAMETERS (GET_PARAMS) 56
6.27 DISPLAY EDGESAFE 40G STATE (GET_DEV_STATE) 57
6.28 DISPLAY DEVICE HARDWARE VERSION (GET_HW_VER) 59
6.29 DISPLAY DEVICE FIRMWARE VERSION (GET_FW_VER) 59
6.30 DISPLAY DEVICE TRACKING NUMBER (GET_DEV_TK_NUM) 59
6.31 DISPLAY DEVICE HEALTH STATE (GET_HEALTH) 60
6.32 DISPLAY APPLICATION STATE (GET_APPL_STATE) 61
6.33 DISPLAY RS232 TERMINAL CONNECTION STATE (GET_TERM_STATE) 61
6.34 DISPLAY/CHANGE RS232 TERMINAL PORT SPEED (GET/SET_RS232_SPEED) 61
6.35 DISPLAY ETHERNET PORT STATE (GET_LINK) 61
6.36 DISPLAY DEVICE LOG FILE (GET_LOG) 62
6.37 RESET LOG FILE (RESET_LOG) 63
6.38 RESET ERROR CONDITION (RESET_ERR) 63
6.39 GET FIRST ERROR (GET_FIRST_ERROR) 63
6.40 GET LAST ERROR (GET_LAST_ERROR) 63
6.41 SET DEFAULT PARAMETERS (SET_DEFAULT) 64
6.42 REBOOT 65
6.43 GET/SET WEB HTTPS STATE (WEB_HTTPS_STATE) 66

6.44 REPLACING THE DEFAULT CERTIFICATE FOR THE WEB UI (SET_CERT) 66
6.44.1 Restore the factory default certificate for the web UI (set_cert) *66*
6.45 GET/SET MANAGEMENT SESSION TIMEOUT (SESSION_EXP_TIME) 67
6.46 GET/SET ETHERNET MANAGEMENT PORT STATUS (MGMT_PORT_STATE) 67
6.47 GET/SET SEGMENT LINK SPEED (GET/SET_SEG_SPEED) 68
6.48 HEARTBEAT PACKET 69
6.48.1 Get heartbeat packet content *69*
6.48.2 Load Heartbeat packet content *69*
6.48.3 Restore default heartbeat packet content *69*
6.48.4 Get/Set heartbeat packet transmit direction *70*
6.48.5 Get/Set criteria for determine heartbeat packet failure. *70*
6.49 REMOTE LOG 71
6.49.1 Get remote log state *71*
6.49.2 Set remote log state *71*
6.49.3 Get remote log server IP *71*
6.49.4 Set remote log server IP *71*
6.50 NTP (NETWORK TIME PROTOCOL) 72
6.50.1 Get NTP state *72*
6.50.2 Set NTP state *72*
6.50.3 Get NTP server IP *72*
6.50.4 Set NTP server IP *72*
6.50.5 Add NTP server IP *73*
6.50.6 Delete NTP server IP *73*
6.50.7 Send NTP request *73*
6.51 TIMEZONE 74
6.51.1 Get timezone list *74*
6.51.2 Get timezone *75*
6.51.3 Set timezone *75*
6.51.4 Get daylight saving state *76*
6.52 GET TECHNICAL SUPPORT INFORMATION. 76
6.53 WEB USER 80
6.53.1 Get WEB user name *80*
6.53.2 Set WEB user name *80*
6.53.3 Set WEB user password *80*
6.54 MULTI CONFIGURATION MECHANISM 80
6.54.1 Display saved EDGESAFE 40G configurations. *80*
6.54.2 Save EDGESAFE 40G configuration. *80*
6.54.3 Restore the EDGESAFE 40G saved configuration. *81*
6.54.4 Remove saved configuration. *81*
6.55 TELNET ACCESS 81
6.56 STATISTICS COUNTERS. 81
6.57 TACACS+ (TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTEM PLUS) AND RADIUS (REMOTE AUTHENTICATION DIAL IN USER SERVICE) SUPPORT. 83
6.57.1 TACACS+/RADIUS state *83*
6.57.2 Set TACACS+ / RADIUS server IP *84*
6.57.1 Add TACACS+ server IP *84*
6.57.1 Del TACACS+ server IP *84*
6.57.1 Get TACACS+ server IP *85*
6.57.1 Set RS232 TACACS+ login *85*
6.57.2 Get RS232 TACACS+ login *85*
6.57.3 Set TACACS+ login fallback *86*
6.57.4 Get TACACS+ login fallback *86*

6.57.5 Set TACACS+ / RADIUS secret key 86
6.57.6 Set TACACS multi users flag 86
6.57.7 Display TACACS multi users flag 87
6.57.8 Set RADIUS authentication port 87
6.57.9 Display RADIUS authentication port 87
6.58 PERMITTED IP SUPPORT. 87
6.58.1 Set/delete permitted IP range 88
6.58.2 Display permitted IP range 88
6.58.3 Check permitted IP range 88
6.58.4 Display current user 89
6.59 M2N MODE 89
6.60 DISPLAYING POWER SUPPLIES STATES. 89
6.60.1 Module power off. 90
6.61 GET/SET INTERNAL VLAN ID 90
6.62 SNMP 91
6.62.1 SNMP_Enrty commands 91
get_snmp_entry To view the current SNMP entry or the view all entries use the command:
get_snmp_entry [entry_index|all] - 91
6.62.2 add_snmp_entry - Add new SNMP entry (up to 11 different entries) 92
6.62.3 Select SNMP entry - sel_snmp_entry - 93
6.62.4 Set/get_snmp_user 94
set_snmp_user XXX - set snmp user name (5 - 30 symbols) 94
6.62.5 snmp version 95
6.62.6 snmp server ip 96
6.62.7 get_snmp_srv_ip 96
6.62.8 add_snmp_srv_ip 97
6.62.9 del_snmp_srv_ip 98
6.62.10 set_snmp_srv_ip - modify the IP address of the main SNMP server 99
6.62.11 snmp community access – get/set_snmp_access 100
6.62.12 snmp password – set_snmp_user_psw 101
6.62.13 snmp community status (get/set_snmp_status) 101
6.62.14 SNMP TRAP IP port - get/set_snmp_trap_port 102
6.62.15 SNMP MSG IP port - get/set_snmp_msg_port 102
6.63 GET/SET SNMP TRAPS ENABLE STATE. (GET/SET_TRAP) 108
6.64 SNMP TRAPS. 110
6.65 SNMP REQUEST EXAMPLES (NET-SNMP APPLICATION) 112
6.66 DISPALYING LOG FILE VIA SNMP 112
6.67 SNMP AGENT, NET-SNMP AND COPYRIGHT 112
7 WEB INTERFACE 113
7.1 DISABLE/ENABLE WEB INTERFACE. 113
7.2 STARTING WEB INTERFACE 114
7.3 LOGIN 114
7.4 INFORMATION PAGE 115
7.4.1 Logoff 115
7.4.2 Module:segment 115
7.4.3 Information area description. 116
7.5 HEALTH PAGE 117
7.5.1 Health status 117
7.6 BYPASS PAGE 118
7.6.1 Bypass configuration area description 118
7.6.2 Advanced features configuration area 119
7.6.3 RX/TX errors processing 120

7.7 FILTERS 122
7.8 SYSTEM PAGE 124
7.8.1 System configuration area 124
7.8.2 TACACS+ / RADIUS configuration area 125
7.8.3 Time configuration area 126
7.8.4 NTP configuration area 126
7.8.5 Ethernet management port area 127
7.9 LAG 128
7.10 ACCOUNT PAGE 129
7.10.1 Interface 129
7.10.2 User/community name 129
7.10.3 Password 129
7.10.4 Session timeout 129
7.11 SNMP PAGE 130
7.11.1 SNMP Entry 130
7.11.2 SNMP server IP address 130
7.11.3 SNMP version 130
7.11.4 Access 131
7.11.5 Name 131
7.11.6 Status 131
7.11.7 SNMP control port 131
7.11.8 SNMP trap account 131
7.11.9 SNMP trap account allow to add/remove/view additional destinations for SNMP traps.SNMP trap control 131
7.12 LOG FILE PAGE 133
7.12.1 Log file control area 133
7.12.2 Remote log file control area 134
7.13 HB PACKET PAGE 135
, 136
7.14 RESCUE PAGE 136
7.14.1 Device firmware update area 137
7.14.2 System restore are 137
7.14.3 Technical support area 137
8 APPENDIXES 138
8.1 BYPASS SPECIFICATIONS 140
8.2 PRODUCTION DEFAULT CONFIGURATION 140
9 TECHNICAL SPECIFICATIONS: 141
9.1 M40G1AC 141
9.1.1 M40G1AC: Bypass Switch 1U Host System Technical Specifications 141
9.1.2 M40G1AC: Bypass Switch 1U Host System LEDs & Switches Specifications 142
9.2 M40GMSBP (50UM) 144
9.2.1 Fiber Gigabit Ethernet Technical Specifications - (40GBase-SR4) Adapters: 144
9.2.2 M40GMSBP and : LED and Connector Specifications 144
9.3 M40GSSBP ..... **ERROR! BOOKMARK NOT DEFINED.**
9.3.1 Fiber 40Gigabit Ethernet Technical Specifications - (40GBase-LR4) Adapters: 145
9.3.2 M40GSSBP and : LED and Connector Specifications 145
9.4 M10GMS2BP ..... **ERROR! BOOKMARK NOT DEFINED.**
9.4.1 Dual rate Fiber 10G/1G Ethernet Technical Specifications - (10GBase-SR / 1000Base-SX) Adapters: 146
9.5 M10GSS2BP ..... **ERROR! BOOKMARK NOT DEFINED.**
9.5.1 Dual rate Fiber 10G/1G Ethernet Technical Specifications - (10G Base-LR / 100BaseLX) Adapters: 147

9.5.2 M10GMS2BP/ M10GSS2BP: LED and Connector Specifications 147
10 SAFETY PRECAUTIONS 147
10.1.1 Safety considerations for the M40GBP rack mounting: 148
10.2 TFTP SERVER INSTALLATION AND CONFIGURATION. 149
10.2.1 Windows TFTP server installation and configuration 149
10.2.2 Linux TFTP server installation and configuration 149
10.3 NET-SNMP COPYRIGHT. 150
10.4 TACACS+ COPYRIGHT. 154
1.1 RADIUS COPYRIGHT 156

List of figures

Figure: 1. M40GBP Normal Mode. 13
Figure: 2. M40GBP Passive Mode. 14
Figure: 3. M40GBP TAP Mode. 15
Figure: 4. M40GBP TAPI12 Mode. 16
Figure: 5. M40GBP TAPA Mode. 17
Figure: 6. M40GBP TAPAI1 Mode. 18
Figure: 7. M40GBP TAPAI2 Mode. 19
Figure: 8. M40GBP TAPAI12 Mode. 20
Figure: 9. M40GBP Linkdrop Mode. 21
Figure: 10. M40GBP front panel. 23
Figure: 11. M40GBP front panel. 23
Figure: 12. M40GBP module front panel 25
Figure: 13. M40GBP module front panel 26
Figure: 14. M40GBP rear panel. 27
Figure: 15. LAG topology with 4 segnemts 41
Figure: 16. White list – redirect 46
Figure: 17. Black list – redirect 47
Figure: 18. Black list – drop 48

1 Introduction

EdgeSafe 40G Bypass Modular Network TAP is second generation of an active external Bypass TAP that protects network integrity from network failures and network maintenance. The Garland Technology intelligent Bypass TAP is a self-generating heartbeat and controls the network switch mode of operation.

The Garland Technology M40GBP is a 1U host system which supports up to three modules. The 1U host system can support mix of 40G Bypass module and dual rate 10G/1G Bypass modules. A 40G module supports one Bypass segment per module. A dual rate 10G/1G Bypass module supports two Bypass segment in a module.

The Garland Technology M40GBP supports 40 Gigabit Ethernet Multimode Fiber (40GBase-SR4) and 40 Gigabit Single mode fiber (40GBase-LR4) network standards. Each 40G Bypass module includes two MPO / LC ports for network ports, and two QSFP+ ports for the attached in-line network system.

The Garland Technology M40GBP supports dual rate 10/1 Gigabit Ethernet Multimode Fiber (10GBase-SR , 1000Base-SX) and 10/1 Gigabit Single mode fiber (10GBase-LR, 1000Base-LX) network standards. Each 10G Bypass module Network includes four LC Duplex Monitor ports and four SFP+ ports for the attached in-line network system.

1.1 Target release

EDGESAFE 40G:	**Number of Bypass modules:**	**module:**	**Power Supply**	**Power cord**
Intelligent 40G Bypass Switch 1U Box	*1: one modules* *2: two modules* *3: three modules*	• 40G module with Bypass will show BSR4 or BQLR4 • 10G (8 ports) module with bypass will show BSR or BLR	*Blank: 90-240 VAC, Redundant – hot swap* *-48V DC*	*Blank: No power cord* *-EU* *-US* *-CN*

P/N:	**Description:**	**Notes:**
M40G1AC-US	Bypass Switch 1U Host System	90-240 VAC Auto-Select, US cable
M40G1AC -48V	Bypass Switch 1U Host System	Power supply -48VDC
M40GMSBP	40G Gigabit (SR4) fiber Intelligent Bypass Switch module	SR4 MMF Single Segment Bypass 40G – (SR4 on the Network and Monitor ports)
M40GSSBP	40G Gigabit (LR4) fiber Intelligent Bypass Switch module	LR4 SMF Single Segment Bypass 40G – (LR4 on the Network and Monitor ports)
M40GMSBP	Intelligent 40G 1U system with 40G (SR4) Bypass Switch module	1U Switch , 40G SR4 MMF Single Segment

		Bypass , 90-240 VAC Auto-Select, EU cable
M40GSSBP	Intelligent 40G 1U system with 40G (LR4) Bypass Switch module	1U Switch , 40G, LR4 SMF, Single Segment Bypass, 90-240 VAC Auto-Select, US cable
M40GSSBP	Intelligent 40G system with one (LR4) Bypass Switch module	1U Switch , 40G, LR4 SMF, Single Segment Bypass and 40G SR4 MMF Single Segment Bypass, 90-240 VAC Auto-Select, US cable
M10GMS2BP	Dual segment 10G/1G Gigabit (SR/SX) fiber Intelligent Bypass Switch	SR/SX MM Dual Segment Bypass, Dual rate 10G/1G – (SR/SX on the Network and Monitor ports)
M10GSS2BP	Dual segment 10G/1G Gigabit (LR/LX) fiber Intelligent Bypass Switch module	LR/LX SM Dual Segment Bypass, Dual rate 10G/1G – (LR/LX on the Network and Monitor ports)
M10GMS2BP	Intelligent 40G with one 10G (SR) Bypass Switch module	1U Switch , with 10G/1G SR/SX MMF dual Segment Bypass , 90-240 VAC Auto-Select, EU cable
M10GMS2BP	Intelligent 40G with one 10G (SR) Bypass Switch module	1U Switch , 10G/1G, LR/LX SM, dual Segment Bypass, 90-240 VAC Auto-Select, US cable
M10GSS2BP	Intelligent 40G with one dual rate 10G/1G (SR/SX) Bypass Switch module and one dual rate 10G/1G (LR/LX) Bypass Switch module	1U Switch , 10G/1G SR/SX MM dual Segment Bypass and 10G/1G, LR/LX SM, dual Segment Bypass , 90-240 VAC Auto-Select, EU cable

2 Features

2.1 General

The Garland Technology EdgeSafe 40G Bypass Modular Network TAP (M40GBP) supports three modes of operations: **Inline, Bypass, Tap** and **Linkdrop**. In **Inline** mode, the M40GBP diverts inline network traffic to attached in-line network system. In Bypass mode, the M40GBP does not divert the traffic to the attached in-line network system and diverts it to other network link. In **Tap** mode, incoming traffic in port NET0 is mirrored to port MON0 and incoming traffic in port NET1 is mirrored to port MON1.In **Linkdrop** mode the M40GBP disables the links on the network ports (NET0, NET1). The M40GBP simulates switch / router cable disconnection.

The M40GBP generates the heartbeat packets and transmits the heartbeat packet to the in-line Monitor / Network appliance port, the Monitor Network appliance receives the heartbeat packets and transmits is to its other port (bridges the heartbeat packet). The M40GBP detects back the heartbeat packet and maintains the **Inline** mode.

The M40GBP sets to **Bypass, Tap** or **Linkdrop** when it does not receive back the heartbeat packet from the Network / Monitor appliance. When the Network / Monitor appliance recovers, it transmits back the heartbeat packet and the Intelligent switch sets to **Inline**. The M40GBP bypasses its Ethernet Monitor ports on event of power failure, Link failure, in-line software application system hang or user request.

The M40GBP includes Double Bypass Safe architecture. The Garland Technology Double Bypass safe architecture is based on two Bypass routing circuitry: An Active Bypass circuitry and Passive Bypass circuitry. If the internal active bypass routing circuitry fails, the passive Bypass routing circuitry is activated.

The M40GBP can be configured using:

- Simple CLI configuration management via a serial communication console port, Ethernet port using Telnet or SSH.
- Web interface management interface.
- SNMP.

The Garland Technology M40GBP Bypass switch includes centralized management to all Bypass segments in the box.
The M40GBP includes two redundant 90 – 240 V AC power supply or two redundant -48 DC power supply.

2.2 Bypass Modes

The M40GBP sets to **Bypass /TAP /Linkdrop** mode when one of the following events occurs:

- Application failure (Heartbeat)
- Monitor Link failure.
- Manual Bypass.
- Power failure or power off.

2.3 Application failure (Heartbeat)

The M40GBP continuously generates heartbeat packets to the in-line Monitor / Network appliance port, the Monitor/ Network appliance receives heartbeat packets and transmits it to its other port (bridges the heartbeat packet).
As long as the M40GBP detects the heartbeat packet is received from the Monitor/ Network appliance, it will maintain the Normal / In-Line mode state.
In event of application failure (including power failure of the Monitor /Network appliance) the heartbeat packets are not transmitted back by the Monitor / Network appliance and since the M40GBP does not receive the heartbeat packet it sets to **Active Bypass** or **TAP** or **Linkdrop** mode according to the predefined settings of the heartbeat expiration state.
During **Active Bypass** and **TAP** modes the network traffic continues to flow through the network ports and is not diverted to the monitor ports. As soon as the Monitor / Network appliance recovers and starts transmitting back the heartbeat packets, the M40GBP will set to Normal / In-Line mode after detecting the heartbeat packets for period set by the "hb_holdtime" parameter.

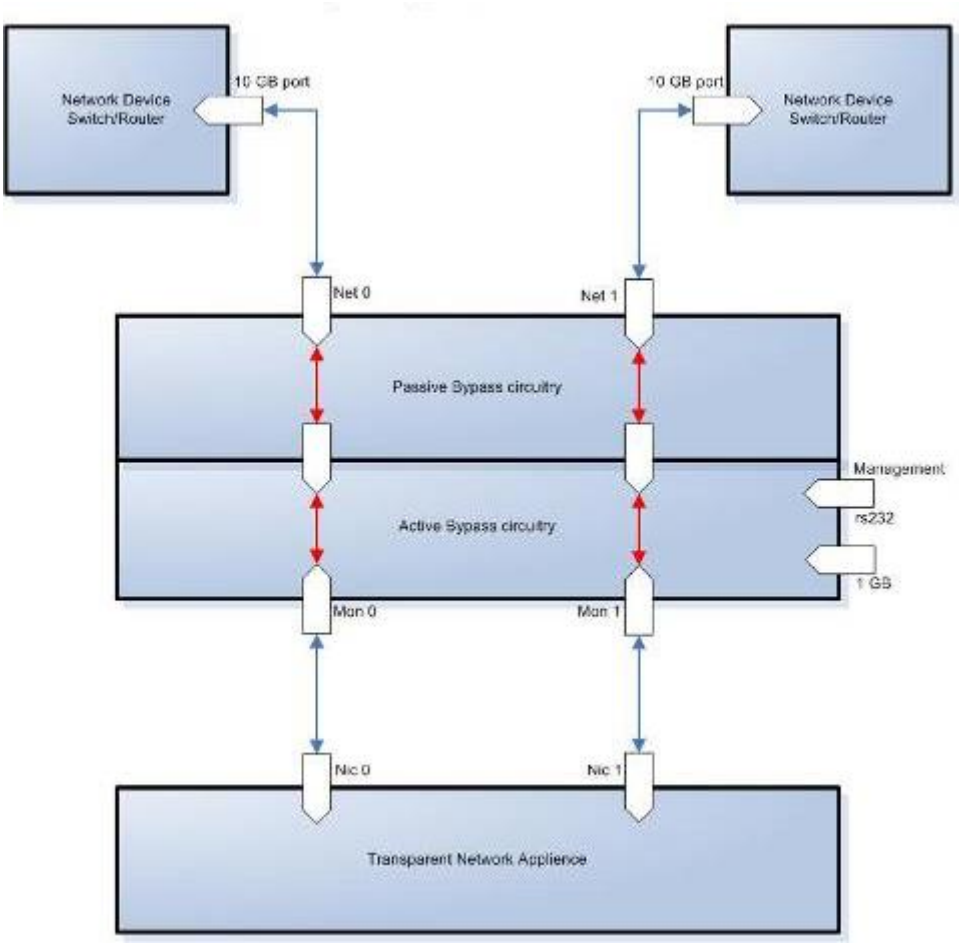


Figure: 1. EdgeSafe 40G Bypass Modular Network TAP Normal Mode.

2.4 Monitor Link failure

The M40GBP supports Monitor ports failure detection. In an event of Link failure on one of the monitor ports, the M40GBP bypasses the Ethernet ports by switching to “Active Bypass” mode. The network traffic continues to flow through the network ports and is not diverted to the monitor ports. When the Monitor link is restored, it transmits back the heartbeat packet, the M40GBP will then set to **Inline** mode state after detecting the heartbeat packets for period set by the "hb_holdtime" parameter.
The "hb_holdtime" parameter can be changed via the management port from its initial default mode.

2.5 Power Failure

The M40GBP supports Bypass on Power failure. In event of power loss the M40GBP bypasses the Ethernet ports by switching to Passive Bypass Mode. The network traffic continues to flow through the network ports and is not diverted to the monitor ports. When power is restored, the M40GBP will set to Normal / **Inline** mode state after detecting the heartbeat packets for the period set by the "hb_holdtime" parameter.
The "hb_holdtime" parameter can be change via management port from their initial default mode.

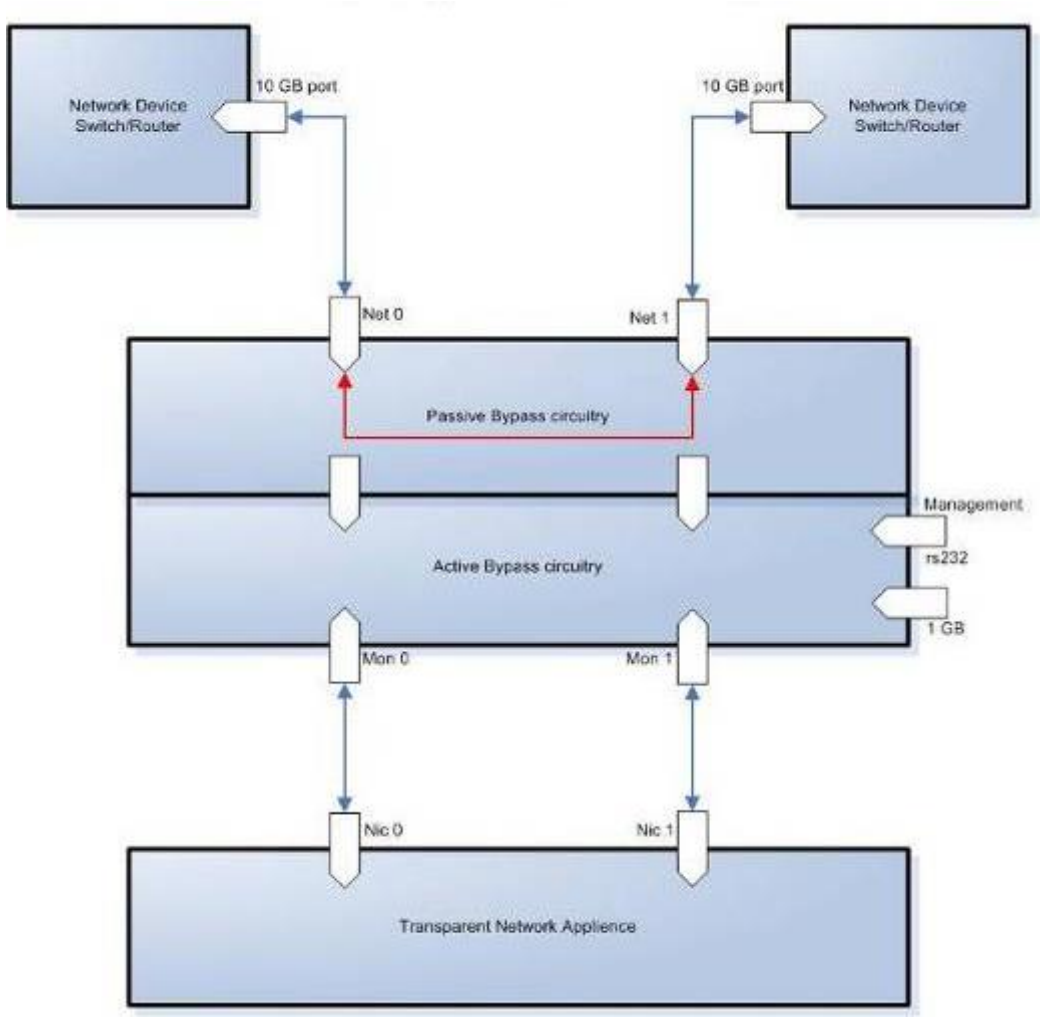


Figure: 2. EdgeSafe 40G Bypass Modular Network TAP Passive Mode.

2.6 TAP Mode

The M40GBP support TAP Mode, when it is enabled, incoming traffic in port NET0 is mirrored to port MON0 and incoming traffic in port NET1 is mirrored to port MON1.

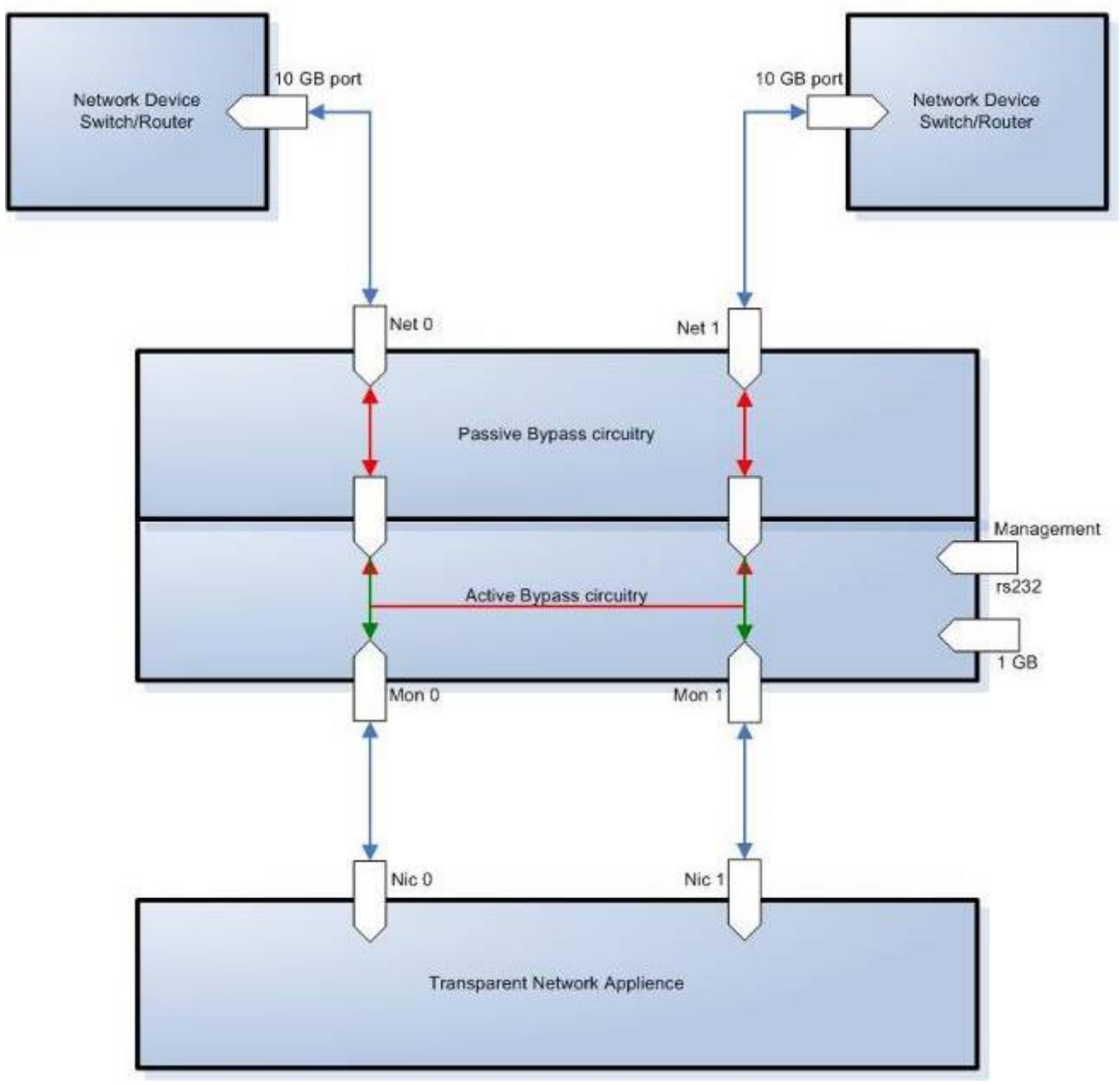


Figure: 3. EdgeSafe 40G Bypass Modular Network TAP TAP Mode.

2.7 TAPI12 mode

The M40GBP support TAPI12 Mode, when it is enabled, incoming traffic in port NET0 is mirrored to port MON0 and incoming traffic in port NET1 is mirrored to port MON1. Packets can be injected from port MON0 to port NET0 and from port MON1 to port NET1.

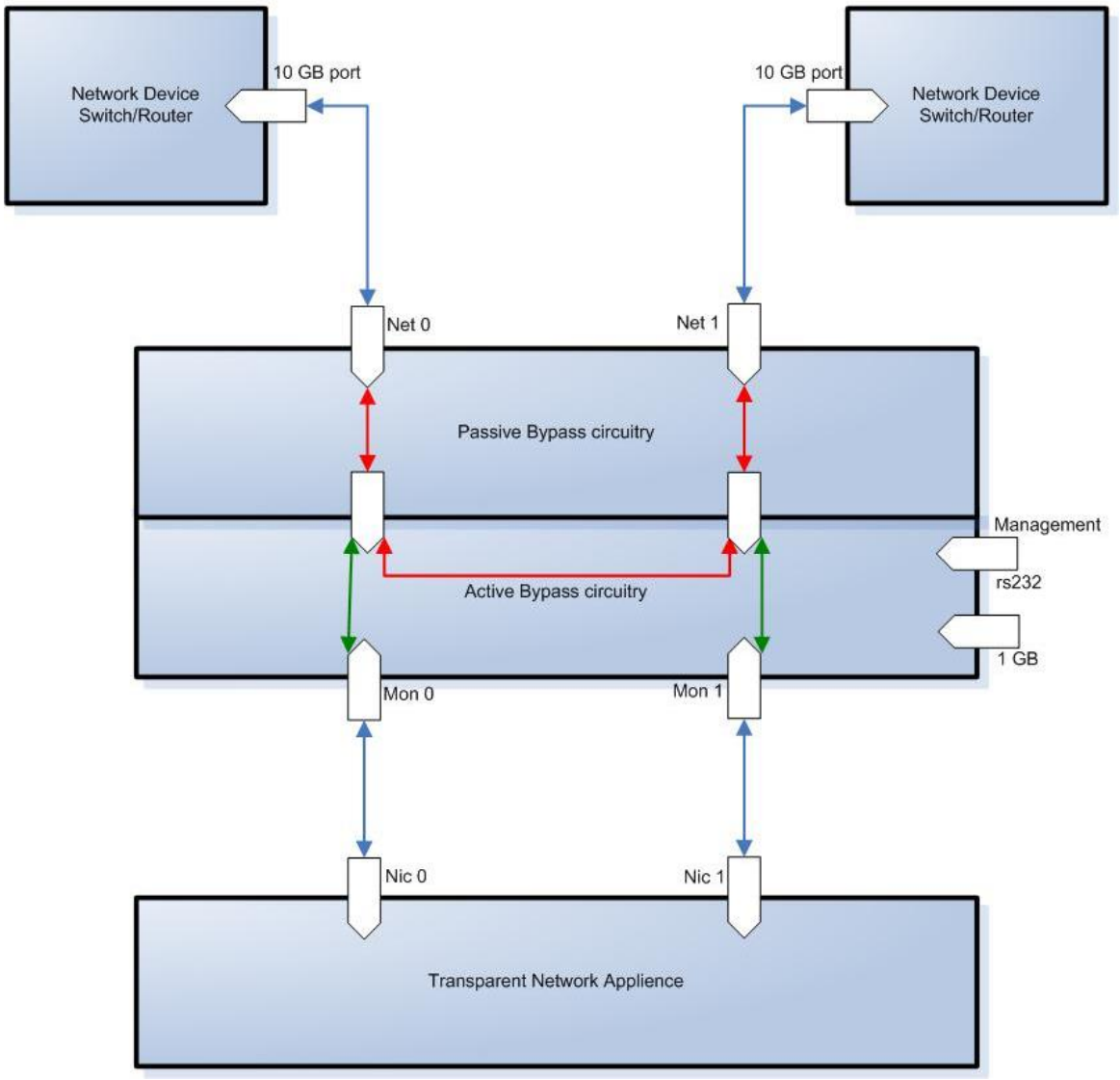


Figure: 4. EdgeSafe 40G Bypass Modular Network TAP TAPI12 Mode.

2.8 TAPA mode

The M40GBP support TAPA Mode, when it is enabled, incoming traffic in port NET0 is mirrored to both monitor ports and incoming traffic in port NET1 is mirrored to both monitor ports.

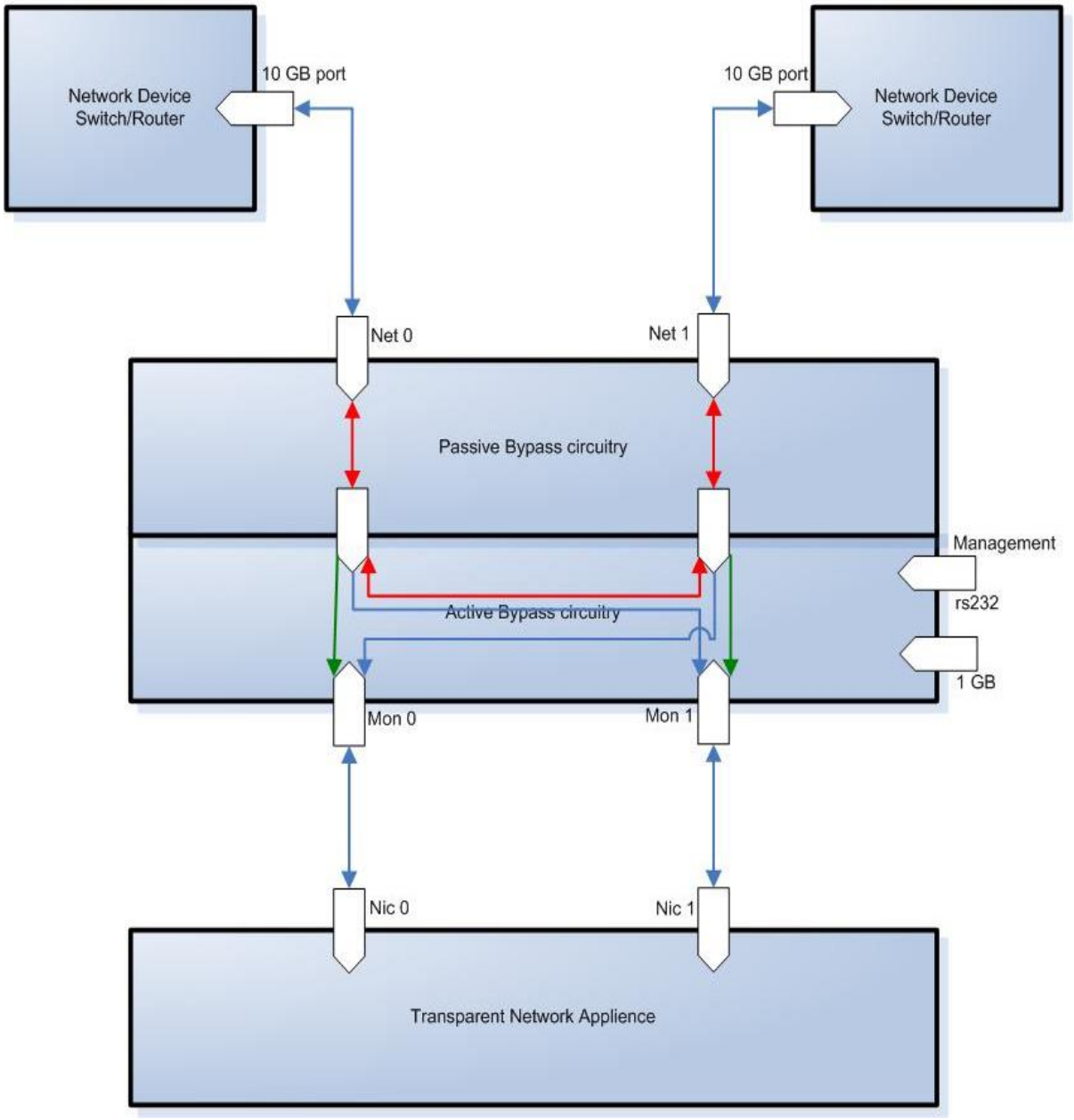


Figure: 5. EdgeSafe 40G Bypass Modular Network TAP TAPA Mode.

2.9 TAPAI1 mode

The M40GBP support TAPAI1 Mode, when it is enabled, incoming traffic in port NET0 is mirrored to both monitor ports and incoming traffic in port NET1 is mirrored to both monitor ports. Packets can be injected from port MON0 to both network ports.

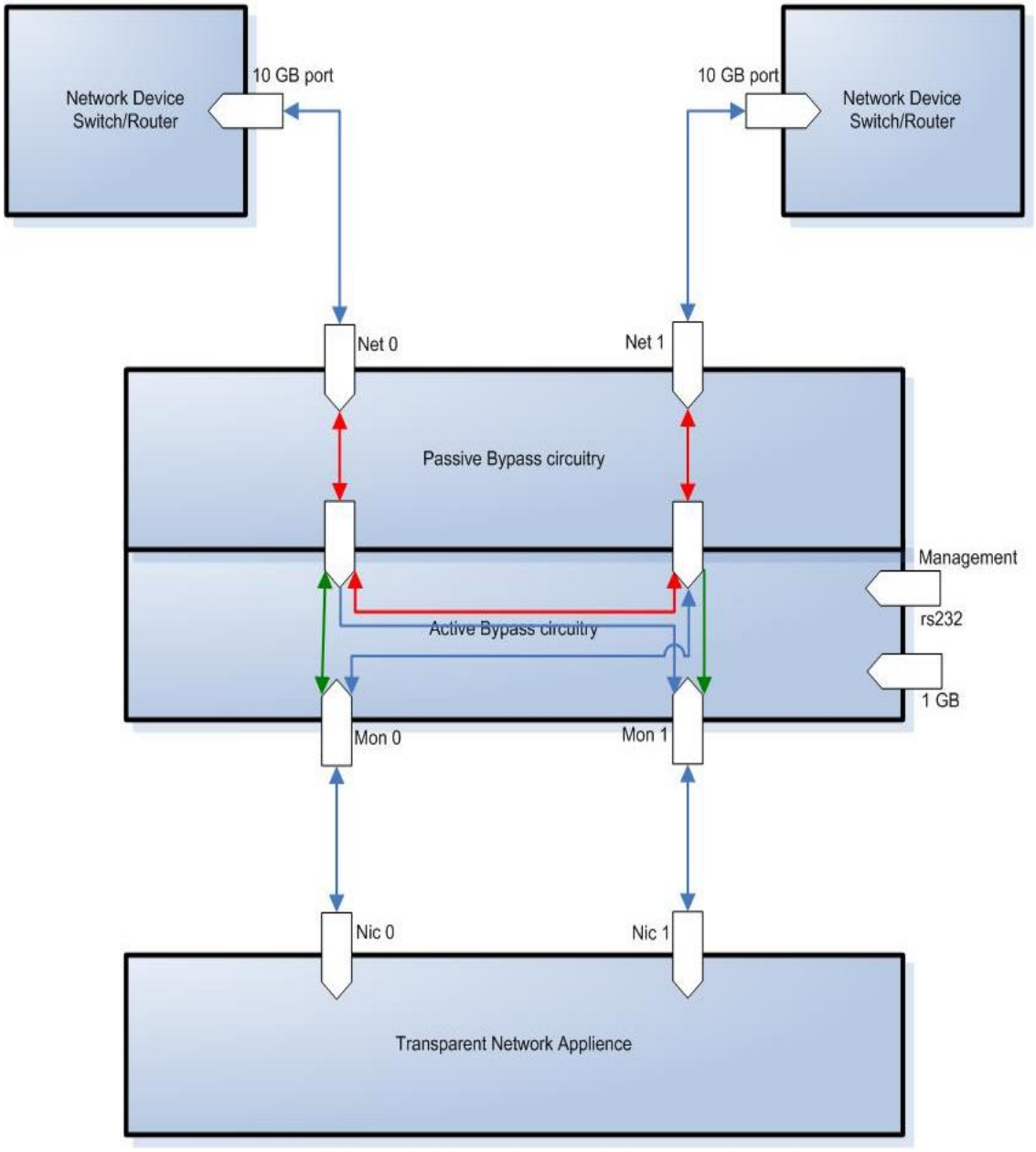


Figure: 6. EdgeSafe 40G Bypass Modular Network TAP TAPAI1 Mode.

2.10 TAPAI2 mode

The M40GBP support TAPAI2 Mode, when it is enabled, incoming traffic in port NET0 is mirrored to both monitor ports and incoming traffic in port NET1 is mirrored to both monitor ports. Packets can be injected from port MON1 to both network ports.

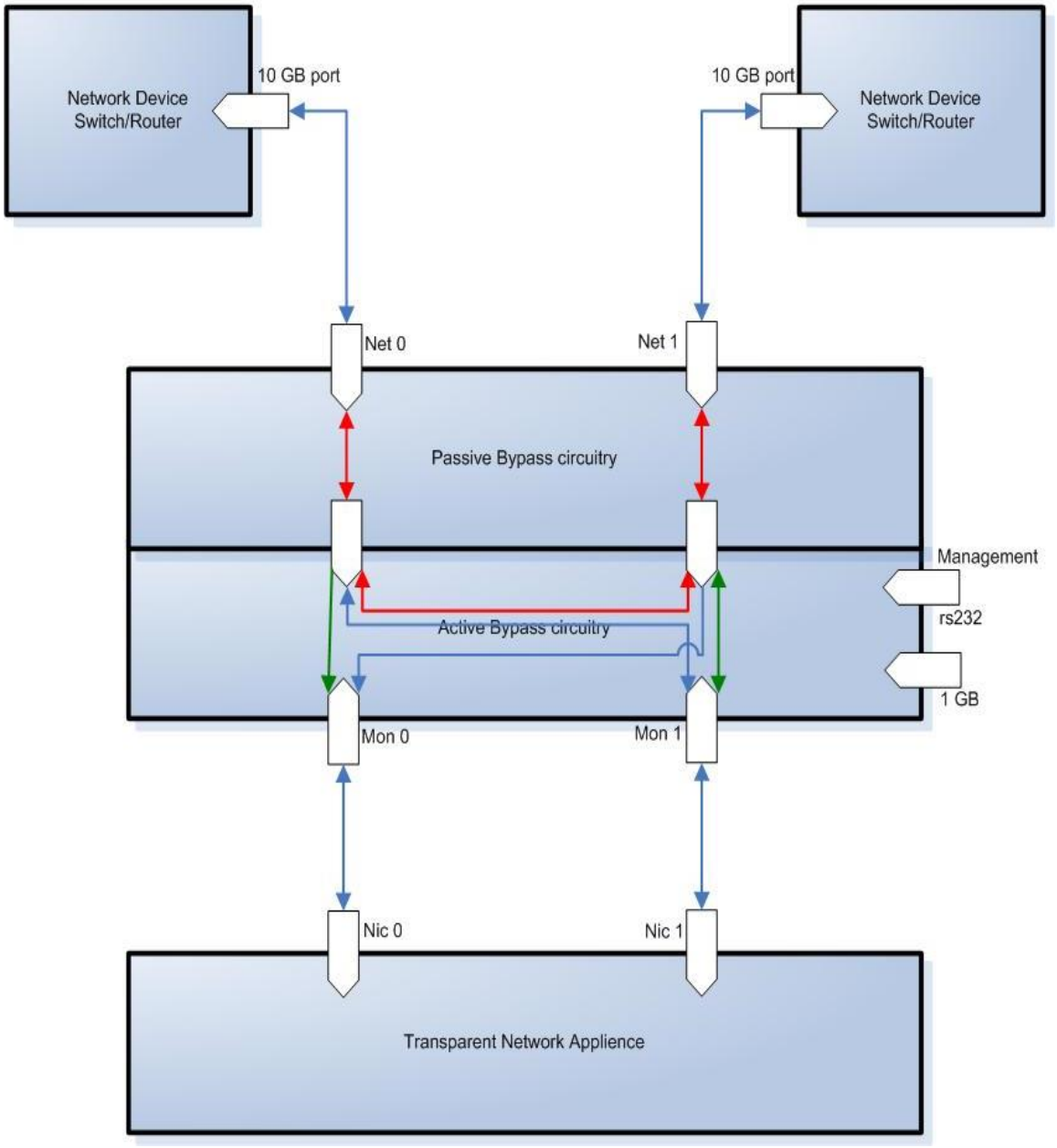


Figure: 7. EdgeSafe 40G Bypass Modular Network TAP TAPAI2 Mode.

2.11 TAPAI12 mode

The M40GBP support TAPAI12 Mode, when it is enabled, incoming traffic in port NET0 is mirrored to both monitor ports and incoming traffic in port NET1 is mirrored to both monitor ports. Packets can be injected from each monitor port to both network ports.

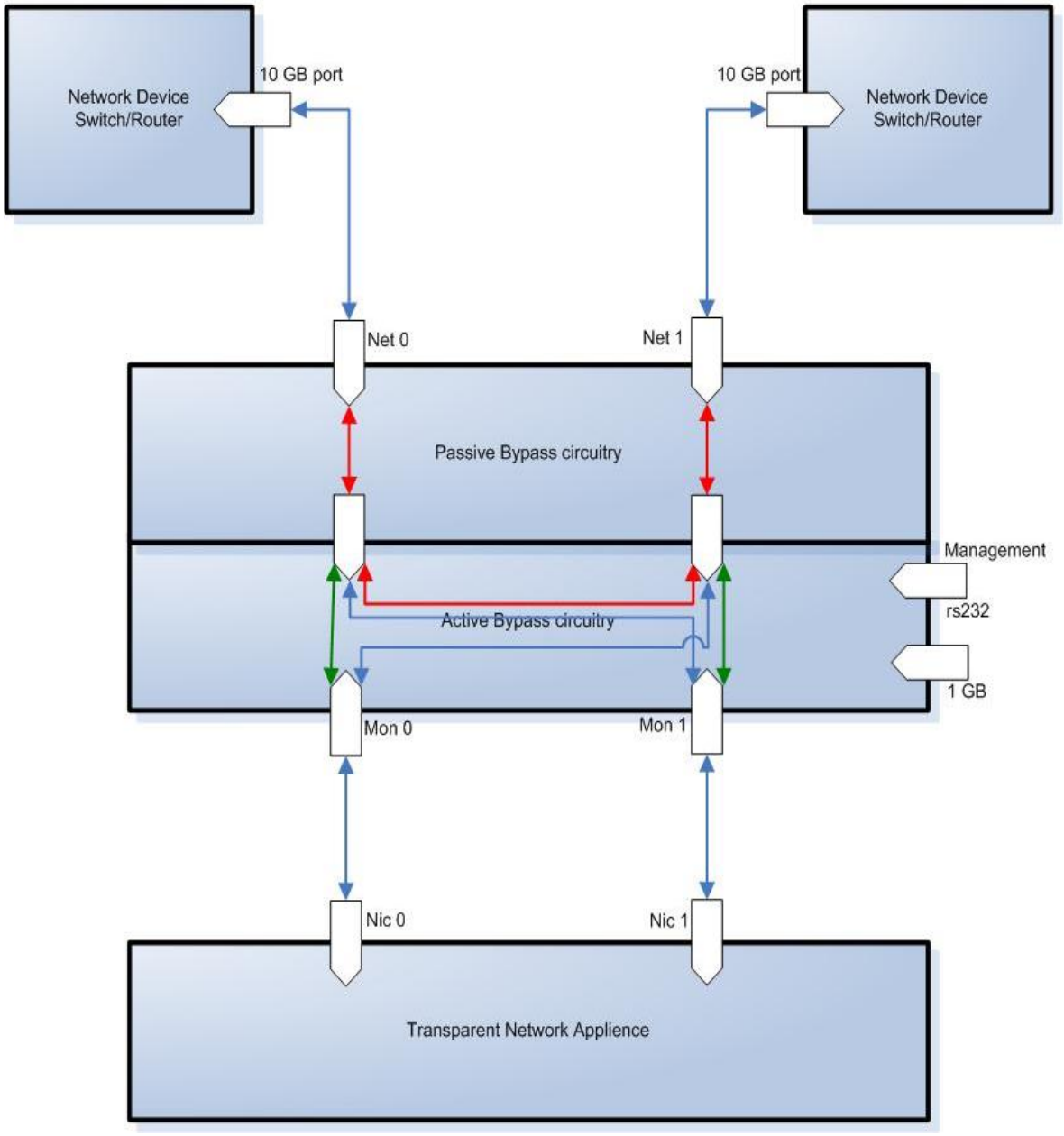
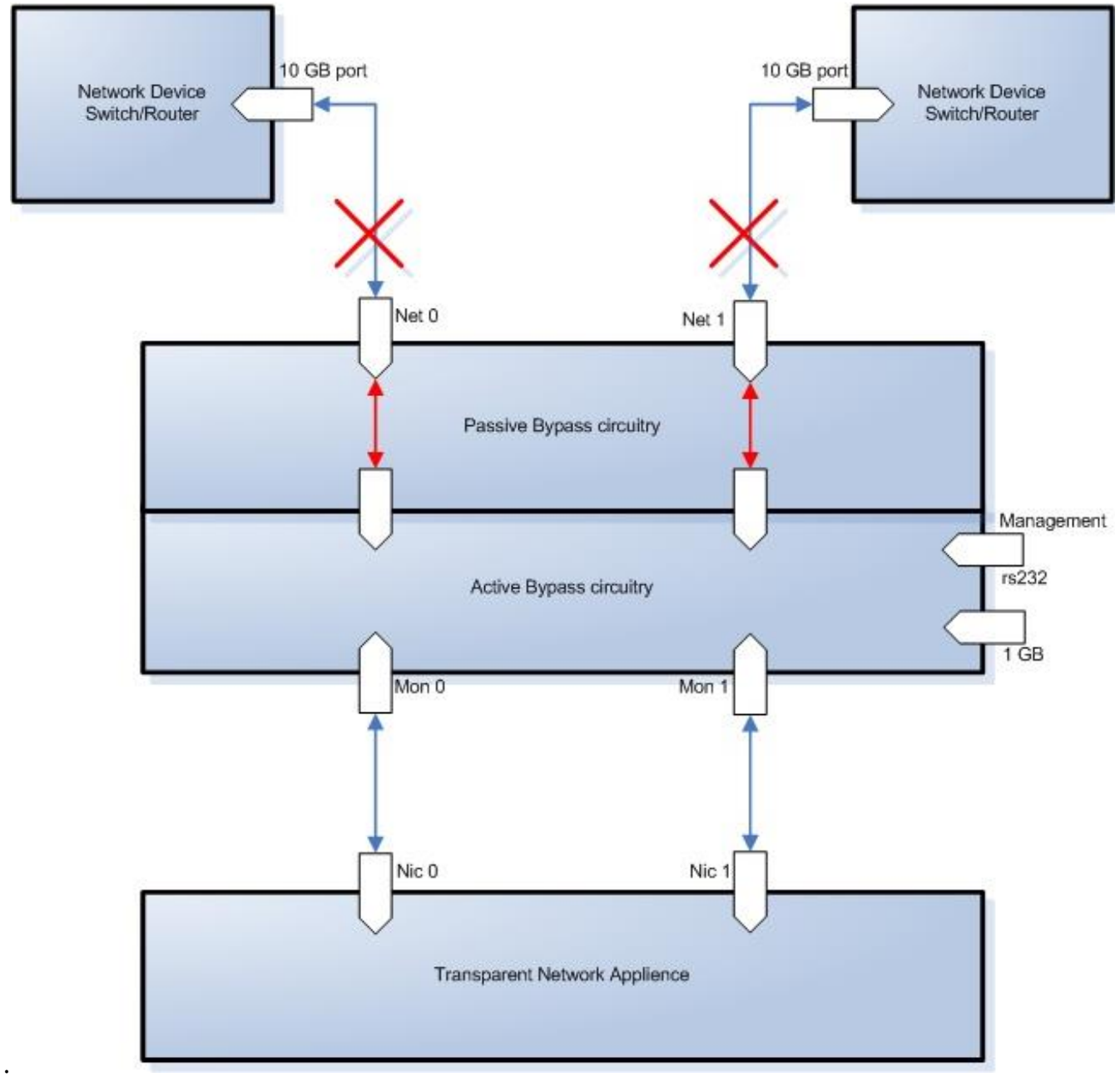


Figure: 8. EdgeSafe 40G Bypass Modular Network TAP TAPAI12 Mode.

2.12 Linkdrop mode

In **Linkdrop** mode the M40GBP disables the links on the network ports (NET0, NET1). The M40GBP simulates switch / router cable disconnection.



.

Figure: 9. EdgeSafe 40G Bypass Modular Network TAP Linkdrop Mode.

2.13 Two Port Link (2PL)

The M40GBP supports a two ports link feature. When enabled, if one of the network ports link fails it will drop the link on the other network port as well.

2.14 Restore from active expire state

The M40GBP supports manual and auto restoring from heartbeat expiration event.

2.15 Heartbeat active mode

When heartbeat active mode is ON and the M40GBP does not detect the heartbeat packet received from the monitor port the M40GBP will switch to **Active Bypass** or **TAP** or **Linkdrop** mode according to the predefined settings of the switch expire state.

When heartbeat active mode is set to OFF the EDGESAFE 40G stops sending the heartbeats and the M40GBP can be set manually via the management port to one of the following modes **Normal (Inline), Active Bypass, TAP** or **Linkdrop** mode.

By default Heartbeat active mode is not preserved after reset or after power off cycle. The Heartbeat active mode can be configured to be preserved after reset or power off cycle by enabling the **keep_hb_act_mode** parameter.

3 Front Panels

3.1 M40G1AC – M40G1AC with 3 M40GBP modules

Figure: 10. M40G1AC front panel.

3.2 M40G1AC – Management panel

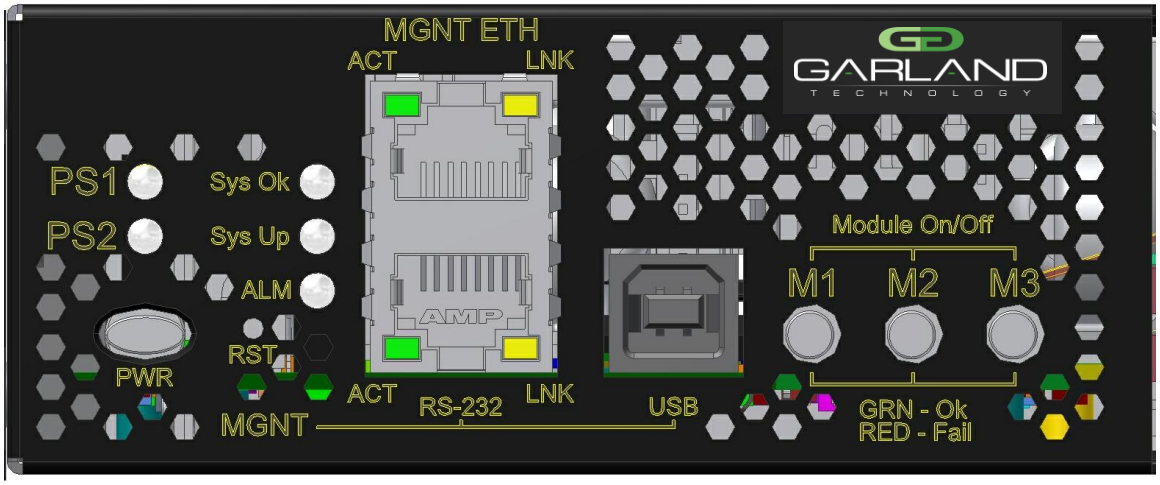


Figure: 11. M40G1AC front panel.

3.2.1 Bypass Switch 1U Host System LEDs & Switches Specifications

LEDs:	----------FRONT---------- Two Power LEDs: PS1, PS2 1. PS1: Green LED will light when power is on and off if there is a failer in power supply module or when extracting the power supply module from the system. 2. PS2: Green LED will light when power is on and off if there is a failer in power supply module or when extracting the power supply module from the system. System Status LEDs: 3 LEDs 1. Sys OK: System Normal Operation – Light Green. Who I'm: in rack identification – Blinking Green. 2. Sys UP: System Init during power up and during shutdown – Light Yellow. 3. ALM: System Alarm – Light Red.

	Module Power LEDs: 1. M1: module1 power on – Light Green.M2: module2 power on – Light Green. 2. M3: module3 power on – Light Green. ----------BACK---------- One bi-color LED indication that integrated on each power supply module: Power Switch On – Green color. Standby(AC/DC In,Only +5VSB output) - Blinking Green color. Power Fail – Red color. Internal Fan Fail – Blinking Red.
Switches	Push button to power the system (PWR). From ON to OFF – Press and hold this push button during 4 second will perform firmware shutdown press and hold this push button during 8 second will perform power shutdown. From OFF to ON – simple push will turn system on. Reset (RST): Small micro-switch stand behind hidden hole : Press and hold for more than 1 sec will perform restart to the system.
Connectors:	Management RJ-11 serial port RJ-45 Ethernet USB port

3.3 EdgeSafe 40G module

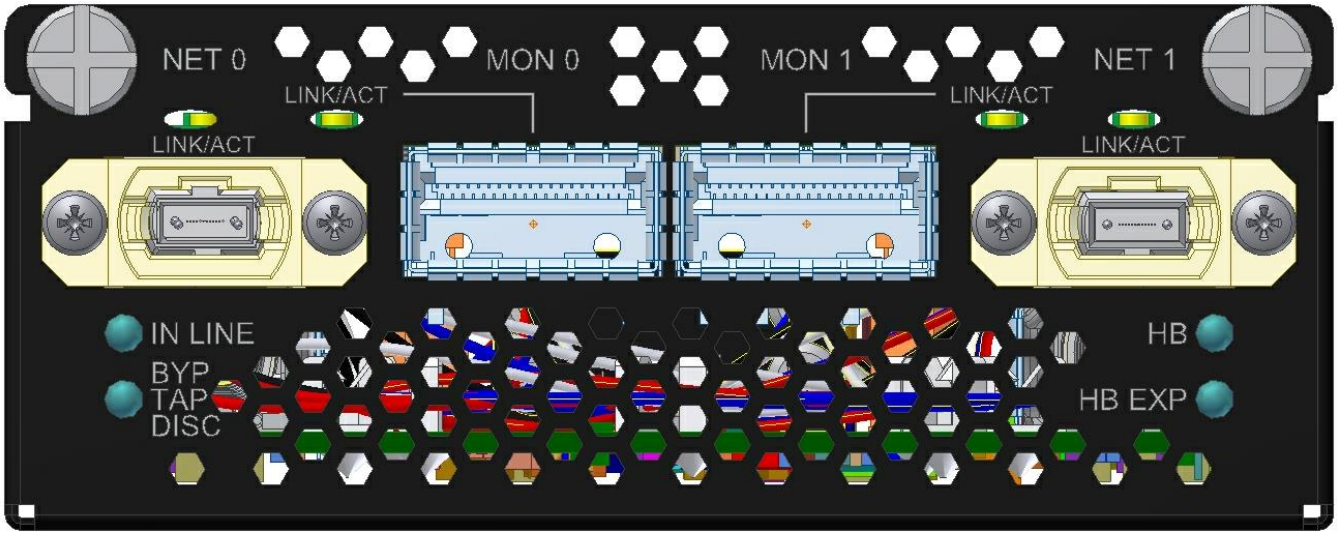


Figure: 12. EDGESAFE 40G module front panel

3.3.1 M40GMSBP/ M40GSSBP: LED and Connector Specifications

LEDs:	Green LED per port (Network / Monitor) Activity : LED will blink. Link : LED will turn on. Two LED: Inline Mode – Green LED. Non Inline Mode :Bypass, TAP, Disconnect – Yellow (Orange) LED. HB Status LED Blinking Green LED – HB is active. LED is off – HB not active.
Connectors:	Network: 2 MPO Monitor: 2 QSFP+

3.4 EDGESAFE 10G module

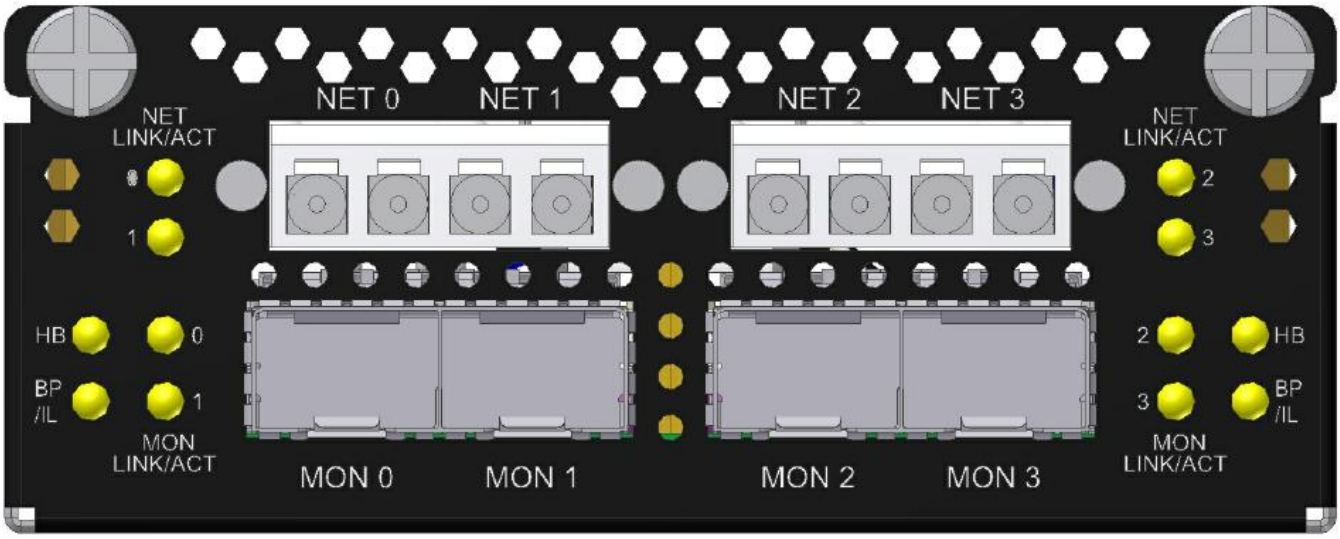


Figure: 13. EdgeSafe 10G module front panel

3.4.1 M10GMS2BP/ M10GSS2BP: LED and Connector Specifications

LEDs:	Green LED per port (Network / Monitor) Activity : LED will blink. Link : LED will turn on. Two LED: Inline Mode – Green LED. Non Inline Mode :Bypass, TAP, Disconnect – Yellow (Orange) LED. HB Status LED Blinking Green LED – HB is active. LED is off – HB not active.
Connectors:	Network: 4 LC Duplex Monitor: 4 SFP+

4 Rear Panels

4.1 M40G1AC - M40G1AC – rear panel

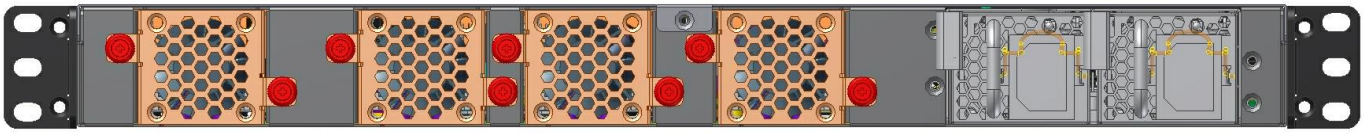


Figure: 14. M40G1AC rear panel.

5 Garland Technology Intelligent Bypass Switch Installation

5.1 Rack mount the M40GBP

The M40GBP is a rack mounting ready box.

5.2 Connecting Power to the 220V/110V M40GBP unit

5.2.1 Connect two power cables to the M40GBP. The PWR led's on the front panel of the M40GBP will illuminate when switching on the power switch power.

5.3 Connecting Power to the -48VDC M40GBP unit

5.3.1 Verify that the power is OFF on the DC power source

5.3.2 Verify that the power switch on the M40GBP unit is OFF

5.3.3 Connect the DC input wires to the DC input terminal on the M40GBP as follows:

5.3.3.1 Connect wire to ground terminal M40GBP (left)

5.3.3.2 Connect -48V return to "+" terminal M40GBP (center)

5.3.3.3 Connect -48V wire to "-" terminal (right) M40GBP

5.3.3.4 Turn on the DC power source The PWR led's on the front panel of the M40GBP will illuminate.

5.4 Connecting the RS232 DB9 management cable

1. Connect the RS232 DB9 cable supplied with the EDGESAFE 40G to the M40GBP Management RS232 port
2. Connect the other side of the RS232 cable to your Appliance RS232 port.
3. Use any terminal emulation software (Minicom, HyperTerminal …) to connect to the CLI interface to in order manage the M40GBP.
4. Set the following terminal communication parameters:
   - 115200 – default or 9600 if set by CLI command
   - 8 bits
   - no parity
   - 1 stop bit
   - no flow control
5. Power on the M40GBP
6. Login prompt will appear in terminal window.
7. The login name: customer, the default password: Garland Technology
8. After login you should change password, user and date. If you plan to use management Ethernet port, set IP address, net mask and gateway parameters.

5.5 Connecting the Ethernet management port

1. Connect Ethernet cable (CAT5) to the Management 1G Ethernet network port
2. Use any Telnet or SSH client to connect to the CLI interface in order to manage the M40GBP
3. The following are the default IP and login parameters
   - IP address: 10.10.10.200
   - Net mask: 255.255.255.0
   - Gateway: 10.10.10.200
   - Login name: admin
   - Password: gtadmin1
4. The following are default snmp user/community name and password (for snmp 3 and TACACS+)
   - user/community name: admin
   - password: gtadmin1

6 Command line interface (CLI)

Login to the command line interface (CLI) using the Rs232 management port or the Ethernet management port. The main menu will prompt after login.
The “help” command displays list of all CLI commands.
The “help full" command displays help for all CLI commands.
The Command parameters can include any letter or number and '_', '/', '.', ';', '.','-' characters. It cannot include space symbols.
Tip: In case of entering partial command the M40GBP will display all the commands which containing this part.

6.1 Main menu

```
M40GBP command line interface:
help        - this screen,
help full   - full help,
exit        - exit from CLI (logoff).
M40GBP$
```

6.2 Commands list

M40GBP command line interface:
get/set_hb_act_mode, get/set_bypass_mode, get/set_2pl,
get/set_hb_interval, get/set_hb_holdtime, get/set_keep_hb_act_mode,
get/set_hb_exp_state, get/set_en_act_hb_restore,
get/set_ip, get/set_netmask, get/set_gateway,
get/set_time, set_user, set_psw,
get/set_unit_name, whoami, get/set_flow_control,
get_ver, get_params, get_dev_state,
get_hw_ver, get_fw_ver, get_dev_tk_num,
get_appl_state, get_term_state,
get_link, get_log, get_current_user,
get/set_snmp_ver, get/set_snmp_srv_ip, get/set_snmp_user,
set_snmp_user_psw, apply_snmp, get/set_trap,
reset_log, set_default, update,
reboot, reset_err, get/set_web_https_state,
get_hb_pkt, load_hb_pkt, set_default_hb_pkt,
get/set_session_exp_time, get/set_mgmt_port_state,
get/set_hb_tx_dir, get/set_hb_fail,
get/set_remote_log_server_ip, get/set_remote_log_state,
get/set_ntp_state, get/set_ntp_server_ip, send_ntp_request,
get_timezone_list, get/set_timezone, get_daylight_state,
get_support_info, get/set_web_user, set_web_user_psw,
save_conf, restore_conf, get_list_conf,
remove_conf, get/set_tacacs_multi_users,
get/set_tacacs_state, set_tacacs_key, get/set_tacacs_server_ip,
get/set_telnet_state, get/clear_stat, get/set_rs232_speed,
set/del_mgmt_permit_ip, get/check_mgmt_permit_ip,
get/set_m2n, get/set_m2m,
get_power_state, power_off,
get/set_hb_dst_mac, get/set_hb_src_mac, set_default_hb_macs,
get/set_web, get/set_seg, get_dev_prop,
get_health, set/restore_cert,
get/set_radius_auth_port, get/set_radius_acct_port,
get_first_error, get_last_error, stop_all_sessions,
get/set_rx_tx_err_mode,
get/set_ssh_state, get/set_snmp_msg_port, get/set_snmp_trap_port,
add/del_ntp_server_ip, get/set_int_vlan, add/del_tacacs_server_ip,
get/set_tacacs_login_fallback, get/set_rs232_tacacs_login,
get/sel_snmp_entry, add/del_snmp_entry, add/del_snmp_srv_ip,
get/set_snmp_access, get/set_snmp_status,
add/del_lag_members, set_lag_min_work_members,
set_slct_bypass_mode, get/set_slct_bypass, add/del_slct_bypass
save_slct_bypass_conf, restore_slct_bypass_conf
remove_slct_bypass_conf, get_list_slct_bypass_conf
help - this screen,
help full - full help,
exit - exit from CLI (logoff).
Ctrl.m1s1.40g: M40GBP$

6.3 Get device properties (get_dev_prop)

The M40GBP can contain up to 3 different modules (40G and 10G). The command get_dev_prop return the info regarding the current installed modules.

Examples:

```
Ctrl: M40GBP$ get_dev_prop
********** module 1 ***************
current:                yes
segment count:            1
port count:               4
type:                   bypass module
speed:                  40 Gb/sec
   ****** segment 1 ******
current:                yes

command succeeded.
Ctrl: M40GBP$
```

On the above example only one 40G bypass module with one bypass segment is installed on the M40GBP chassis.

6.4 Get/Set segment (get/set_seg)

The command set_seg is used to determine which one of the current module/ segments will be controlled.
The command get_seg is used to check which module/segment is currently controlled

```
Ctrl: M40GBP$ set_seg 1 1
command succeeded.
Ctrl: M40GBP$ get_seg
Current module:segment      1:1.
command succeeded.
Ctrl: M40GBP$
```

6.5 Heartbeat active mode. (hb_act_mode)

When heartbeat active mode is ON the M40GBP sends heartbeat packets on its monitor ports. If the M40GBP does not detect the heartbeat packet received from the monitor ports the M40GBP will switch to **Active Bypass** or **TAP** or **Linkdrop** mode according to the predefined settings of the Heartbeat Expiration state.

When heartbeat active mode is set to OFF the M40GBP stops sending the heartbeats and the Active Bypass circuitry can be set manually via the management port to one of the following modes **Normal (Inline), Active Bypass, TAP** or **Linkdrop** mode.

Examples:

```
M40GBP$ get_hb_act_mode
hb active mode:          on.
command succeeded.
M40GBP$ set_hb_act_mode off
command succeeded.
M40GBP (manual)$ get_hb_act_mode
hb active mode:          off.
command succeeded.
M40GBP$
```

Notes:

- Set heartbeat active mode ON cause passive bypass switch to inline state.
- If “keep_hb_act_mode” is OFF the heartbeat active mode is always ON after power on or restart event.
- If “keep_hb_act_mode” is ON the heartbeat active mode preserves its state after power on or restart event.

6.6 Active Bypass mode

When heartbeat active mode is set to OFF the M40GBP stops sending the heartbeats packets, the Active Bypass circuitry can be controlled manually to be set to one of the following modes **Normal (Inline), Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop**.
In order to check the current mode of the Active bypass circuitry use the command "get_bypass_mode"
In order to change set the Active bypass circuitry use the command " set_bypass_mode" .

Examples:

```
M40GBP(manual)$ get_bypass_mode
active state:        inline.
command succeeded.
M40GBP (manual)$ set_bypass_mode bypass
command succeeded.
M40GBP (manual)$ get_bypass_mode
active state:        bypass.
command succeeded.
M40GBP(manual)$ set_bypass_mode tap
command succeeded.
M40GBP(manual)$ get_bypass_mode
active state:        tap.
command succeeded.
M40GBP(manual)$ set_bypass_mode linkdrop
command succeeded.
M40GBP(manual)$ get_bypass_mode
active state:        linkdrop.
command succeeded.
M40GBP(manual)$ set_bypass_mode tapi12
command succeeded.
M40GBP(manual)$ set_bypass_mode tapa
command succeeded.
M40GBP(manual)$ set_bypass_mode tapai1
command succeeded.
M40GBP(manual)$ set_bypass_mode tapai2
command succeeded.
M40GBP(manual)$ set_bypass_mode tapi12
command succeeded.
M40GBP$
```

6.7 Two port link (2PL)

The M40GBP supports two ports link. When enabled (on), if one of the network ports link fails it drops the link on the other network port. Two ports link is disabled (off) by default.

Example:

```
M40GBP$get_2pl
two port link:          off.
command succeeded.
M40GBP$set_2pl on
command succeeded.
M40GBP$get_2pl
two port link:          on.
command succeeded.
M40GBP$set_2pl off
command succeeded.
M40GBP$get_2pl
two port link:          off.
command succeeded.
M40GBP$
```

6.8 Monitor ports two port link (M2M)

M2M (monitor ports two port link) When enabled (on), if one of the monitor ports link fails it drops the link on the other monitor port. M2M k is disabled (off) by default.

```
M40GBP$get_m2m
m2m:                    off.
command succeeded.
M40GBP$ set_m2m on
command succeeded.
M40GBP$ get_m2m
m2m:                    on.
command succeeded.
M40GBP$
```

6.9 hb_interval (hb_interval)

The M40GBP generates a heartbeat packet to monitor PORT0 every “hb_interval” msec. (default - 5, min - 3, max - 10000). The Heartbeat interval should be at least 3 times less than heartbeat hold time. The " hb_interval " value is preserved after reset and power off events.

Example:

```
M40GBP$get_hb_interval
hb_interval:            5 ms.
command succeeded.
M40GBP$set_hb_interval 3
command succeeded.
M40GBP$get_hb_interval
hb_interval:            3 ms.
command succeeded.
M40GBP$
```

6.10 hb_holdtime (hb_holdtime)

The M40GBP monitors the received packets on monitor port1, if heartbeat packets do not arrive within "hb_holdtime" msec, the M40GBP will set the Active Bypass to **Bypass/TAP/Linkdrop** mode, depend on active switch expire state .
To secure reliable detection of Application failure, the " hb_holdtime " value should be at least 3 times the "hb_interval" parameter value. (default - 20, min - 10, max - 50000)
The " hb_holdtime " value is preserved after reset and power off events.
Example:

```
M40GBP$ get_hb_holdtime
hb_holdtime:            20 ms.
command succeeded.
M40GBP$ set_hb_holdtime 10
command succeeded.
M40GBP$ get_hb_holdtime
hb_holdtime:            10 ms.
command succeeded.
M40GBP$
```

6.11 Keep heartbeat active mode (keep_hb_act_mode)

When " keep_hb_act_mode" is ON the state of heartbeat active mode is preserved after reboot or after power on events. When the keep_hb_act_mode is OFF the state of heartbeat active mode is automatically set to ON after reboot or after power on.
Default value of the keep_hb_act_mode is OFF (disabled).
Example:

```
M40GBP$ get_keep_hb_act_mode
keep_hb_act_mode:       off.
command succeeded.
M40GBP$ set_keep_hb_act_mode on
command succeeded.
M40GBP$ set_keep_hb_act_mode off
command succeeded.
M40GBP$
```

6.12 Heartbeat expiration state (hb_exp_state)

When the M40GBP does not receive the heartbeat packet within the hb_holdtime time it will set the Active Bypass circuitry to the state that was set by the hb_exp_state (Bypass, Tap, Tapi12, Tapa, Tapai1, Tapai2, Tapai12 or linkdrop mode).

```
M40GBP$ get_hb_exp_state
hb expired state:        bypass.
command succeeded.
M40GBP$ set_hb_exp_state tap
command succeeded.
M40GBP$ get_hb_exp_state
hb expired state:        tap.
command succeeded.
M40GBP$ set_hb_exp_state linkdrop
command succeeded.
M40GBP$ get_hb_exp_state
hb expired state:        linkdrop.
command succeeded.
M40GBP$ set_hb_exp_state tapi12
command succeeded.
M40GBP$ set_hb_exp_state tapa
command succeeded.
M40GBP$ set_hb_exp_state tapai1
command succeeded.
M40GBP$ set_hb_exp_state tapai2
command succeeded.
M40GBP$ set_hb_exp_state tapai12
command succeeded.
M40GBP$
```

6.13 Restore from Heartbeat expiration event (en_act_hb_restore)

The M40GBP support automatic or manual heartbeat restore after a heartbeat expiration event.
The default value for the en_act_hb_restore is ON.
When the en_act_hb_restore is ON the M40GBP will restore to **Inline (Normal)** state when the heartbeat packets will be received from the Monitor port.
When the en_act_hb_restore is OFF the M40GBP preserves its state and no heartbeat packets are generated.
The following actions should be taken to restore the normal operation:

- Restore external environment to normal work.
- Send command “set_bypass_mode inline”
- Send command “set_hb_act_mode on”

```
M40GBP$ get_en_act_hb_restore
restore active state:      on.
command succeeded.
M40GBP$ set_en_act_hb_restore off
command succeeded.
M40GBP$ get_en_act_hb_restore
restore active state:      off.
command succeeded.
M40GBP$
```

6.14 Change Bypass state on RX/TX error detection (rx_tx_err_mode)

The M40GBP can place itself into Bypass or Linkdrop in case it detects RX/TX errors on the Monitor ports or on the Network ports.

Example:

```
M40GBP$ get_rx_tx_err_mode
rx and tx error processing mode:
trap:                enable
timeout:              5 sec
mon:                 bypass
net:                 none
threshold:            10 err/sec
command succeeded.

M40GBP$ set_rx_tx_err_mode trap timeout mon net
threshold
                    - set rx and tx error processing mode
                      trap: on|off - enable/disable trap
                      timeout: >0 - minimal time between traps
                      mon: none/bypass/linkdrop -   changing
                      Bypass mode when number of errors per
                      second on MONx ports exceeds threshold
                      net: none/linkdrop -
                      changing Bypass mode when number of
                      errors per second on NETx ports exceeds
                      threshold
                      threshold : >0 (default - 10)

M40GBP$ set_rx_tx_err_mode on 4 linkdrop linkdrop 20
```

6.15 LAG configuration

The M40GBP supports Link Aggregate Groups (LAG)
The LAG feature supported by the following capabilies:

- Up to 4 x 10G bypass segments
- Up to 2 x 40G bypass segments
- heartbeat is sent on all monitor ports (different HB packet on each bypass segment). The HB packet can return on a different segment than the one that it was sent.
- Heartbeat failutre (not due to link failure) will cause the LAG segments to switch to Bypass mode.
- A link failure by one of the LAG segments will cause all the LAG segments to switch to Bypass mode only of the number of avliable links is the LAG falls below the threshold (set_lag_min_work_members).
- All segments in the same LAG must be from the same type of module (10G or 40G, SR or LR) the LAG will use the HB and the bypass mode settings of the first member (minimum hb_ interval – 70ms, hb_holdtime – 210 ms).

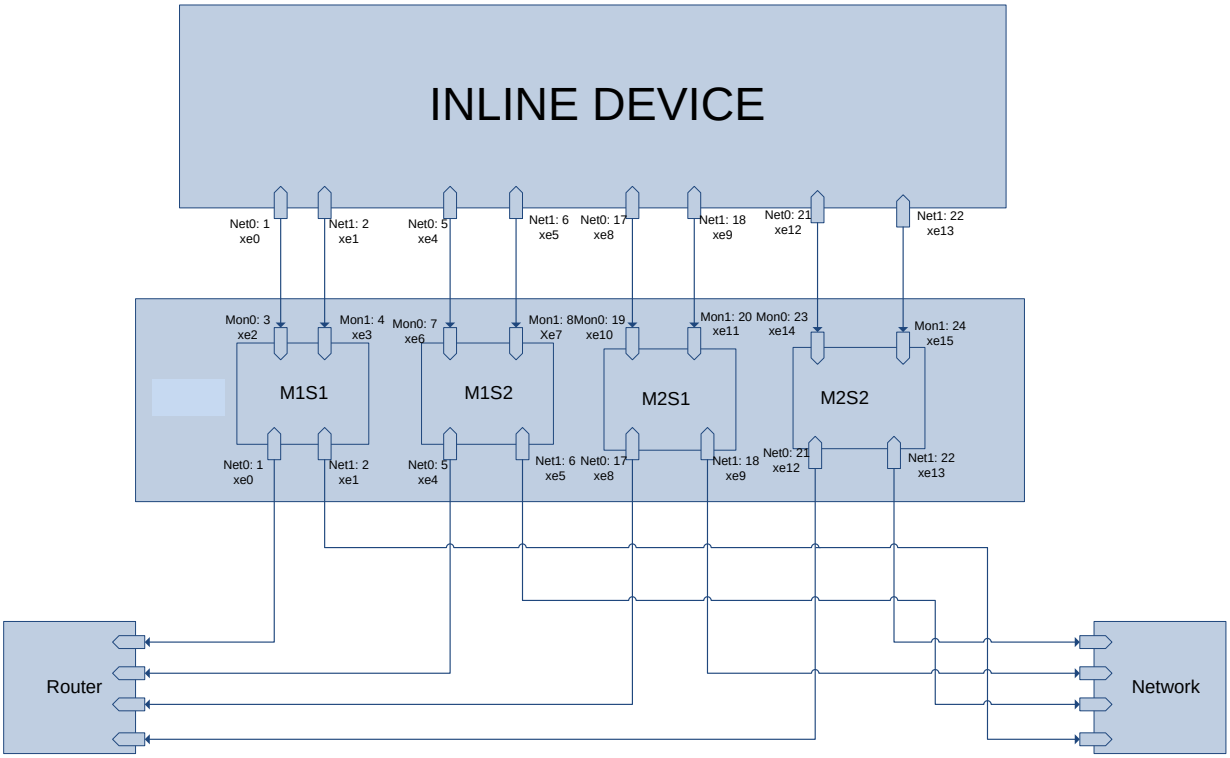


Figure: 15. LAG topology with 4 segnemts

Configuring the LAGs

6.15.1 Get lag (get_lag)

The get_lag commad dispay the current configured lag, lag status, lag members and link state of each port

```
Ctrl.lag1m1s1.10g: M40GBP$ get_lag
============ lag1 ==========
lag hb active:            on
lag state:              inline
application state:        unknown
minimum working members:   1
members:                  m1s1, m1s2, m3s2
net0:                   m1s1:down, m1s2:down, m3s2:down
net1:                   m1s1:down, m1s2:down, m3s2:down
mon0:                    m1s1:down, m1s2:up,   m3s2:down
mon1:                    m1s1:down, m1s2:up,   m3s2:down
m1s1:                    failed
m1s2:                    ok
m3s2:                    failed
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$
```

6.15.1 Add lag Get lag (add_lag_member)

The command add_lag_members, creates new LAG and add lag members to existing lag

```
add_lag_members lag_name <module:segment> .. <module:segment>
                    - add LAG members
                      lag_name - LAG name (1 - 20 characters)
                      module  - module number ( 1 - 3)
                      segment - segment number ( 1 - 2).
Ctrl.lag1m1s1.10g: M40GBP$ add_lag_members LAG2 2:1 2:2
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$get_lag
============ LAG2 ==========
lag hb active:            on
lag state:              inline
application state:        unknown
minimum working members:   1
members:                  m2s1, m2s2
net0:                   m2s1:up,   m2s2:down
net1:                   m2s1:down, m2s2:down
mon0:                    m2s1:up,   m2s2:down
mon1:                    m2s1:up,   m2s2:down
m2s1:                    ok
m2s2:                    failed
command succeeded.
```

6.15.2 Set minimum lag working members (set_lag_min_work_members)

A link failure by one of the LAG segments will cause all the LAG segments to switch to Bypass mode only of the number of avliable links is the LAG falls below the threshold
The command set_lag_min_work_members defins this threshold

```
set_lag_min_work_members lag_name count
                    - set the minimal number of LAG working segments
                      before LAG switch to expired state.
Ctrl.lag1m1s1.10g: M40GBP$ set_lag_min_work_members LAG2 2
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$ Ctrl.lag1m1s1.10g: M40GBP$ get_lag
============ LAG2 ==========
lag hb active:          on
lag state:             tap
application state:      unknown
minimum working members:   2
members:                m2s1, m2s2
net0:                  m2s1:up,   m2s2:down
net1:                  m2s1:down, m2s2:down
mon0:                   m2s1:up,   m2s2:down
mon1:                   m2s1:up,   m2s2:down
m2s1:                   ok
m2s2:                   failed
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$
```

6.15.3 Delete lag members (del_lag_members)

```
del_lag_members lag_name <module:segment> .. <module:segment>
                - delete LAG members
                  lag_name - LAG name (1 - 20 characters)
                  module  - module number ( 1 - 3)
                  segment - segment number ( 1 - 2
Ctrl.lag1m1s1.10g: M40GBP$ get_lag
============ lag1 ==========
lag hb active:            on
lag state:              inline
application state:        unknown
minimum working members:   1
members:                  m1s1, m1s2, m3s2
net0:                   m1s1:down, m1s2:down, m3s2:down
net1:                   m1s1:down, m1s2:down, m3s2:down
mon0:                    m1s1:down, m1s2:up,   m3s2:down
mon1:                    m1s1:down, m1s2:up,   m3s2:down
m1s1:                   failed
m1s2:                   ok
m3s2:                   failed
Ctrl.lag1m1s1.10g: M40GBP$ del_lag_members lag1 3:2
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$ get_lag
============ lag1 ==========
lag hb active:            on
lag state:              inline
application state:        unknown
minimum working members:   1
members:                  m1s1, m1s2
net0:                   m1s1:down, m1s2:down
net1:                   m1s1:down, m1s2:down
mon0:                    m1s1:down, m1s2:up
mon1:                    m1s1:down, m1s2:up
m1s1:                   failed
m1s2:                   ok
command succeeded.
Ctrl.lag1m1s1.10g: M40GBP$
```

6.15.4 Delete lag (del_lag)

The command del_lag delete existing lag

```
Ctrl.lag1m1s1.10g: M40GBP$ del_lag lag1
command succeeded
```

6.16 Selective bypass filters

The Selective Bypass filter provides the ability to filter and Bypass packet between Net0/Net1 based on IP/MPLS tag/VLAN id (It is possible to set the filter to specific value or the range by entering mask value). When white list is enabled, all filtered traffic goes from one network port to other and vice versa. All other traffic goes according to bypass mode.
When black redirect list enabled, all traffic except filtered goes from one network port to other and vice versa. Filtered traffic goes according to bypass mode.
When black drop list is enabled, all traffic except filtered dropped.Filtered traffic goes according to bypass mode.
xxx_up - direction from NET0 to NET1
xxx_down - direction from NET1 to NET0

6.16.1 White list – redirect

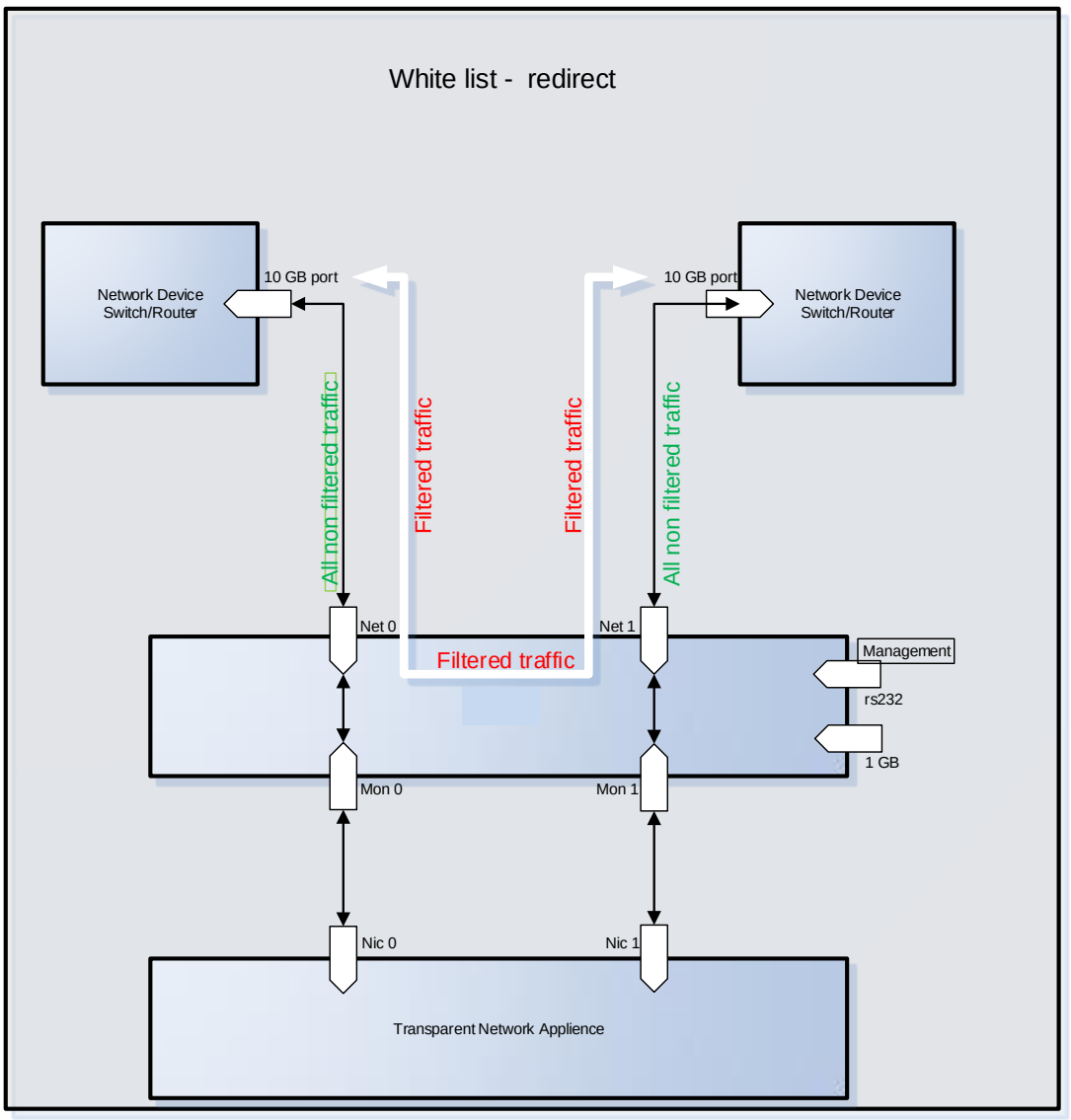


Figure: 16. White list – redirect

When white list is enabled, all filtered traffic goes from one network port to other and vice versa. All other traffic goes according to bypass mode.

6.16.2 Black list – redirect

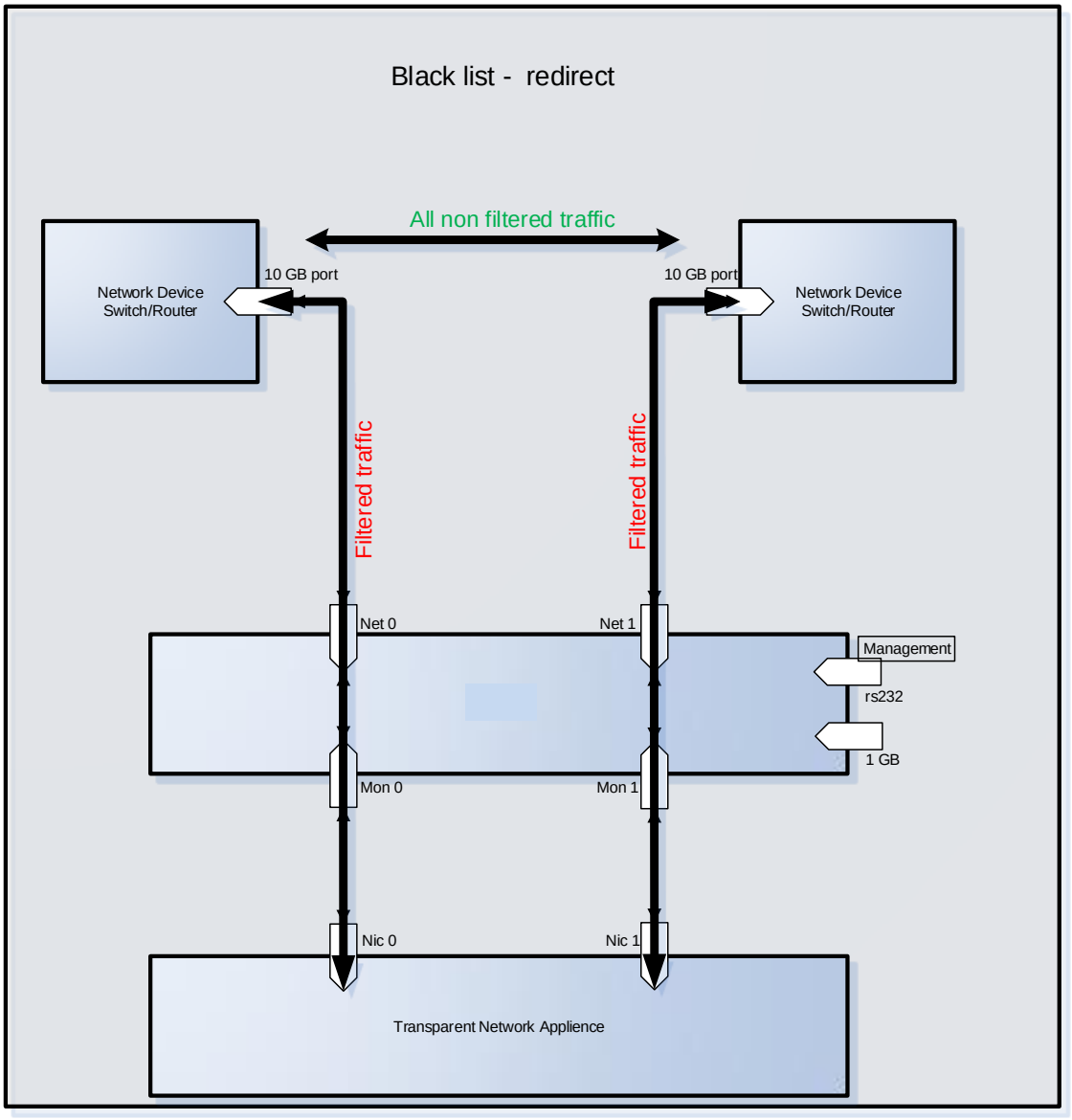


Figure: 17. Black list – redirect

When black redirect list enabled, all traffic except filtered goes from one network port to other and vice versa. Filtered traffic goes according to bypass mode.

6.16.3 Black list – drop

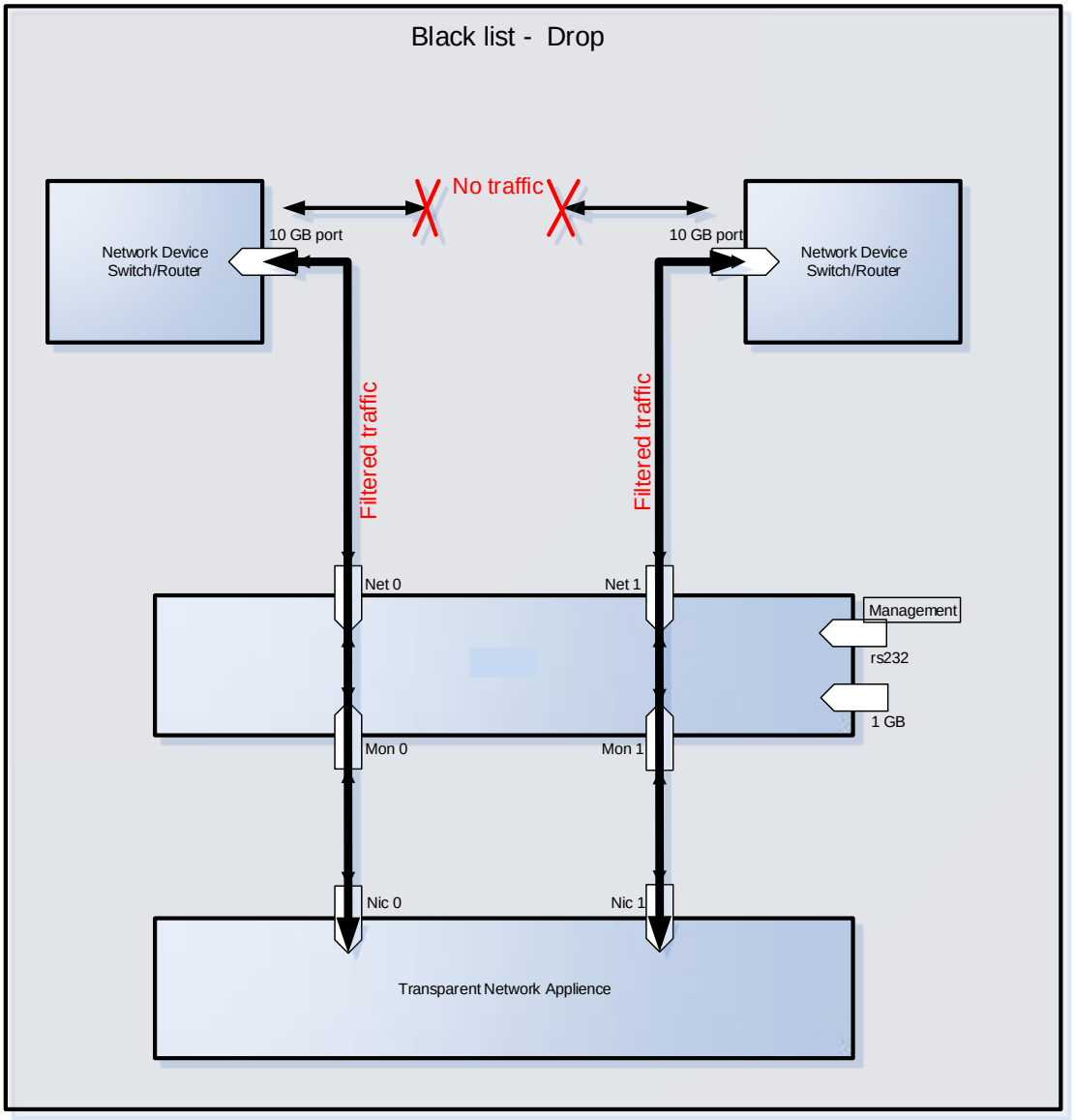


Figure: 18. Black list – drop

When black drop list is enabled, all traffic except filtered dropped.Filtered traffic goes according to bypass mode.

6.16.4 Defune the selective bypass mode (set_slct_bypass_mode)

```
set_slct_bypass_mode
            white_list_up|white_list_down
           |black_redir_list_up|black_redir_list_down
           |black_drop_list_up|black_drop_list_down
                - When white list is enabled, all filtered
                  traffic goes from one network port to other
                  and vice versa.
                  Other traffic goes according to bypass mode.
                  When black redirect list enabled, all traffic
                  except filtered goes from one network port
                  to other and vice versa.
                  Filtered traffic goes according to bypass mode.
                  When black drop list is enabled, all traffic
                  except filtered dropped.
                  Filtered traffic goes according to bypass mode.
                  xxx_up   - direction from NET0 to NET1
                  xxx_down - direction from NET1 to NET0
```

6.16.5 Add selective bypass rule (add_slct_bypass)

```
add_slct_bypass
add_slct_bypass [rule_id] mpls_up|mpls_down redir|drop
   mpls_lable mpls_lable_mask [group]
add_slct_bypass [rule_id] vlan_up|vlan_down redir|drop
   vlan_id vlan_id_mask [group]
add_slct_bypass [rule_id] ip_up|ip_down redir|drop
   src_ip/src_ip_mask|n/a dst_ip/dst_ip_mask|n/a
   src_port|n/a src_port_mask|n/a dst_port|n/a dst_port_mask|n/a [group]
add_slct_bypass [rule_id] mac_up|mac_down redir|drop
   src_mac|n/a src_mac_mask|n/a dst_mac|n/a dst_mac_mask|n/a [group]
add_slct_bypass [rule_id] proto_up|proto_down redir|drop
   protocol protocol_mask [group]
                - add selective bypass rule.
                  when using n/a - parameter not applicable.
                  rule_id - (optional), when it
                  does not set device will set it automatically.
                  rule_id - 1 (highest) - 244 (lowest) priority
                  group (optional) 1 - 16, default - 1
                  xxx_up   - direction from NET0 to NET1
                  xxx_down - direction from NET1 to NET0
                  to get additional help enter:
                  add_slct_bypass mpls|vlan|ip|mac|proto
```

6.16.6 Delete skective bypass filter (del_slct_bypass)

del_slct_bypass
del_slct_bypass all
del_slct_bypass rule_id
del_slct_bypass mpls_up|mpls_down redir|drop
mpls_lable mpls_lable_mask [group]
del_slct_bypass vlan_up|vlan_down redir|drop vlan_id vlan_id_mask [group]
del_slct_bypass ip_up|ip_down redir|drop
src_ip/src_ip_mask|n/a dst_ip/dst_ip_mask|n/a
src_port|n/a src_port_mask|n/a dst_port|n/a dst_port_mask|n/a [group]
del_slct_bypass mac_up|mac_down redir|drop
src_mac|n/a src_mac_mask|n/a dst_mac|n/a dst_mac_mask|n/a [group]
del_slct_bypass proto_up|proto_down redir|drop
protocol protocol_mask [group]
- delete selective bypass rule.
when "all" or rule id does not set
parameters should be the same as for
correspondent add_slct_bypass command.

6.16.7 Set selective bypass on/off (set_slct_bypass on/off)

set_slct_bypass on|off [group|all]
- enable/disable selective bypass rules
group (1 - 16).
when group does not set processed group 1.
"all" used for processing all groups.

6.16.8 Get selective bypass on/off (set_slct_bypass on/off)

get_slct_bypass [on|off] [group]

6.16.9 Get selective bypass rule list (get_slct_bypass rule_list)

get_slct_bypass rule_list|group_list

6.16.10 Get selective bypass filter (get_slct_bypass filter)

get_slct_bypass filter [on|off] [group]

6.16.11 get_slct_bypass x_range (get_slct_bypass x_range first last [on|off] [group])

get_slct_bypass x_range first last [on|off] [group]
- get selective bypass rules.
without parameters displays all rules for segment.
rule_list displays used rules list.
group_list displays used groups.
filter (mpls_up|mpls_down|vlan_up|vlan_down|ip_up|
ip_down|mac_up|mac_down|proto_up|proto_down|all)
displays rules for selected filters.
x_range (where "x" rule_id|mpls_up|mpls_down|
vlan_up|vlan_down|ip_up_src_ip|ip_down_src_ip|
ip_up_dst_ip|ip_down_dst_ip|ip_up_src_port|
ip_down_src_port|ip_up_dst_port|ip_down_dst_port|
mac_up_src|mac_down_src|mac_up_dst|
mac_down_dst|proto_up|proto_down)
displays rules range.
group (optional) filter for certain rules group.
on|off (optional) displays enabled/disabled rules.

6.17 Ethernet management port IP address

The Ethernet management port default IP address: 10.10.10.20000
The IP address can be set to different IP address using the command set_ip .

Example:

```
M40GBP$ get_ip
device ip address:      192.168.0.100
command succeeded.
M40GBP$ set_ip 192.168.0.101
New system IP will take effect after reboot.
command succeeded.
M40GBP$ get_ip
device ip address:      192.168.0.101
command succeeded.
M40GBP$
```

Notes:

- New IP address will take effect only after performing device reboot.
- Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new IP address.

6.18 Ethernet management port net mask address

The Ethernet management port default net mask address is 255.255.255.0.
The net mask address can be set to different IP address using the command: set_netmask

Example:

```
M40GBP$ get_netmask
netmask:            255.255.255.0
command succeeded.
M40GBP$ set_netmask 254.255.255.0
New network mask will take effect after reboot.
command succeeded.
M40GBP$ get_netmask
netmask:            254.255.255.0
command succeeded.
M40GBP$
```

Notes:

- New net mask address will take effect only after performing device reboot.
- Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new net mask address.

6.19 Ethernet management port gateway IP address

The Ethernet management port default gateway IP address is 10.10.10.200.
The net default gateway IP address can be set to different IP address using the command: set_gateway

Example:

```
M40GBP$ get_gateway
default gateway ip address: 10.10.10.200
command succeeded.
M40GBP$ set_gateway 10.10.10.200
New default gateway will take effect after reboot.
command succeeded.
M40GBP$ get_gateway
default gateway ip address: 10.10.10.200
command succeeded.
M40GBP$
```

Notes:

- New gateway address will take effect only after performing device reboot.
- Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new gateway address.

6.20 Time

To change the M40GBP date and time use the command “set_time mm DD HH MM YYYY”
Where:

- mm - month,
- DD - day,
- HH - hour (24 hours format),
- MM - minute,
- YYYY -year

Example:

```
M40GBP$get_time
Time:                Thu Feb  5 13:10:00 2009
command succeeded.
M40GBP$set_time 2 5 13 10 2010
Thu Feb  5 13:10:34 2009  0.000000 seconds
Fri Feb  5 13:10:00 2010  0.000000 seconds
command succeeded.
M40GBP$get_time
Time:                Fri Feb  5 13:10:02 2010
command succeeded.
M40GBP$
```

6.21 System user (set_user)

To change the M40GBP user name (factory default user name is: "customer") use the command "set_user" . The new user name will take effect after the next login.
Example:

```
M40GBP$ set_user Tomcat
System user name changed, this operation requires logoff.
Continue? (Y/n).
n
command succeeded.
M40GBP$
```

6.22 System password (set_psw)

To change the M40GBP system password (factory default is "gtadmin1") Use the command "set_psw" . The new password will take effect after the next login.

Example:

```
M40GBP$ set_psw
Changing password for customer
Old password:
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and
numbers.
Enter new password:
Re-enter new password:
Password changed.
command succeeded.
M40GBP$
```

6.23 Unit name.

The M40GBP supports individual names for each M40GBP unit on the network. The User can set the M40GBP unit name (default unit name: M40GBP) using the command: set_unit_name. Unit name can be up to 25 symbols
Example:

```
M40GBP$ get_unit_name
unit name: M40GBP
command succeeded.
M40GBP$ set_unit_name first
command succeeded.
M40GBP$
```

6.24 Who am I (whoami)

Blink the **S.OK** LED on currently controlled M40GBP unit in order to identify the relevant unit.
Example:

```
M40GBP$ whoami on
command succeeded.
M40GBP$ whoami off
command succeeded.
M40GBP$
```

6.25 Display M40GBP versions (get_ver)

Display the M40GBP hardware, firmware and software versions.
Example:

```
Ctrl: M40GBP$ get_ver
hardware version:  22.1.0.40 (P2041 rev. 1.1)
firmware version:  0.0.9.7
swdaemon version:  1.1.64.30, Mon Jan 20 13:59:37 2014
swctl version:     1.1.64.30, Mon Jan 20 13:59:43 2014
u-boot version:    U-Boot 2011.12-sl:00.01, Dec 25 2013, 11:46:56
kernel version:    3.0.34-sl:00.01-rt55, #88 SMP Thu Apr 11 09:42:32 IDT 2013
command succeeded.
Ctrl: M40GBP$
```

6.26 Display M40GBP parameters (get_params)

Show the current M40GBP parameters values.
Example:

```
Ctrl: M40GBP$ get_params
Time:                   Tue Jan 21 11:38:05 2014
hb expired state:       bypass.
hb active mode:         on.
keep_hb_act_mode:       off.
restore active state:   on.
restore passive state:  on.
two port link:          off.
hb_interval:            5 ms.
hb_holdtime:            20 ms.
hb_dir:                 MON0.
hb_fail:                unidirectional.
device ip address:      192.168.0.100
netmask:                255.255.255.0
gateway ip address:     192.168.0.1
https:                  on.
web expire time:        900 sec.
snmp version:           1
snmp server ip address: 192.168.0.6
tftp server ip address: 192.168.0.6
tftp root path:         "".
command succeeded.
Ctrl: M40GBP$
```

6.27 Display M40GBP state (get_dev_state)

Show the current M40GBP Bypass and operational mode state.
Note: This command resets the Alarm LED. Example:

```
Ctrl: M40GBP$ get_dev_state 1
ERROR: wrong parameter number!
get_dev_state              - get current state.
Ctrl: M40GBP$ get_dev_state
Time:         Tue Jan 21 09:54:24 2014
active state:          inline.
passive state:         inline.
eth management port:    on.
application:           alive.
rs232 terminal:        connected.
network port 0:        link down.
network port 1:        link down.
monitor port 0:        link up.
monitor port 1:        link up.
----------------------------------------
Sensor name     current (C)     peak(C)
SD10 (FN11)     32              33
SD11 (FN12)     36              36
SD12 (FN13)     30              31
SD13 (FN10)     34              34
SI10 (FN11)     34              35
SD20            33              34
SI20            27              27
CP01            36              -
CP02            41              -
CP03            35              -
CP04            35              -
CP07            47              -
MO11            37              -
BCM1            43              44
BCM2            40              41
BCM3            41              42
BCM4            40              42
BCM5            45              46
BCM6            41              42
BCM7            41              42
BCM8            44              45
----------------------------------------
```

```
-----------------------------------------
Fan name        Fault   Warn    Status  Speed (RPM)     Run time
(hours)
FN11            OK      OK      UNKNOWN 9213            0
FN12            OK      OK      UNKNOWN 14591           0
FN13            OK      OK      GREEN   15756           0
FN14            OK      OK      UNKNOWN 14478           0
command succeeded.
Ctrl: M40GBP$
```

6.28 Display device hardware version (get_hw_ver)

Example:

```
M40GBP$ get_hw_ver
hardware version: 22.01.00.40
command succeeded.
M40GBP$
```

6.29 Display device firmware version (get_fw_ver)

Device firmware version is the generalize version that allow to determine versions of all software components.
Example:

```
M40GBP$ get_fw_ver
firmware version: 0.0.9.7
command succeeded.
M40GBP$
```

6.30 Display device Tracking number (get_dev_tk_num)

Example:

```
M40GBP$ get_dev_tk_num
product tracking number: C083101000007
command succeeded.
M40GBP$
```

6.31 Display device health state (get_health)

Fan and temperature status displayed
Example:
For the M40GBP10:

```
Ctrl: M40GBP$ get_health
-----------------------------------------
Sensor name     current (C)     peak(C)
SD10 (FN11)     32              33
SD11 (FN12)     36              36
SD12 (FN13)     30              31
SD13 (FN10)     34              34
SI10 (FN11)     34              34
SD20            33              33
SI20            26              27
CP01            41              -
CP02            41              -
CP03            29              -
CP04            35              -
CP07            47              -
MO11            28              -
BCM1            43              43
BCM2            40              40
BCM3            40              42
BCM4            40              41
BCM5            44              46
BCM6            40              42
BCM7            40              42
BCM8            43              44
-----------------------------------------
Fan name        Fault   Warn    Status  Speed (RPM)
Run time (hours)
FN11            OK      OK      UNKNOWN 9191
0
FN12            OK      OK      GREEN   15182           1
FN13            OK      OK      GREEN   15756           1
FN14            OK      OK      GREEN   15000           1
command succeeded.
Ctrl: M40GBP$
```

6.32 Display application state (get_appl_state)

The command get_appl_state display the current status of the application installed on the monitor appliance that is connected to the M40GBP monitor ports:

- Alive – The link on the monitor ports are ON and the M40GBP receives the heartbeat packets
- fail, - The link on the monitor ports are ON and the M40GBP does not receive the heartbeat packets
- unknown - The link on the monitor ports are OFF

Example:

```
M40GBP$ get_appl_state
application:          alive.
command succeeded.
M40GBP$
```

6.33 Display rs232 terminal connection state (get_term_state)

Example:

```
M40GBP$get_term_state
rs232 terminal:       connected.
command succeeded.
M40GBP$
```

6.34 Display/change rs232 terminal port speed (get/set_rs232_speed)

Default rs232 port speed set to 115200. It can be changed to 9600. Changing rs232 port speed requires rebooting the device.

```
M40GBP$ get_rs232_speed
rs232 speed:      115200
command succeeded.
M40GBP$ set_rs232_speed 9600
Completing the rs232 speed settings requires a reboot of the device.
Continue? (Y/n)
```

6.35 Display Ethernet port state (get_link)

The command “get_link XXX” display the port link state.
Where XXX:

- MON0 – monitor port 0
- MON1 – monitor port 1
- NET0 – network port 0
- NET1 – network port 1

Example:

```
M40GBP$ get_link MON0
monitor port 0:       link up.
command succeeded.
M40GBP$
```

6.36 Display device log file (get_log)

The command get_log display the M40GBP log file
get_log [user ip log_name][last_lines_cnt]
display the full log file or its last lines
or copies full log file to remote server.
remote server user name.
remote server IP.
remote server log file destination name.
parameters length: 4 - 20 characters.

Example:

```
M40GBP$ get_log
swdaemon (version 1.0.0.4) started: Thu Feb  5 13:02:40 2013
Mon port 0: link up     Thu Feb  5 13:02:48 2009
Mon port 1: link up     Thu Feb  5 13:02:48 2009
Net port 0: link up     Thu Feb  5 13:02:48 2009
Net port 1: link up     Thu Feb  5 13:02:48 2009
Appliance recovered:  Thu Feb  5 13:02:49 2009
command succeeded.
M40GBP$
```

6.37 Reset log file (reset_log)

The default log file is stored in the internal FLASH memory. The log is saved also after reboot or power off. The log file is saved in 2 x 4096KB cyclic blocks. When two blocks are full, the older block is cleared and the new information is written in the location of the old block.

Example:

```
M40GBP$ reset_log
command succeeded.
M40GBP$
```

6.38 Reset error condition (reset_err)

The Command “reset_err” is used to reset error condition in the M40GBP.

```
M40GBP$ reset_err
command succeeded.
M40GBP$
```

6.39 Get first error (get_first_error)

The Command “get_first_error” is used to get the first error on the log file.

6.40 Get last error (get_last_error)

The Command “get_last_error” is used to get the last error on the log file

6.41 Set default parameters (set_default)

Restore the factory default settings for all parameters including system user name and password. Command does not restore rs232 port speed.
Example:

```
M40GBP$ set_default
command succeeded.
M40GBP$
```

The factory default settings are:

- IP address: 10.10.10.200
- Net mask: 255.255.255.0
- Gateway: 10.10.10.200
- hb_interval : 5 ms
- hb_holdtime: 20 ms
- enable snmp traps: disabled all snmp trap -
- snmp server ip: 192.168.0.6
- snmp version: 1
- Session expired time: 900 sec
- WEB https: enabled
- TFTP server ip: 192.168.0.6
- SNMP user: admin
- SNMP password: gtadmin1
- Unit name: M40GBP
- TFTP root: tftpboot
- Two port link: disabled
- Expire state: Bypass
- Keep heartbeat active mode: disabled
- Management port: enabled
- Heartbeat active mode: ON
- System user: admin
- System user password: gtadmin1
- Heartbeat packet transmit direction: mon0
- Heartbeat packet fail criteria: unidir
- Ethernet Management port parameters: auto
- Remote log state: disabled
- NTP: off
- Telnet: off
- Remote log server IP: 192.168.0.6
- NTP server IP: 192.168.0.6
- Timezone: UTC
- Tacacs state: off
- Tacacs server IP: 192.168.0.6
- WEB user name: admin
- WEB user password: gtadmin1
- Tacacs secret key: default_tac_key

6.42 Reboot

The reboot command forces a reboot of the M40GBP.

Example:

```
M40GBP reboot
rebooting...
```

6.43 Get/Set WEB HTTPS state (web_https_state)

The M40GBP Web interface supports HTTPS and HTTP protocol
While the HTTPS is set to OFF (default ON) the Web interface will use HTTP protocol.
.
Example:

```
M40GBP$ get_web_https_state
https:                  off.
command succeeded.
M40GBP$ set_web_https_state on
command succeeded.
M40GBP$ get_web_https_state
https:                  on.
command succeeded.
M40GBP$
```

6.44 Replacing the default certificate for the web UI (set_cert)

For HTTPS connections with the web UI, the M40GBP has its certificate. By default, the M40GBP "Factory" certificate can be used to encrypt the connection.
To replace the certificate with one that is signed by your own CA use the command set_cert

set_cert [tftp_server_ip tftp_server_root]
- set new ssl certificate for https connection
tftp_server_ip - tftp server ip address
tftp_server_root - tftp server root directory

```
M40GBP$ set_cert 192.168.0.06 tftpboot
command succeeded.
```

6.44.1 Restore the factory default certificate for the web UI (set_cert)

To restore the factory default certificate use the command restore_cert

```
M40GBP$ restore_cert command succeeded.
```

6.45 Get/Set management session timeout (session_exp_time)

The session_exp_time command sets the time that the session can be passive (does not send request to the M40GBP) before the session will be terminated by the M40GBP (default 900 sec).
In case that the WEB session was terminated the Login screen will appear on the WEB browser.
Example:

```
M40GBP$ get_session_expired_time
session timeout:          900 sec.
command succeeded.
M40GBP$ set_session_expired_time 1000
command succeeded.
M40GBP$ get_session_expired_time
session timeout:          1000 sec.
command succeeded.
M40GBP$
```

6.46 Get/Set Ethernet management port status (mgmt_port_state)

The M40GBP Ethernet management port can be disabled /enabled (factory default = enabled)
When enabled all management operation can be performed remotely via this port. When disabled – WEB interface, SNMP, Telnet, SSH management protocols are disabled.
Example:

```
M40GBP$ get_mgmt_port_state
eth management port:    on.
command succeeded.
M40GBP$ set_mgmt_port_state off
command succeeded.
M40GBP$ get_mgmt_port_state
eth management port:    off.
command succeeded.
M40GBP$
```

6.47 Get/Set segment link speed (get/set_seg_speed)

The 10G Bypass modules (M10GMS2BP & M10GSS2BP) support dual rate 10G/1G link speed.
The 10G bypass segments can be configured to force the link speed to 1G , 10G or auto.
When it is set to Auto, the 10 Bypass segments autodetect the link speed during the bootup of the M40GBP unit. In case that no cable is connected to the Monitor or to the Network ports, the segment speed will be set to the last known speed.

Example:

```
Ctrl.m1s2.10g: M40GBP$ set_seg_speed
set_seg_speed [all] auto|10g|1g
                    - set segment speed.
                      all - (optional) set all segments speed,
                      auto - segment speed will be set
                      automatically on device power on or reboot,
                      10g - segment speed will be set to 10Gb,
                      1g - segment speed will be set to 1Gb.
Ctrl.m1s2.10g: M40GBP$ set_seg_speed all auto
command succeeded.
Ctrl.m1s2.10g: M40GBP$ get_seg_speed
segment speed:          10 Gb/sec (auto)
command succeeded.
Ctrl.m1s2.10g: M40GBP$ get_seg_speed all
****** module 1, segment 1 ******
segment speed:          1 Gb/sec (auto)
****** module 1, segment 2 ******
segment speed:          10 Gb/sec (auto)
****** module 3, segment 1 ******
segment speed:          40 Gb/sec
command succeeded.
```

6.48 Heartbeat packet

6.48.1 Get heartbeat packet content

Display the current heartbeat packet content:

```
M40GBP$ get_hb_pkt
0000: 00 e0 ed 13  24 ff 00 e0    ed 13 24 fe  81 00 00 04
0010: 81 37 ff ff  00 30 00 00    00 00 40 04  ec a2 c6 13
0020: 01 02 c6 13  01 01 00 00    00 00 00 00  00 00 00 00
0030: 00 00 00 00  00 00 00 00    00 00 00 00  00 00 00 00
0040: a0 07 37 99
command succeeded.
M40GBP$
```

6.48.2 Load Heartbeat packet content

The new Heartbeat packet content should be loaded from tftp server. The file name for the new heartbeat packet should be “hb.bin”
Heartbeat packet length: 24 – 1024 bytes.

Destination MAC	XX XX XX XX XX XX	This value will be replaced by the M40GBP to the M40GBP port0/port1 MAC address
Source MAC	XX XX XX XX XX XX	This value will be replaced by the M40GBP to the M40GBP port0/port1 MAC address
VLAN	81 00 00 04	This value will be removed by device before transmitting. The user MUST include this field when preparing heartbeat packet
Packet content		Any data can be included
Checksum place holder	00 00 00 00	Real packet checksum will put here.

```
M40GBP$ load_hb_pkt 10.10.10.200 tftpboot
command succeeded.
M40GBP$
```

6.48.3 Restore default heartbeat packet content

Default heartbeat packet content can be restored by command:

```
M40GBP$ set_default_hb_pkt
command succeeded.
M40GBP$
```

6.48.4 Get/Set heartbeat packet transmit direction

Heartbeat packets can be transmitted from either MON0 or MON1 or from both ports.
By default the heartbeat packets are transmitted from MON0 port and are received by MON1 port.

```
M40GBP$ get_hb_tx_dir
hb_dir:                 mon0.
command succeeded.
M40GBP$
M40GBP$ set_hb_tx_dir mon1
command succeeded.
M40GBP$ set_hb_tx_dir bidir
command succeeded.
M40GBP$ set_hb_tx_dir mon0
command succeeded.
M40GBP$
```

6.48.5 Get/Set criteria for determine heartbeat packet failure.

The heartbeat packet failure criteria can be set to Unidirectional or Bidirectional.
The heartbeat packet failure criteria function varies according to the heartbeat packet transmit direction

While the heartbeat packets transmit direction is set to MON0 or MON1, the heartbeat packets failure criteria will be set to unidirectional state and the heartbeat packets are expected to be received by the second monitor port. If the second monitor port does not receive the heartbeat packets within the hb_holdtime time it will set the Active Bypass circuitry to the state that was set by the hb_exp_state (Bypass, Tap or linkdrop mode).

While the heartbeat packets transmit direction is set to Bidirectional (HB packets are transmitted from both monitor ports) the heartbeat packet failure criteria can be set to unidirectional or bidirectional.

Unidirectional: The M40GBP will change its state if one of the monitor ports does not receive heartbeat packets. The M40GBP will restore to its default state when both monitor ports receives the heartbeat packets.

Bidirectional: The M40GBP will change its state if both monitor ports do not receive the heartbeat packets. The M40GBP will restore to its default state if at least one of the monitor ports receives the heartbeat packets.

```
M40GBP$ get_hb_fail
hb_fail:                unidirectional.
command succeeded.
M40GBP$
M40GBP$ set_hb_fail bidir
hb_dir:                 bidirectional.
command succeeded.
M40GBP$
```

6.49 Remote log

The M40GBP is capable to send the log messages to remote log server (factory default = disable)
The Remote log should be enabled on remote server to receive messages from device.

6.49.1 Get remote log state

The M40GBP remote log state can be retrieved by command “get_remote_log_state”.

```
M40GBP$ get_remote_log_state
remote log state:          off.
command succeeded.
M40GBP$
```

6.49.2 Set remote log state

The M40GBP remote log state can be set by command “set_remote_log_state”.

```
M40GBP$ set_remote_log_state on
command succeeded.
M40GBP$ get_remote_log_state
remote log state:          on.
command succeeded.
M40GBP$ set_remote_log_state off
command succeeded.
M40GBP$
```

6.49.3 Get remote log server IP

The Remote log server IP can be retrieved by command “get_remote_log_server_ip”.
Default remote log server IP: 192.168.0.6.

```
M40GBP$ get_remote_log_server_ip
remote log server ip:       192.168.0.6
command succeeded.
M40GBP$
```

6.49.4 Set remote log server IP

The M40GBP remote log server IP can be set by command “set_remote_log_server_ip”.

```
M40GBP$ set_remote_log_server_ip 192.168.0.6
command succeeded.
M40GBP$
```

6.50 NTP (Network Time Protocol)

The M40GBP clock can be synchronized using the NTP protocol
The IBS support multi NTP servers –up to 3
NTP can be enabled or disabled (default: disable).

6.50.1 Get NTP state

The M40GBP NTP state can be retrieved by command “get_ntp_state”.

```
M40GBP$ get_ntp_state
NTP state:              off.
command succeeded.
M40GBP$
```

6.50.2 Set NTP state

The M40GBP NTP can be enabled or disabled by command “set_NTP_state”.

```
M40GBP$ set_ntp_state on
command succeeded.
M40GBP$ get_ntp_state
NTP state:              on.
command succeeded.
M40GBP$ set_ntp_state off
command succeeded.
M40GBP$
```

6.50.3 Get NTP server IP

The NTP server IP can be retrieved by command “get_ntp_server_ip”.
Default NTP server IP: 10.10.10.200

```
M40GBP$ get_ntp_server_ip
NTP server ip:          192.168.0.6
command succeeded.
M40GBP$
```

6.50.4 Set NTP server IP

The M40GBP NTP server IP can be set by command “set_ntp_server_ip”.

```
M40GBP$ set_ntp_server_ip 192.168.0.6
command succeeded.
M40GBP$
```

6.50.5 Add NTP server IP

Add NTP server IP

```
M40GBP$ get_ntp_server_ip
NTP server ip:          192.168.0.6
command succeeded.
M40GBP$ add_ntp_server_ip 192.168.0.55
command succeeded.
M40GBP$ get_ntp_server_ip
NTP server ip:          192.168.0.6
                192.168.0.55
```

6.50.6 Delete NTP server IP

```
M40GBP$ get_ntp_server_ip
NTP server ip:          192.168.0.6
command succeeded.
M40GBP$ add_ntp_server_ip 192.168.0.55
command succeeded.
M40GBP$ get_ntp_server_ip
NTP server ip:          192.168.0.6
                192.168.0.55
command succeeded.
M40GBP$ del_ntp_server_ip 192.168.0.55
command succeeded.
M40GBP$ get_ntp_server_ip
```

6.50.7 Send NTP request

Force NTP request using the command send_ntp_request

6.51 Timezone

6.51.1 Get timezone list

The Command “get_timezone_list” displays the supported time zones. The Time zones are united to groups. The Command timezone can retrieve time zone group names, all time zones in group, all time zones or all time zone which names contain some characters.

```
get_timezone_list XXX       - get timezone list (
                    all - get all timezones,
                    group - get all timezone groups,
                    "Name" - displays timezone group "Name",
                    "XXX" - get all timezones contain "XXX").
```

```
M40GBP$ get_timezone_list group
Timezone group list:
    Africa
    America/Argentina
    America/Indiana
    America/Kentucky
    America/North_Dakota
    America
    Antarctica
    Arctic
    Asia
    Atlantic
    Australia
    Brazil
    Canada
    Chile
    Etc
    Europe
    Indian
    Mexico
    Mideast
    Pacific
    US
command succeeded.
M40GBP$
```

```
M40GBP$ get_timezone_list Ala
Timezone group: Africa
        Dar_es_Salaam (GMT+3)
Is the above information OK? (Y/n)n
Timezone group: Africa
Douala (GMT+1)
Is the above information OK? (Y/n)n
Timezone group: Africa
        Kampala (GMT+3)
Is the above information OK? (Y/n)n
Timezone group: Africa
    Malabo (GMT+1)
Is the above information OK? (Y/n)n
Timezone group: America
    Guatemala (GMT-6)
Is the above information OK? (Y/n)n
Timezone group: Asia
    Kuala_Lumpur (GMT+8)
Is the above information OK? (Y/n)n
Timezone group: Pacific
Galapagos (GMT-6)
Is the above information OK? (Y/n)n
Timezone group: Pacific
Palau (GMT+9)
Is the above information OK? (Y/n)n
Timezone group: US
Alaska (GMT-9)
Is the above information OK? (Y/n)n
FAILED on error: "Not found"
M40GBP$
```

6.51.2 Get timezone

Command “get_timezone” retrieves current time zone. Default time zone is UTC (GMT+0) time zone.

```
M40GBP$ get_timezone
timezone:           Etc/UTC (GMT-0).
command succeeded.
M40GBP$
```

6.51.3 Set timezone

Several time zones supported daylight saving changes. When setting time zone the daylight saving mode can be disabled or enabled. Also can be set timezone GMT-/+ X from “Etc” group.

```
set_timezone [daylight] XXX - set current timezone (daylight - off,
                    see get_timezone_list for possible timezones).
```

```
M40GBP$ set_timezone off Mountain
Timezone group: Canada
      Mountain (GMT-7)
Is the above information OK? (Y/n)y
command succeeded.
M40GBP$ set_timezone Mountain
Timezone group: Canada
      Mountain (GMT-7)
Is the above information OK? (Y/n)n
Timezone group: US
      Mountain (GMT-7)
Is the above information OK? (Y/n)
command succeeded.
M40GBP$
```

6.51.4 Get daylight saving state

Daylight saving state can be retrieved by command “get_daylight_state”.

```
M40GBP$ get_daylight_state
daylight saving state:     off.
command succeeded.
M40GBP$
```

6.52 Get technical support information.

The command gather all the necessary information needed for the Technical Support team in order to help resolving technical problems.

```
get_support_info [XXX]      - get technical support information.
                        without parameters - get versions, build dates
                        and configuration information.
                        swd_log X - get last X lines of swdaemon log file.
                        pas_log X - get last X lines of passive bypass
                        daemon log file.
                        swctl_log X - get last X lines of swctl log file.
                        kern_log X - get last X lines of kernel (dmesg)
                        log file.
                        snmp_log X - get last X lines of snmp log file.
                        auth_log X - displays the last X lines of
                        authentication log file.
```

```
Ctrl: M40GBP$ get_support_info
--- Technical support information ---
Tue Jan 21 13:27:55 2014
full device part number:      does not set yet
device product part number:   M40GBP
Unit name:                    ibs
product tracking number:      does not set yet
device hardware version:      22.1.0.40 (P2041 rev. 1.1)
device firmware version:      0.0.9.7
device swdaemon version:      1.1.64.30
device swctl version:         1.1.64.30
u-boot version and date:      U-Boot 2011.12-sl:00.01, Dec 25 2013, 11:46:56
kernel version and date:      3.0.34-sl:00.01-rt55, #88 SMP Thu Apr 11 09:42:32 IDT 2013
swdaemon build date:          Mon Jan 20 13:59:37 2014
swctl build date:             Mon Jan 20 13:59:43 2014
badas build date:             Mon Jan 20 13:59:50 2014
snmpd build date:             Wed Jan  8 14:34:04 2014
support driver build date:    Sun Jul 28 06:05:13 2013
kernel bde driver build date: Sun Jul  7 13:41:52 2013
user bde driver build date:   Sun Jul  7 13:41:52 2013
-------------------------------------
       Configuration information
hb_count_value=5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5
hb_check_count_value=20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20, 20
watchdog_count_value=70
wdt_period=20
wdt_mode=1
features=0x040498e4, 0x040498e4, 0x040498e4, 0x040498e4, 0x040498e4, 0x040498e4,
0x040498e4,    0x040498e4, 0x040498e4, 0x040498e4, 0x040498e4, 0x040498e4
features1=0x00010080, 0x00000080, 0x00000080, 0x00000080, 0x00000080, 0x00000080,
0x00000080,    0x00000080, 0x00000080, 0x00000080, 0x00000080, 0x00000080
ip_address=0xc0a80064
subnet_mask=0xffffff00
default_gateway=0xc0a80001
enable_trap=0x0000000000000001
snmp_server_ip_address=0xc0a80006
snmp_version=1
snmp_msg_port=161
snmp_trap_port=162
radius_auth_port=1812
radius_acct_port=1813
ses_timeout=900
rx_tx_err_trap_timeout=5
rx_tx_err_threshold=10
tftp_server_ip=0xc0a80006
hb_src_mac_high=0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28,
0x00e0ed28, 0x00e   0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28
0x00380000
```

```
hb_dst_mac_high=0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28,
0x00e0ed28, 0x00e   0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28, 0x00e0ed28
hb_dst_mac_low=0x00230000, 0x00250000, 0x00270000, 0x00290000, 0x002b0000,
0x002d0000, 0x002f   0000, 0x00310000, 0x00330000, 0x00350000, 0x00370000,
0x00390000
remote_log_server_ip=0xc0a80006
ntp_server_ip=0xc0a80006
ntp_request_period=36000
tz_state=0x000e0000
uboot_param_offset=0x00000000
rootfs_size=0x00000000
mgmt_mac_high=0x00000000
mgmt_mac_low=0x00000000
rs232_speed=0
fw_ver=0x00000000
tacacs_state=0x00000000
tacacs_snmp_state=0x00000000
tacacs_server_ip=0xc0a80006
max_log_file_size=8388608
snmp_user=
snmp_read_user=customer
snmp_password=
unit_name=ibs
tftp_root=
system_user=
timezone=Etc/UTC
web_user=
web_password=
sn=does_not_set
prd_name=does_not_set
tacacs_key=
-----------------------------------
command succeeded.
Ctrl: M40GBP$
```

```
trl: M40GBP$ get_support_info kern_log 20
mpc-i2c ffe119000.i2c: timeout 1000000 us
mpc-i2c ffe119100.i2c: timeout 1000000 us
EDAC MC: Ver: 2.1.0
IPv4 over IPv4 tunneling driver
TCP cubic registered
Initializing XFRM netlink socket
NET: Registered protocol family 10
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 17
NET: Registered protocol family 15
Registering the dns_resolver key type
rtc-ds1307 0-0068: setting system clock to 2014-01-21 13:08:48 UTC (1390309728)
RAMDISK: gzip image found at block 0
VFS: Mounted root (ext2 filesystem) on device 1:0.
Freeing unused kernel memory: 244k freed
sup_drv version 0.99.5 (28/07/2013)
sup_drv: CPU version 0x82100111
linux_kernel_bde: module license 'Proprietary' taints kernel.
Disabling lock debugging due to kernel taint
eth0: no IPv6 routers present
command succeeded.
M40GBP$
```

6.53 WEB user

The command controls the WEB user name and password used for WEB interface logging.
Default WEB user name: admin
Default WEB user password: gtadmin1
WEB user name length can be from 5 to 30 characters.
WEB user password length can be from 8 to 60 characters.

6.53.1 Get WEB user name

WEB user name can be retrieved by command “get_web_user”.

```
M40GBP$ get_web_user
web user: admin
command succeeded.
M40GBP$
```

6.53.2 Set WEB user name

WEB user name can be set by command “set_web_user”.

```
M40GBP$ set_web_user customer
command succeeded.
M40GBP$
```

6.53.3 Set WEB user password

WEB user password can be set by command “set_web_user_psw”.

```
set_web_user_psw OLD NEW    - set web user password (8 - 60 characters).
```

6.54 Multi configuration mechanism

The user can save and restore several (~100) different configurations of the M40GBP parameters.
The M40GBP saves these different configurations on internal flash memory (~1 MB).
Configuration can be saved locally or on remote server by SCP protocol.
To work with remote server should be used additional parameter:
user@ScpSrvIP:[Path/][ConfName]

6.54.1 Display saved M40GBP configurations.

Command “get_list_conf” used for display the local saved M40GBP configurations.

```
M40GBP$ get_list_conf
saved configurations:
        cust1_03
        cust2_31
command succeeded.
M40GBP$
```

6.54.2 Save M40GBP configuration.

Command “save_conf” used for local and remote saving the M40GBP configuration.

```
M40GBP$ save_conf cust2_31
command succeeded.
M40GBP$
```

6.54.3 Restore the M40GBP saved configuration.

To restore saved configuration the command “restore_conf” should be used (to display saved configurations run “get_list_conf”).
After restoring configuration the M40GBP must be rebooted.

```
M40GBP$ restore_conf cust2_31
Restoring configuration require reboot device.
Continue? (Y/n)
y
rebooting...
```

6.54.4 Remove saved configuration.

The command “remove_conf” is used to remove saved configuration form the Flash memory.

```
M40GBP$ remove_conf cust1_03
command succeeded.
M40GBP$
```

6.55 Telnet access

The M40GBP support Telnet protocol. By default the Telnet access is Disabled.
The Command “get_telnet_state” is used to retrieve telnet access state.
The Command “set_telnet_state” is used to enable or disable telnet access.

```
M40GBP$ get_telnet_state
telnet state:          off.
command succeeded.
M40GBP$ set_telnet_state on
command succeeded.
M40GBP$ get_telnet_state
telnet state:          on.
command succeeded.
M40GBP$ set_telnet_state on
command succeeded.
M40GBP$
```

6.56 Statistics counters.

The M40GBP support several statistics counters. Statistics can be displayed and cleared.

```
M40GBP$ clear_stat
command succeeded.
M40GBP$
```

```
M40GBP$ get_stat
                SUM         Mon0        Mon1        Net0        Net1
RxPkts:         0           0           0           0           0
RxOctets:       0           0           0           0           0
TxOctets:       30357184    30357184    0           0           0
RxPktGood:      0           0           0           0           0
RxUnicastPkts:  0           0           0           0           0
RxMulticastPkts: 0          0           0           0           0
RxBroadcastPkts: 0          0           0           0           0
TxPktGood:      474337      474337      0           0           0
TxUnicastPkts:  474339      474339      0           0           0
TxMulticastPkts: 0          0           0           0           0
TxBroadcastPkts: 0          0           0           0           0
RxDiscards:     0           0           0           0           0
TxDiscards:     0           0           0           0           0
command succeeded.
M40GBP$
```

Statistic description:

#	Name in M40GBP statistic	Name	RFC
1	RxPkts	snmpEtherStatsPkts	RFC 1757
2	RxOctets	snmpIfInOctets	RFC 1213
3	TxOctets	snmpIfOutOctets	RFC 1213
4	RxPktGood	snmpEtherStatsRXNoErrors	RFC 1757
5	RxUnicastPkts	snmpIfInUcastPkts	RFC 1213
6	RxMulticastPkts	snmpEtherStatsMulticastPkts	RFC 1757
7	RxBroadcastPkts	snmpEtherStatsBroadcastPkts	RFC 1757
8	TxPktGood	snmpEtherStatsTXNoErrors	RFC 1757
9	TxUnicastPkts	snmpIfHCOutUcastPkts	RFC 2233
10	TxMulticastPkts	snmpIfHCOutMulticastPkts	RFC 2233
11	TxBroadcastPkts	snmpIfHCOutBroadcastPckts	RFC 2233
12	RxDiscards	snmpIfInDiscards	RFC 1213
13	TxDiscards	snmpIfOutDiscards	RFC 1213

6.57 TACACS+ (Terminal Access Controller Access Control System Plus) and RADIUS (Remote Authentication Dial In User Service) support.

The M40GBP support TACACS+ and RADIUS for remote access (WEB access, SNMP access, SSH access, Telnet access).
The M40GBP TACACS+ supports:

- clear and encrypted mode.
- Authentication and Accounting (tac_plus.rfc.1.78.txt).
- Inbound PAP Login (Password Authentication Protocol).

TACACS+ /RADUIS disabled by default.
TACACS+ / RADIUS secret key length can be from 8 to 127 characters.
Default secret key: default_tac_key.
Default TACACS+ /RADIUS server IP: 192.168.0.6
By default the Serial port access TACACS+ support is disabled.
By default there is no login fallback when the TACACS server is not available.

6.57.1 TACACS+/RADIUS state

TACACS+ /RADIUS can be enabled or disabled by command “set_tacacs_state”.
TACACS+ /RADIUS state can be retrieved by command “get_tacacs_state”.

```
set_tacacs_state XXX snmp   - set TACACS state (off - default,
                              on_clear, on_encrypted, on_radius).
                              snmp - on: enable tacacs for snmp.
                              snmp - off: disable tacacs for snmp.

Ctrl: M40GBP$ set_tacacs_state on_radius off
command succeeded.
Ctrl: M40GBP$ get_tacacs_state
TACACS state:              on, radius.
TACACS state for snmp:     off.
command succeeded.
Ctrl: M40GBP$ set_tacacs_state on_clear on
command succeeded.
Ctrl: M40GBP$ get_tacacs_state
TACACS state:              on, clear text.
TACACS state for snmp:     on.
command succeeded.
Ctrl: M40GBP$
```

6.57.2 Set TACACS+ / RADIUS server IP

The M40GBP support multi TCACS servers, the command set_tacacs_server_ip sets the main TACACS+ server.

```
M40GBP$ set_tacacs_server_ip 192.168.0.6
command succeeded.
M40GBP$
```

6.57.3 Add TACACS+ server IP

The M40GBPS support multi TACACS+/RaDIUS servers (up to 10 servers), additional TACACS+/RADIUS server can be added to the TACACS+ servers using the command add_tacacs_server_ip

```
M40GBP$ add_tacacs_server_ip 192.168.1.159
command succeeded.
M40GBP$
```

6.57.4 Del TACACS+ server IP

TCACS+ server IP can be deleted from the TACACS+ server list using the command : del_tacacs_server_ip (Main TACACS+ server cannot be deleted).

```
M40GBP$ del_tacacs_server_ip 192.168.1.159
command succeeded.
M40GBP$
```

6.57.5 Get TACACS+ server IP

TACACS+ server IP can be retrieved by command “get_tacacs_server_ip”

```
M40GBP$
TACACS server ip:  192.168.0.6
                   192.168.1.159
                   192.168.1.157
                   192.168.1.155
                   192.168.1.153
                   192.168.1.149
                   192.168.1.48
 M40GBP$
```

6.57.6 Set RS232 TACACS+ login

By default there is no TACACS+ server login validate for RS232 access.
The command set_rs232_tacacs_login enable/disable the TACACS+ login validation for RS232 access

```
M40GBP$
set_rs232_tacacs_login on|off
                   - set rs232 login via tacacs. M40GBP$ set_rs232_tacacs_login
on
M40GBP$ set_rs232_tacacs_login on
command succeeded.
M40GBP$ set_rs232_tacacs_login off

command succeeded.
```

6.57.7 Get RS232 TACACS+ login

The TACACS+ RS232 access status can be retrieved by command “get_rs232_tacacs_login”

```
M40GBP$
get_rs232_tacacs_login
rs232 tacacs login:       off
command succeeded.
M40GBP$
```

6.57.8 Set TACACS+ login fallback

By default in case that there is no TACACS+ server to validate the login credentials the login will fail and it will be possible to login to the IBS only via the Serial port.
The command set_tacacs_login_fallback enables/disable the login fallback to the local IBS credentials in case that no TACACS+ server is available.

```
M40GBP$ set_tacacs_login_fallback  on
command succeeded.
M40GBP$
```

6.57.9 Get TACACS+ login fallback

TACACS+ login fallback status can be retrieved by command "set_tacacs_login_fallback"

```
M40GBP$ get_tacacs_login_fallback
TACACS login fall back:     off
command succeeded.
M40GBP$
```

6.57.10 Set TACACS+ / RADIUS secret key

TACACS+ /RADIUS secret key can be set by command "set_tacacs_key".

```
M40GBP$ set_tacacs_key default_key
command succeeded.
M40GBP$
```

6.57.11 Set TACACS multi users flag

Multi users control allows enable/disable TACACS multi users mode.
When TACACS multi users flag is set device will not check the user account, it will rely on TACACS server.
When TACACS multi users flag is reset user can login if the M40GBP and TACACS server have this account.
TACACS multi users flag can be set by command "set_tacacs_multi_users" (default: on)

```
M40GBP$ set_tacacs_multi_users off|on
command succeeded.
M40GBP$
```

6.57.12 Display TACACS multi users flag.

The state of TACACS multi users flag can be displayed by command “get_tacacs_multi_users”

```
M40GBP$ get_tacacs_multi_users
TACACS multi-users:        off.
command succeeded.
M40GBP$
```

6.57.13 Set RADIUS authentication port

RADIUS authentication port can be set by command “set_radius_auth_port” [1024 - 49151].

```
M40GBP$ set_radius_auth_port 1812
command succeeded.
Ctrl: M40GBP$
```

6.57.14 Display RADIUS authentication port

The state of RADIUS authentication port can be displayed by command “get_ radius_auth_port”

```
Ctrl: M40GBP$ get_radius_auth_port
radius auth port:       1812
command succeeded.
Ctrl: M40GBP$
```

6.58 Permitted IP support.

The M40GBP support restricted IP address access from HTTP (HTTPS), SSH, TELNET and SNMP.
By default access allowed from any IP address.
Restricted IP access rules:
Three parameters participate in acceptance of host IP address:

1) Network IP (NetIP)
2) Network MASK (NetMask)
3) Host IP (IP)

The access is accepted only if NetIP == IP & NetMask.
Maximum number of permitted IP ranges – 20.

6.58.1 Set/delete permitted IP range

New permitted IP range can be added by command “set_ mgmt_permit_ip”

```
M40GBP$ set_mgmt_permit_ip 192.168.0.0/24
command succeeded.
M40GBP$
```

Permitted IP range can be removed by command “del_ mgmt_permit_ip”
Command get parameter NetIp/NetMask or “all”
With parameter “all” command remove all permitted IP ranges and device will receive commands from all IP.

```
M40GBP$ del_mgmt_permit_ip 192.168.0.0/24
command succeeded.
M40GBP$
```

6.58.2 Display permitted IP range

Permitted IP range can be displayed by command “get_ mgmt_permit_ip”

```
M40GBP$ get_mgmt_permit_ip
permitted ip:           192.168.0.0/24
command succeeded.
M40GBP$
```

6.58.3 Check permitted IP range

Permitted IP range can be checked by command “check_mgmt_permit_ip”

```
M40GBP$ check_mgmt_permit_ip 192.168.0.0/24
All management servers can be accessed.
command succeeded.
M40GBP$
```

6.58.4 Display current user

Current user can be displayed by command “get_current_user”

```
M40GBP$ get_current_user
current user:          customer
M40GBP$
```

6.59 M2N mode

M2N (monitor port to network port link fail) mode support link drop on network port if correspondent monitor port link gone. This Mode can be set independent for each monitor port.

```
M40GBP$ get_m2n
m2n (Mon port 0):      off.
m2n (Mon port 1):      off.
command succeeded.
M40GBP$ set_m2n MON0 on
command succeeded.
M40GBP$ get_m2n
m2n (Mon port 0):      on.
m2n (Mon port 1):      off.
command succeeded.
M40GBP$ set_m2n MON1 on
command succeeded.
M40GBP$ get_m2n
m2n (Mon port 0):      on.
m2n (Mon port 1):      on.
command succeeded.
M40GBP$ set_m2n MON1 off
command succeeded.
M40GBP$ get_m2n
m2n (Mon port 0):      on.
m2n (Mon port 1):      off.
command succeeded.
M40GBP$
```

6.60 Displaying power supplies states.

The command get_power_state displays the status of the 1U chassis power supplies
This command supported only with hardware version 0.3.0.0.11 and up.

```
M40GBP$ get_power_state
Power 1:               OK
Power 2:               OK
PASS
M40GBP$ get_power_state
Power 1:               FAIL
Power 2:               OK
PASS
```

6.60.1 Module power off.

The command power_off , causing the individual M40GBP module to be powered off.
It enable the user to replace individual M40GBP module while the rest of the M40GBP modules on the same 1U chassis are powered on up and running.
This command supported only with hardware version 0.3.0.0.11 and up.

```
M40GBP$ power_off
Shutdown….
```

6.61 Get/Set Internal VLAN ID

The IBS default internal Vlan Id is :1 .
Using the command set_int_vlan it is possible to set the internal vlan id
To command get_int_vlan_id display the current internal vlan id

```
IBSG10P set_int_vlan 2
command succeeded.
BS10GP$ get_int_vlan
Internal VLAN:        2
command succeeded.
```

6.62 SNMP

The IBS supports up to 11 different SNMP entries (Entry = user name/community).
Each entry support up to 8 different SNMP servers.
Each entry support different level of access (read only, read/write, trap only, read Only with Trap, read/write with Trap) and different SNMP version 1, 2c, and 3 (SHA and AES) and SNMP discovery.

6.62.1 SNMP_Enrty commands

There are 4 different commands which enable the option to view/select/add/delete the SNMP entries.

get_snmp_entry

To view the current SNMP entry or the view all entries use the command:
get_snmp_entry [entry_index|all] -

get current snmp entry,
all - get all entries,
1 - 11 - get correspondent entry.

```
get_snmp_entry [entry_index|all] -
                    get current snmp entry,
                    all - get all entries,
                    1 - 11 - get correspondent entry.
M40GBP$ get_snmp_entry all
snmp msg port:          161
snmp trap port:         162
TACACS state:           off.
TACACS state for snmp:  off.
permitted ip:           all
========== entry index 1 ============
snmp user:              customer
snmp version:           1
snmp community status:  on
snmp community access:  read, write, trap.
snmp server ip address: 192.168.0.6
                        192.168.0.111
snmp password:          ***
command succeeded.
M40GBP$
```

6.62.2 add_snmp_entry - Add new SNMP entry (up to 11 different entries)

```
M40GBP$ add_snmp_entry
snmp entry 2 was created
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_entry all
snmp msg port:            161
snmp trap port:           162
TACACS state:             off.
TACACS state for snmp:    off.
permitted ip:             all
========== entry index 1 ============
snmp user:                customer
snmp version:             1
snmp community status:    on
snmp community access:    read, write, trap.
snmp server ip address:   192.168.0.6
                          192.168.0.111
snmp password:            ***
========== entry index 2 ============
snmp user:
snmp version:             1
snmp community status:    off
snmp community access:    read.
snmp server ip address:
snmp password:
command succeeded.
M40GBP$
```

6.62.3 Select SNMP entry - sel_snmp_entry -

In order to modify the SNMP entry, select the entry from the list of current active entries which showed by the get_snmp_entry

sel_snmp_entry entry_index - select snmp entry (1 - 11).

```
M40GBP$ sel_snmp_entry 2
command succeeded.
M40GBP$
M40GBP$ get_snmp_entry
========== entry index 2 ============
snmp user:
snmp version:              1
snmp community status:     off
snmp community access:     read.
snmp server ip address:
snmp password:
command succeeded.
M40GBP$
```

6.62.4 Set/get_snmp_user

set_snmp_user XXX - set snmp user name (5 - 30 symbols).

```
M40GBP$ set_snmp_user test1
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_user
snmp user:              test1
command succeeded.
M40GBP$
M40GBP$ get_snmp_entry
========== entry index 2 ============
snmp user:              test1
snmp version:            1
snmp community status:     off
snmp community access:     read.
snmp server ip address:
snmp password:
command succeeded.
M40GBP$
M40GBP$
M40GBP$ get_snmp_entry all
snmp msg port:           161
snmp trap port:          162
TACACS state:            off.
TACACS state for snmp:     off.
permitted ip:            all
========== entry index 1 ============
snmp user:              customer
snmp version:            1
snmp community status:     on
snmp community access:     read, write, trap.
snmp server ip address:    192.168.0.6
                        192.168.0.111
snmp password:           ***
========== entry index 2 ============
snmp user:              test1
snmp version:            1
snmp community status:     off
snmp community access:     read.
snmp server ip address:
snmp password:
command succeeded.
```

6.62.5 snmp version

set_snmp_ver XXX - set snmp version (1, 2c, 3, default - 1)
get_snmp_ver

```
M40GBP$ get_snmp_ver
snmp version:            1
command succeeded.
M40GBP$ set_snmp_ver 3
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_ver
snmp version:            3
command succeeded.
M40GBP$
M40GBP$ get_snmp_entry
========== entry index 2 ============
snmp user:               test1
snmp version:            3
snmp community status:   off
snmp community access:   read.
snmp server ip address:
snmp password:
command succeeded.
M40GBP$
```

6.62.6 snmp server ip

The IBS support up to 8 different SNMP servers, each SNMP server can be assigned to one of the 11 SNMP entries.
There are 4 different commands to control the SNMP servers IP:
get_snmp_srv_ip - show the SNMP servers IP for the current selected entry
add_snmp_srv_ip - add SNMP server IP to the current selected entry
del_snmp_srv_ip - delete SNMP server IP from the current selected entry
set_snmp_srv_ip - modify the main SNMP server IP for the current selected entry

6.62.7 get_snmp_srv_ip

Show the SNMP servers IP for the current selected entry

```
M40GBP$ get_snmp_srv_ip
snmp server ip address:     192.168.0.44
command succeeded.
M40GBP$ sel_snmp_entry 1
command succeeded.
M40GBP$ get_snmp_srv_ip
snmp server ip address:     192.168.0.44
                            192.168.0.111
                            192.168.0.33
command succeeded.
M40GBP$ sel_snmp_entry 2
command succeeded.
M40GBP$ get_snmp_srv_ip
snmp server ip address:     192.168.0.44
command succeeded.
M40GBP$
```

6.62.8 add_snmp_srv_ip

```
M40GBP$ get_snmp_srv_ip
snmp server ip address:     192.168.0.44
                            192.168.0.111
command succeeded.
M40GBP$ del_snmp_srv_ip 192.168.0.111
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_srv_ip
snmp server ip address:     192.168.0.44
command succeeded.
M40GBP$
```

6.62.9 del_snmp_srv_ip

Note: The main SNMP srv_ip cannot be deleted.

```
M40GBP$ get_snmp_entry
========== entry index 1 ============
snmp user:                customer
snmp version:               1
snmp community status:      on
snmp community access:      read, write, trap.
snmp server ip address:     192.168.0.44
                            192.168.0.111
                            192.168.0.33
snmp password:              ***
command succeeded.
M40GBP$ del_snmp_srv_ip 192.168.0.33
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_entry
========== entry index 1 ============
snmp user:                customer
snmp version:               1
snmp community status:      on
snmp community access:      read, write, trap.
snmp server ip address:     192.168.0.44
                            192.168.0.111
snmp password:              ***
command succeeded.
M40GBP$
```

6.62.10 set_snmp_srv_ip - modify the IP address of the main SNMP server

set_snmp_srv_ip xxx.xxx.xxx.xxx
- set MAIN snmp server ip address
(default - 192.168.0.6).

```
M40GBP$ sel_snmp_entry 2
command succeeded.
M40GBP$ get_snmp_entry
========== entry index 2 ============
snmp user:                test1
snmp version:              3
snmp community status:     off
snmp community access:     read.
snmp server ip address:    192.168.0.7
                           192.168.0.33
snmp password:
command succeeded.
M40GBP$ set_snmp_srv_ip 192.168.0.44
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_entry
========== entry index 2 ============
snmp user:                test1
snmp version:              3
snmp community status:     off
snmp community access:     read.
snmp server ip address:    192.168.0.44
                           192.168.0.33
snmp password:
command succeeded.
M40GBP$
```

6.62.11 snmp community access – get/set_snmp_access

Each entry support different level of access (read only, read/write, trap only, read only with Trap.

set_snmp_access access - set snmp community access
read, read_write,
trap, read_trap, read_write_trap.

get_snmp_access

```
M40GBP$ get_snmp_access
snmp community access:      read.
command succeeded.
M40GBP$ set_snmp_access read_write
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
scommand succeeded.
M40GBP$ get_snmp_access
snmp community access:      read, write.
command succeeded.
M40GBP$ get_snmp_entry
========== entry index 1 ============
snmp user:                  customer
snmp version:               1
snmp community status:      on
snmp community access:      read, write.
snmp server ip address:     192.168.0.44
                            192.168.0.111
snmp password:              ***
command succeeded.
M40GBP$
```

6.62.12 snmp password – set_snmp_user_psw

The SNMP V 3 requires to set password to encrypt decrypt the SNMP information.
set_snmp_user_psw
set_snmp_user_psw [OLD] NEW - set snmp user password (8 - 60 symbols).

```
M40GBP$ set_snmp_user_psw gtadmin1
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$
```

6.62.13 snmp community status (get/set_snmp_status)

The snmp_comunity_status activate or deactivate the SNMP entry
set_snmp_status off/on - set snmp community status.

```
M40GBP$ get_snmp_status
snmp community status:      on
command succeeded.
M40GBP$ set_snmp_status off
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
command succeeded.
M40GBP$ get_snmp_status
snmp community status:      off
command succeeded.
M40GBP$
```

6.62.14 SNMP TRAP IP port - get/set_snmp_trap_port

Control the SNMP tap IP port
set_snmp_trap_port XXX - set snmp trap port
(min - 1, max - 49151,default - 162).
get_snmp_trap_port

```
M40GBP$ get_snmp_trap_port
snmp trap port:          166
command succeeded.
M40GBP$ set_snmp_trap_port 162
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
^[[Acommand succeeded.
M40GBP$ get_snmp_trap_port
snmp trap port:          162
command succeeded.
M40GBP$
```

6.62.15 SNMP MSG IP port - get/set_snmp_msg_port

Control the SNMP msg IP port
set_snmp_msg_port XXX - set snmp msg port
(min - 1, max - 49151,default - 161).
get_snmp_msg_port

```
M40GBP$ get_snmp_msg_port
snmp trap port:          164
command succeeded.
M40GBP$ set_snmp_trap_port 161
New SNMP setting will take effect after apply_snmp.
command succeeded.
M40GBP$ apply_snmp
SNMP restart is in progress, please wait.
^[[Acommand succeeded.
M40GBP$ get_snmp_trap_port
snmp trap port:          161
command succeeded.
M40GBP$
```

SNMP variables
Variable code:
.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).GarlandTechnologies(39974).M40GBP(2).X.0

Variable name	Variable code (X=)	Type	Attributes	Value	Description
M40GBPDevName	1.2	OCTET STRING (SIZE(1..32))	read-only		Unit name.
M40GBPDevTrackingNumber	1.3	OCTET STRING (SIZE(1..32))	read-only		Get device tracking number.
M40GBPDevHwVer	1.4	OCTET STRING (SIZE(1..32))	read-only		Get device hardware version.
M40GBPDevFwVer	1.5	OCTET STRING (SIZE(1..32))	read-only		Get device firmware version.
M40GBPSnmpAgentVer	1.6	OCTET STRING (SIZE(1..32))	read-only		SNMP agent version
M40GBPMon0Link	1.8	INTEGER	read-only	down(1), up(2)	Monitor port 0 link status.
M40GBPMon1Link	1.9	INTEGER	read-only	down(1), up(2)	Monitor port 1 link status.
M40GBPNet0Link	1.10	INTEGER	read-only	down(1), up(2)	Network port 0 link status.
M40GBPNet1Link	1.11	INTEGER	read-only	down(1), up(2)	Network port 1 link status.
M40GBPApplState	1.12	INTEGER	read-only	unknown(1), fail(2), alive(3)	Application state.
M40GBPTermStatus	1.13	INTEGER	read-only	disconnected(1), connected(2)	Rs232 management port status.
M40GBPLogLastLine	1.14	INTEGER	read-only		Get log file last line number.
M40GBPLogReadLine	1.15	INTEGER	read-write		Get/set log file line number to read from.
M40GBPGetLog	1.16	OCTET STRING (SIZE(1..2048))	read-only		Get log file content (20 lines beginning from the last read line).
M40GBPDevUbootVer	1.17	OCTET STRING (SIZE(1..128))	read-only		Get U-boot version.
M40GBPDevKernelVer	1.18	OCTET STRING (SIZE(1..128))	read-only		Get kernel version.
M40GBPLogType	1.19	INTEGER	read-write	swdaemon(1), swctl(2), passive(3), snmp(4), kern(5), auth(6)	Get/set log file type.
M40GBPSupportInfo	1.20	OCTET STRING (SIZE(1..2550))	read-only		Get technical support information.
M40GBPStatistics	1.21	OCTET STRING (SIZE(1..2550))	read-only		Get device statistics counters.
M40GBPClearStatistics	1.22	INTEGER	read-write	clear(1)	Clear device statistics. Set only variable, read will return zero.
M40GBPPowerStatus	1.23	OCTET STRING (SIZE(10.128))	read-only		Get device power status
M40GBPHealthStatus	1.24	OCTET STRING (SIZE(25..2550))	read-only		Get fan status and temperature info
M40GBPSupportParams	1.25	OCTET STRING (SIZE(1..2550))	read-only		Get the current M40GBP parameters values
M40GBP SnmpVer	2.1	INTEGER	read-write	1(1), 2c(2), 3(3)	Set SNMP version. Take effect after setting M40GBPSnmpApply
M40GBP SnmpServerIp	2.2	IpAddress	read-write		Set/Get SNMP server IP address. Take effect after setting M40GBP SnmpApply
M40GBP SnmpUser	2.3	OCTET STRING (SIZE(1..64))	read-write		Set SNMP user/community and WEB interface user name.

					Take effect after setting M40GBPSnmpApply
M40GBP SnmpPassword	2.4	OCTET STRING (SIZE(17..121))	write-only		Define the SNMP v3 and WEB interface password. Parameter consists of old and new passwords separated by semicolon. Take effect after setting M40GBPSnmpApply
M40GBP SnmpApply	2.5	INTEGER	write-only	apply (1)	Activate all the SNMP changes.
M40GBP SysTime	3.1	OCTET STRING (SIZE(1..32))	read-write		Set/Get device current time/Date.
M40GBP SysIp	3.3	IpAddress	read-write		Set/Get M40GBP IP address.
M40GBP SysNetmask	3.4	IpAddress	read-write		Set/Get M40GBP IP subnet mask.
M40GBP SysGateway	3.5	IpAddress	read-write		Set/Get M40GBP gateway IP address.
M40GBP SysResetLog	3.6	INTEGER	write-only	reset	Reset/Clear M40GBP log file.
M40GBP SysReboot	3.8	INTEGER	write-only	reboot (1)	Reboot the M40GBP.
M40GBP UnitName	3.9	OCTET STRING (SIZE(1..32))	read-write		Set/Get unit name
M40GBP SysTftpIp	3.10	IpAddress	read-write		Set/Get TFTP server IP address.
M40GBP SysTftpRoot	3.11	OCTET STRING (SIZE(1..64))	read-write		Set/Get TFTP server root directory.
M40GBP SysUpdate	3.12	INTEGER	read-write	update(1), force(2)	Update the M40GBP firmware. .
M40GBP SysUpdateStatus	3.13	OCTET STRING (SIZE(1..1024))	read-only		Get M40GBP firmware update status.
M40GBP SysResetErr	3.14	INTEGER	read-write	reset(1)	Reset/Clear M40GBP errors.
M40GBPSysWhoami	3.15	INTEGER	read-write	on(1), off(2)	Unit identification. On/off system OK led blink.
M40GBPSysRemoteLog	3.16	INTEGER	read-write	on(1), off(2)	Get/set remote log state. NOTE: next SNMP command should be send not before 1 sec after this command
M40GBPSysRAemoteLogIp	3.17	IpAddress	read-write		Set/Get remote log server IP address. NOTE: next SNMP command should be send not before 1 sec after this command
M40GBPSysNTP	3.18	INTEGER	read-write	on(1), off(2)	Get/set NTP state.
M40GBPSysNTPServerIp	3.19	IpAddress	read-write		Set/Get NTP server IP address.
M40GBPSysDayLight	3.20	INTEGER	read-write	default(1), off(2)	Get/set daylight saving mode. The daylight saving mode will be set finally by M40GBPSysTimezone.
M40GBPSysTimezone	3.21	OCTET STRING (SIZE(1..64))	read-write		Get/set device timezone. Timezone examples: America/Barbados, Asia/Bangkok. Full list of supported names can be found in Linux. Command sets the default daylight saving mode. To disable default daylight saving mode perform
M40GBPSysWebUser	3.22	OCTET STRING (SIZE(5..30))	read-write		Get/set the WEB user name.
M40GBPSysWebPassword	3.23	OCTET STRING (SIZE(17..121))	read-write		Set the WEB user password.Set only variable, read will return zero length string. Parameter consists of old and new passwords separated by semicolon.
M40GBPSysSaveConfig	3.24	OCTET STRING (SIZE(4..20))	read-write		Save device configuration. Set only variable, read will return zero.
M40GBPSysRestoreConfig	3.25	OCTET STRING (SIZE(4..20))	read-write		Restore device configuration. Set only variable, read will return zero. The unit will be rebooted.

M40GBPSysRemoveConfig	2.26	OCTET STRING (SIZE(4..20))	read-write		Remove device configuration. Set only variable, read will return zero.
M40GBPSysGetConfig	2.27	OCTET STRING (SIZE(1..2550))	read-only		Get saved device configurations.
M40GBPSysGetConfigNext	3.28	OCTET STRING (SIZE(1..2550))	read-only		Get saved device configurations next buffer.
M40GBPSysTacacsKey	3.29	OCTET STRING (SIZE(8..127))	read-write		Set the Tacacs secret key.
M40GBPSysTacacsState	3.30	INTEGER	read-write	off(1), on_clear(2), on_encrypted (2)	Get/set TACACS state.
M40GBPSysTacacsServerIp	3.31	IpAddress	read-write		Get/set the IP address of the TACACS server.
M40GBPSysTelnetState	3.32	INTEGER	read-write	off(1), on(2)	Get/set Telnet state.
M40GBPSysSetMgmtPermitIP	3.35	OCTET STRING (SIZE(9..2550))	read-write		Add the management port permitted network IP address. String consists of IP and netmask separated by semicolon (192.168.0.0/24;193.151.0.0/22)
M40GBPSysRemoveMgmtPermitIP	3.36	OCTET STRING (SIZE(9..2550))	read-write		Remove one or all management port permitted network IP. String consists of IP address and netmask address separated by semicolon (192.168.0.0/24;193.151.0.0/22 | all_permitted_ip)
M40GBPSysGetMgmtPermitIP	3.37	OCTET STRING (SIZE(9..2550))	read-write		Display management port permitted network IP. String consists of IP and netmask separated by semicolon (192.168.0.0/24;193.151.0.0/22)
M40GBPSysTacacsMultiUsers	3.38	INTEGER	read-write	off(1), on(2)	Get/set TACACS multi users state.
M40GBPSysSetTrapAccount	3.39	OCTET STRING (SIZE(9..2550))	read-write		Add the SNMP monitor server trap account. String consists of IP addresses, community name and password separated by semicolon. (192.168.0.0/community1/gt82d7yfr; 193.151.0.0/community2/) Take effect after setting M40GBPSnmpApply.
M40GBPSysRemoveTrapAccount	3.40	OCTET STRING (SIZE(9..2550))	read-write		Remove one or all SNMP monitor server trap accounts. String consists of IP addresses separated by semicolon. (192.168.0.0;193.151.0.0 | all_trap_accounts) Take effect after setting M40GBPSnmpApply.
M40GBPSysGetTrapAccount	3.41	OCTET STRING (SIZE(9..2550))	read-only		"Display SNMP monitor server trap accounts. String consists of IP addresses and community name and password separated by semicolon. (192.168.0.0/community1/**********; 193.151.0.0/community2/not set)
M40GBPSysPowerOff	3.42	INTEGER	read-write	Poweroff(1)	Power off the M40GBP unit.
M40GBPSysCurrentSeg	3.43	OCTET STRING (SIZE(2..4))	read-only		Get current module:segment. module id and segment id separated by colon
M40GBPSysGetDevProp	3.44	CTET STRING (SIZE(9..2550))	read-only		Display device properties
M40GBPSysRadiusAuthPort	3.45	INTEGER	read-write	Default - 1812, min - 1024, max -	Get/set the Radius authentication port

				49151	
M40GBPSysRadiusAcctPort	3.46	INTEGER	read-write	Default - 1812, min - 1024, max - 49151	Get/set the Radius accounting port
ibsSysRxTxErrTrap	3.48	INTEGER	read-write	off(1), on(2)	Enable generating trap when rx/tx error happened
M40GBPSysRxTxErrTrapTimeout	3.49	INTEGER	read-write		Next rx/tx trap will be generated not earlier than timeout time (sec). Timeout value should be set more than zero
M40GBPSysRxTxErrMonAction	3.50	INTEGER	read-write		Allow to choose network ports state when errors detected on monitor port
M40GBPSysRxTxErrNetAction	3.51	INTEGER	read-write		Allow to choose network ports state when errors detected on network ports
M40GBPSysRxTxErrRateThreshold	3.52		read-write		Network ports state that was configured will be activated, when error rate threshold will be reached (err/sec). Error rate threshold value should be set more than zero
ibsSysSegSpeed	3.53	INTEGER	read-write	auto(1), 10g(2), 1g(3),	Get/set dual-rate segment speed.
M40GBPConf2pl	4.1	INTEGER	read-write	enable (1), disable (2)	Get/Set two-port link mode
M40GBPConfHbExpState	4.2	INTEGER	read-write	bypass(2), tap(3), linkdrop(4) tapi12(5), tapa(6), tapai1(7), tapai2(8), tapai12(9)	Get/Set heartbeat expiration mode.
M40GBPConfHbInterval	4.3	INTEGER	read-write		Get/Set heartbeat interval.
M40GBPConfHbHoldTime	4.4	INTEGER	read-write		Get/Set heartbeat hold time
M40GBPConfHbActModeLock	4.5	INTEGER	read-write	enable (1), disable (2)	Get/Set heartbeat active mode lock state.
M40GBPConfHttps	4.6	INTEGER	read-write	enable (1), disable (2)	Get/Set HTTPS protocol enable status.
M40GBPConfSesTimeout	4.7	INTEGER	read-write		Get/Set WEB session timeout.
M40GBPConfEnActHbRestore	4.8	INTEGER	read-write	enable (1), disable (2)	Set/Get enable active heartbeat restore.
M40GBPConfHbPkt	4.11	OCTET STRING (SIZE(48..2048))	read-write		Get current heartbeat packet content. Set new heartbeat packet content. Packet size: 24-1024 bytes.
M40GBPConfHbTxDir	4.12	INTEGER	read-write	mon0(1) mon1(2) bidir(3)	Set/Get heartbeats transmit port. If M40GBPConfHbTxDir is set to either mon0 or mon1 the M40GBPConfHbFail will be reset to unidir.
M40GBPConfHbFail	4.13	INTEGER	read-write	unidir(1) bidir(2)	Set/Get criteria for determine heartbeat failure. If M40GBPConfHbTxDir set to either mon0 or mon1, the M40GBPConfHbFail must be set to unidir.
M40GBPConfDefHbPkt	4.14	INTEGER	read-write	default(1)	Restore default heartbeat packet content. Set only variable, read will return zero.
M40GBPConfMgmtPortParams	4.15	INTEGER	read-write	auto(1), force_10h(2)	Set/Get ethernet management port parameters.

M40GBPConfM2n	4.16	OCTET STRING (SIZE(5..7))	read-write		Set/Get the monitor port link to network link feature state. Set Example: 'on;off' - enable this feature for MON0 and disable for MON1 Get Example: 'MON0: on;MON1: off'.
M40GBPConfWeb	4.17	INTEGER	read-write	off(1), on(2)	Set/Get WEB interface state (on/off)
M40GBPOpHbActMode	5.1	INTEGER	read-write	on (1), off (2)	Get/Set heartbeat active mode on/off.
M40GBPOpActBypass	5.2	INTEGER	read-write	off (1), on (2), tap (3), linkdrop(4), tapi12(5), tapa(6), tapai1(7), tapai2(8), tapai12(9)	Get/Set the state of the active bypass state (inline/bypass/tap/linkdrop).
M40GBPOpPasBypass	5.3	INTEGER	read-only	off (1), on (2)	Get the state of the passive bypass state.
M40GBPRecoveryDefault	6.1	INTEGER	write		Restore system default parameter.
M40GBPTrapConfApplFail	7.2	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on application failed/restored events status change: M40GBP TrapApplFail / M40GBPTrapApplRecover.
M40GBPTrapConfBypass	7.3	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on bypass(passive and Active) status change events: M40GBPTrapActBypassOn / M40GBP TrapActInlineOn, M40GBP TrapPasBypassOn / M40GBPTrapPasBypassOff, M40GBP TrapTapOn, M40GBPTrapLinkDropOn, M40GBP TrapTapi12On, M40GBP TrapTapaOn, M40GBP TrapTapai1On, M40GBP TrapTapai2On, M40GBP TrapTapai12On.
M40GBPTrapConfMonLink	7.4	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on Monitor ports Link status change events: M40GBP TrapMon0LinkDown / M40GBPTrapMon0LinkUp, M40GBP TrapMon1LinkDown / M40GBPTrapMon1LinkUp.
M40GBPTrapConfNetLink	7.5	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on Network ports Link status change events: M40GBP TrapNet0LinkDown / M40GBP TrapNet0LinkUp, M40GBP TrapNet1LinkDown / M40GBPTrapNet1LinkUp.
M40GBPTrapConfTerm	7.6	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on Terminal connect / disconnect status change events: M40GBP TrapTermDisc / M40GBP TrapTermCon.
M40GBPTrapConfErr	7.7	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on error reports from the system: M40GBPTrapErr.

M40GBPTrapConfLogSize	7.8	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on Log size overflow: M40GBP TrapLogSize.
M40GBPTrapConfUpdate	7.10	INTEGER	read-write	enable (1), disable (2)	Enable/Disable getting trap info on update finish event: M40GBPTrapUpdate, M40GBPTrapUpdateReboot

6.63 Get/Set snmp traps enable state. (get/set_trap)

SNMP traps can be enabled or disabled from CLI interface by using set_trap command.
Default – all traps disabled.
Command gets several parameters:

set_trap [trap,..] trap new_state

- new_state – on/off
- trap –
  - appl - application state change trap.
  - bp - bypass state change trap.
  - mon - monitor ports state change trap.
  - net - network ports state change trap.
  - term - terminal port state change trap.
  - error - error happened trap, power supply restored, CPU fan restored.
  - update - update finished trap.
  - all - all traps.

SNMP trap enable state can be get by get_en_trap command. Command does not get parameters.

```
M40GBP$ get_trap
trap status: 0x00000000
trap M40GBPTrapApplFailed          : off
trap M40GBPTrapApplRecovered    : off
trap M40GBPTrapMon0LinkDown   : off
trap M40GBPTrapMon0LinkUp       : off
trap M40GBPTrapMon1LinkDown   : off
trap M40GBPTrapMon1LinkUp       : off
trap M40GBPTrapNet0LinkDown    : off
trap M40GBPTrapNet0LinkUp       : off
trap M40GBPTrapNet1LinkDown   : off
trap M40GBPTrapNet1LinkUp       : off
trap M40GBPTrapTermDisc          : off
trap M40GBPTrapTermConnect      : off
trap M40GBPTrapError               : off
trap M40GBPTrapLogSize           : off
trap M40GBPTrapPasBypassOff    : off
trap M40GBPTrapPasBypassOn     : off
trap M40GBPTrapActNormalOn     : off
trap M40GBPTrapActBypassOn     : off
trap M40GBPTrapActTrapOn         : off
trap M40GBPTrapUpdate              : off
trap M40GBPTrapLinkDropOn        : off
trap M40GBPTrapUpdateReboot    : off
trap M40GBPTrapTapi12On          : off
trap M40GBPTrapTapaOn              : off
PASS
M40GBP$
```

```
trap M40GBPTrapTapai1On          : off
trap M40GBPTrapTapai2On          : off
rap M40GBPTrapTapai12            : off
trap M40GBPTrapPower1OK                  : off
trap M40GBPTrapPower2OK                  : off
trap M40GBPTrapTemperatureOK     : off
trap M40GBPTrapRxTxError         : off

M40GBP$ set_trap  on all
PASS
M40GBP$
M40GBP$ set_trap  off appl bp mon
PASS
M40GBP$
```

6.64 SNMP traps.

Trap	Value	Description
M40GBPTrapStart	1	Reserved
M40GBPTrapApplFail	2	Trap is sent when the Monitor application does not send back the HB packets within the hold time Interval defined by hb_holdtime variable.
M40GBPTrapApplRecover	3	Trap is sent when the Monitor application starts again to send the HB packets
M40GBPTrapPasBypassOn	4	Trap is sent when passive bypass changes to bypass mode.
M40GBPTrapPasBypassOff	5	Trap is sent when passive bypass changes to inline mode.
M40GBPTrapActBypassOn	6	Trap is sent when active bypass changes to bypass mode.
M40GBPTrapActInlineOn	7	Trap is sent when active bypass changes to inline mode.
M40GBPrapMon0LinkDown	8	Trap is sent when monitor port-0 link drops.
M40GBPTrapMon0LinkUp	9	Trap is sent when monitor port-0 link is restored.
M40GBPTrapMon1LinkDown	10	Trap is sent when monitor port-1 link drops.
M40GBPTrapMon1LinkUp	11	Trap is sent when monitor port-1 link is restored.
M40GBPTrapNet0LinkDown	12	Trap is sent when network port-0 link drops.
M40GBPTrapNet0LinkUp	13	Trap is sent when network port-0 link is restored.
M40GBPTrapNet1LinkDown	14	Trap is sent when network port-1 link drops.
M40GBPTrapNet1LinkUp	15	Trap is sent when network port-1 link is restored.
M40GBPTrapTermDisc	16	Trap is sent when local serial RS232 connection is disconnected.
M40GBPTrapTermCon	17	Trap is sent when local serial RS232 connection is connected.
M40GBPTrapErr	18	Trap is sent as indication of an error within the M40GBP, with some description of the error.
M40GBPTrapLogSize	19	Trap is sent when the log file size exceed its maximum allowed size.
M40GBPTrapTapOn	20	This trap is sent when switch changes mode to tap.
M40GBPTrapUpdate	21	Trap is sent when firmware update is finished.
M40GBPTrapLinkDropOn	22	This trap is sent when switch changes mode to linkdrop.
M40GBPTrapUpdateReboot	23	Trap is sent when firmware update is finished and device is rebooted.
M40GBPTrapTapi12On	24	Trap is sent when active bypass changes to TAPI12 mode.
M40GBPTrapTapaOn	25	Trap is sent when active bypass changes to TAPA mode.
M40GBPTrapTapai1On	26	Trap is sent when active bypass changes to TAPAI1 mode.
M40GBPTrapTapi2On	27	Trap is sent when active bypass changes to TAPAI2 mode.
M40GBPTrapTapi12On	28	Trap is sent when active bypass changes to TAPAI12 mode.
M40GBPTrapPower1OK	29	This trap is sent when power supply 1 restored from failure.
M40GBPTrapPower2OK	30	This trap is sent when power supply 2 restored from failure.
M40GBPTrapCpuFanOK	31	This trap is sent when CPU FAN restored from failure.
M40GBPTrapRxTxError	32	This trap is sent when device detect RX or TX error.
ibsTrapNet0Disable2pl	33	This trap is sent when network port 0 was disable by 2pl function
ibsTrapNet0Enable2pl	34	This trap is sent when network port 0 was enable by 2pl function
ibsTrapNet1Disable2pl	35	This trap is sent when network port 1 was disable by 2pl function

ibsTrapNet1Enable2pl	36	This trap is sent when network port 1 was enable by 2pl function
ibsTrapNet0Disable2plM2n	37	This trap is sent when network port 0 was disable by 2pl/m2n function
ibsTrapNet0Enable2plM2n	38	This trap is sent when network port 0 was enable by 2pl/m2n function
ibsTrapNet1Disable2plM2n	39	This trap is sent when network port 1 was disable by 2pl/m2n function
ibsTrapNet1Enable2plM2n	40	This trap is sent when network port 1 was enable by 2pl/m2n function
ibsTrapNTPError	41	This trap is sent when NTP server does not respond

6.65 SNMP request examples (net-snmp application)

SNMP v1 get request:

snmpget -v 1 -c customer 10.10.10.20000 M40GBP-MIB::M40GBP TrapConfTerm**.0**

SNMP v1 set request:

snmpset -v 1 -c customer 10.10.10.20000 M40GBP-MIB::M40GBP TrapConfTerm**.0** = **on**

SNMP v2c get request:

snmpget -v 2c -c customer 10.10.10.20000 M40GBP-MIB::M40GBP TrapConfTerm**.0**

SNMP v2c set request:

snmpset v 2c -c customer 10.10.10.20000 M40GBP-MIB::M40GBP TrapConfTerm**.0** = **on**

SNMP v3 get request:

snmpget -v 3 -u customer -l authPriv -a SHA -A gtadmin1 -x AES -X gtadmin1 10.10.10.20000 M40GBP-MIB:: M40GBP TrapConfTerm**.0**

SNMP v3 set request:

snmpset -v 3 -u customer -l authPriv -a SHA -A gtadmin1 -x AES -X gtadmin1 10.10.10.20000 M40GBP-MIB:: M40GBP TrapConfTerm**.0** = **on**

6.66 Dispalying log file via SNMP

Use the following command to control the log display via SNMP

1) M40GBPLogType xxx – set log file type (swdaemon, swctl, passive, snmp, kernel, auth)
2) M40GBPLogLastLine – Get log file last line number.
3) M40GBPLogReadLine 0 (xxx) - Read the log file from line xxx
4) M40GBPGetLog - Read 20 lines form the log file

Note: When reading the log file forward incrementing read line number is automatic.
When reading the log file backward read line number should be set by “M40GBPLogReadLine xxx

6.67 SNMP agent, net-snmp and copyright

Device SNMP agent based on net-snmp-5.4.1 package. (see NET-SNMP Copyright.)

7 Web interface

7.1 Disable/Enable WEB interface.

The command set_web is used for disable/enable WEB interface.
The command get_web is used for displaying WEB interface state.

```
M40GBP$ get_web
WEB interface:          on.
command succeeded.
M40GBP $ set_web off
command succeeded.
M40GBP $ get_web
WEB interface:          off.
command succeeded.
```

7.2 Starting web interface

The M40GBP WEB interface can be access from any WEB browser. To connect to the M40GBP WEB interface use the following address on your WEB browser:

- If https enabled: “https://device_ip_address/index.html.en”
- If https disabled: “http:// device_ip_address/index.html.en”

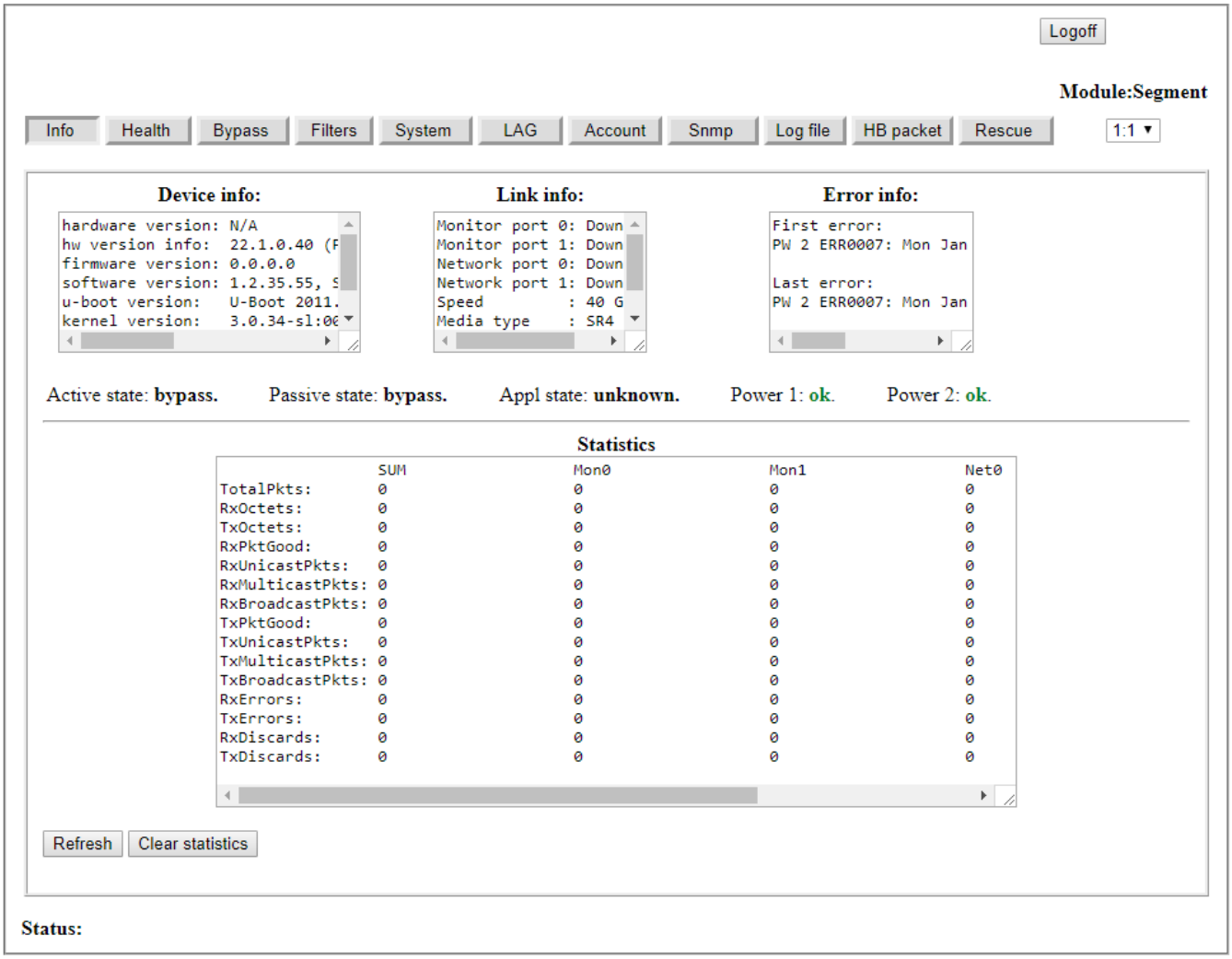
Where device_ip_address – M40GBP Ethernet Management port IP address.
Note:

- If the WEB interface is inactive more than the web_expired_time, a login screen will be prompt.
- Most web application fields contain context help.
- The new settings in the WEB interface will take affect only after clicking the “**apply**” button.

7.3 Login

On the login screen type the user name and the password. (Default user name is “admin”. Default password is “gtadmin1”).
User name should include minimum 5 symbols and can be up to 64 symbols.
Password should include minimum 8 symbols and can be up to 128 symbols.
The first user that will be logged in to the WEB interface will get all the rights (Control /monitor) of the Web interface application, the next users will not able to control device, they will be able only to monitor the M40GBP parameters.
When first user will be logged off from the WEB interface, the next user will receive his rights and will be able to (Control /monitor) the WEB interface.

7.4 Information page



7.4.1 Logoff

The M40GBP will terminate the WEB session in case that the WEB session is passive (does not send request to the M40GBP) for more than the time defined by the web_expired_time (default 900 sec).
If the main WEB interface window will be closed others than by pressing on "Logoff" button, the WEB interface will be unavailable for the time defined by the web_expired_time (default 900 sec).

7.4.2 Module:segment

The selected value on the **module:segment** pull down menu determine which module /segment is currently controlled by the current web session.

7.4.3 Information area description.

The WEB interface includes five Information areas:

- Device info
- Link info
- Error info
- Status info
- Statistics

The Information area includes read only information

7.4.3.1 Device info area description

The Device info area contains common information:

- Device hardware version
- Device firmware version
- Device software version
- Device U-boot version
- Device Kernel version
- Device tracking number

7.4.3.2 Link info area description

The Link info area contains link information:

- Monitor ports link status (down/up)
- Network port link status (down/up)
- Rs232 management port connect status (connected/disconnected)

7.4.3.3 Error info

Error info area contains the first and last error (Hardware /software) descriptions.

7.4.3.4 Status information

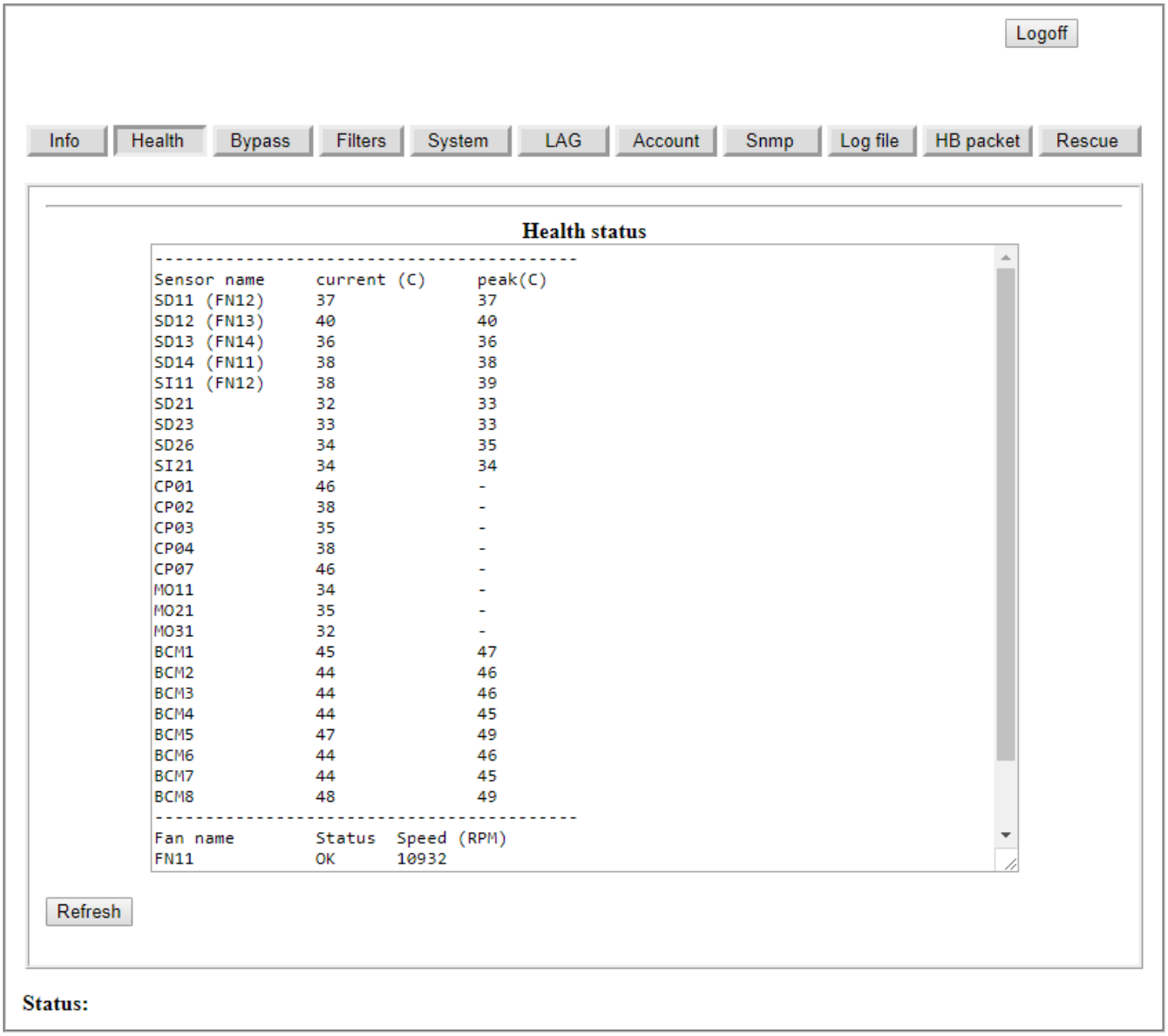
The Status information area contains status information:

- Active state (bypass/inline/tap/linkdrop)
- Passive state (bypass/inline)
- Application state (alive/fail/unknown)
- First power supply status
- Second power supply status

7.4.3.5 Statistic information

The Statistic information area contains network statistic information on the different M40GBP ports:

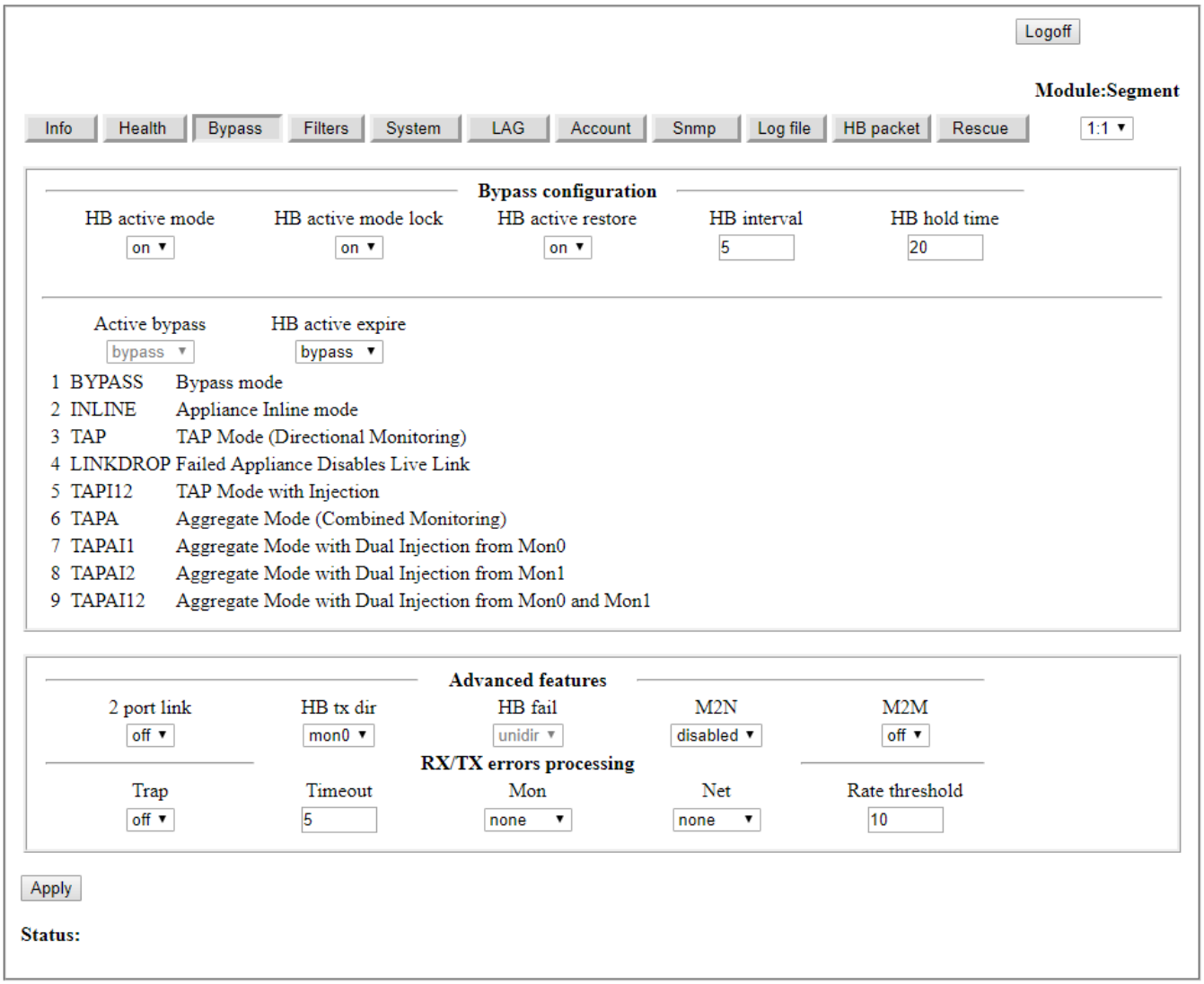
7.5 Health Page



7.5.1 Health status

The Health page displays the status of the Fans and the measured / peak temperature on different area within the M40GBP.
In case of a fan failure or over temperature event the M40GBP will report the error via log/display/SNMP trap.

7.6 Bypass page



7.6.1 Bypass configuration area description

7.6.1.1 Heartbeat active mode select box

When heartbeat active mode is ON the M40GBP send heartbeat packets on its monitor ports. If the M40GBP does not detect the heartbeat packet received from the monitor ports the M40GBP will switch to **Active Bypass** or **TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop** mode according to the predefined settings of the HB active expire select box.

When heartbeat active mode is set to OFF the M40GBP stops sending the heartbeats and the Active Bypass circuitry can be set manually via the management port to one of the following modes **Normal (Inline), Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop**.

7.6.1.2 Heartbeat active mode lock select box

When HB active mode lock is ON the state of heartbeat active mode preserve after reboot or after power on events. When HB active mode lock is OFF the state of heartbeat active mode is automatically set to ON after reboot or after power on.

7.6.1.3 Heartbeat active restore select box

When the HB active mode is ON the M40GBP will restore to **Inline (Normal)** state when the heartbeat packets will be received from the Monitor port.
When HB active mode is OFF the M40GBP preserves its state and no heartbeat packets are generated.
The following actions should be taken to restore the normal operation:

- Restore external environment to normal work.
- Set the active Bypass select box to inline
- Set the HB active mode to on

7.6.1.4 Active bypass select box

When heartbeat active mode is set to OFF the M40GBP stops sending the heartbeats and the Active Bypass circuitry can be controlled manually by the Active bypass select box to one of the following modes **Normal (Inline), Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop** mode.

7.6.1.5 HB active expire select box

When heartbeat active mode is ON the M40GBP send heartbeat packets on its monitor ports. If the M40GBP does not detect the heartbeat packet received from the monitor ports the M40GBP will switch to **Active Bypass** or **TAP, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop** mode according to the predefined settings of the HB active expire select box.

7.6.1.6 Heartbeat interval textbox

The M40GBP generates heartbeat packet to monitor PORT0 every “hb_interval” msec. (default - 5, min - 3, max - 10000). Heartbeat interval should be at least 3 times less than heartbeat hold time.

7.6.1.7 Heartbeat hold time textbox

The M40GBP monitor the received packets on monitor port1, if heartbeat packets do not arrive within “hb_holdtime” msec, the M40GBP will set the Active Bypass to Bypass/Tap/Linkdrop mode, depend on active switch expire state .
To secure reliable detection of Application failure, the " hb_holdtime " value should be at least 3 times the “hb_interval” parameter value. (default - 20, min - 10, max - 50000)
The " hb_holdtime " value is preserved after reset and power off events.

7.6.2 Advanced features configuration area

7.6.2.1 2 port link

The M40GBP supports two ports link. When enabled (on), if one of the network ports link fails it drop the link on the other network port. Two ports link is disabled (off) by default.
unit.

7.6.2.2 Hb tx dir

Set/Get the heartbeats transmit port. The heartbeats can be transmitted for port mon0, port mon1 or form both of them (bidir)

7.6.2.3 HB fail

Set /get the HB fail criteria.

While the HB tx dir is set to bidirectional (HB packets are transmitted from both ports (mon0 and mon1) the HB fail criteria can be set to:

Bidirectional: The M40GBP will change its state if both monitor ports do not receive the heartbeat packets. The M40GBP will restore to its default state if at least one of the monitor ports receives the heartbeat packets.

Unidirectional: The M40GBP will change its state if one of the monitor ports do not receive heartbeat packet. The M40GBP will restore to its default state when both monitor ports receives the heartbeat packets.

7.6.2.4 M2N

M2N (monitor port to network port link fail) mode support link drop on network port if correspondent monitor port link gone. This Mode can be set independent for each monitor port.

7.6.2.5 Speed

The 10G Bypass modules (M10GMS2BP & M10GSS2BP) support dual rate 10G/1G link speed.
The 10G bypass segments can configured to force the link speed to 1G , 10G or auto.
When it is set to Auto, the 10 Bypass segments autodetect the link speed during the bootup of the M40GBP unit. In case that no cable is connected to the Monitor or to the Network ports, the segment speed will be set to the last known speed.

7.6.3 RX/TX errors processing

The IBS can place itself into Bypass or Linkdrop in case it detects RX/TX errors on the Monitor ports or on the Network ports.

7.6.3.1 Trap

ON/OFF - turn on or off the Trap on case of error detection.

7.6.3.2 Timeout

Set the timeout for sending the RX/TX traps

7.6.3.3 Mon

Change the to Bypass mode to (none/bypass/linkdrop) when number of errors per second on MONx ports exceeds threshold

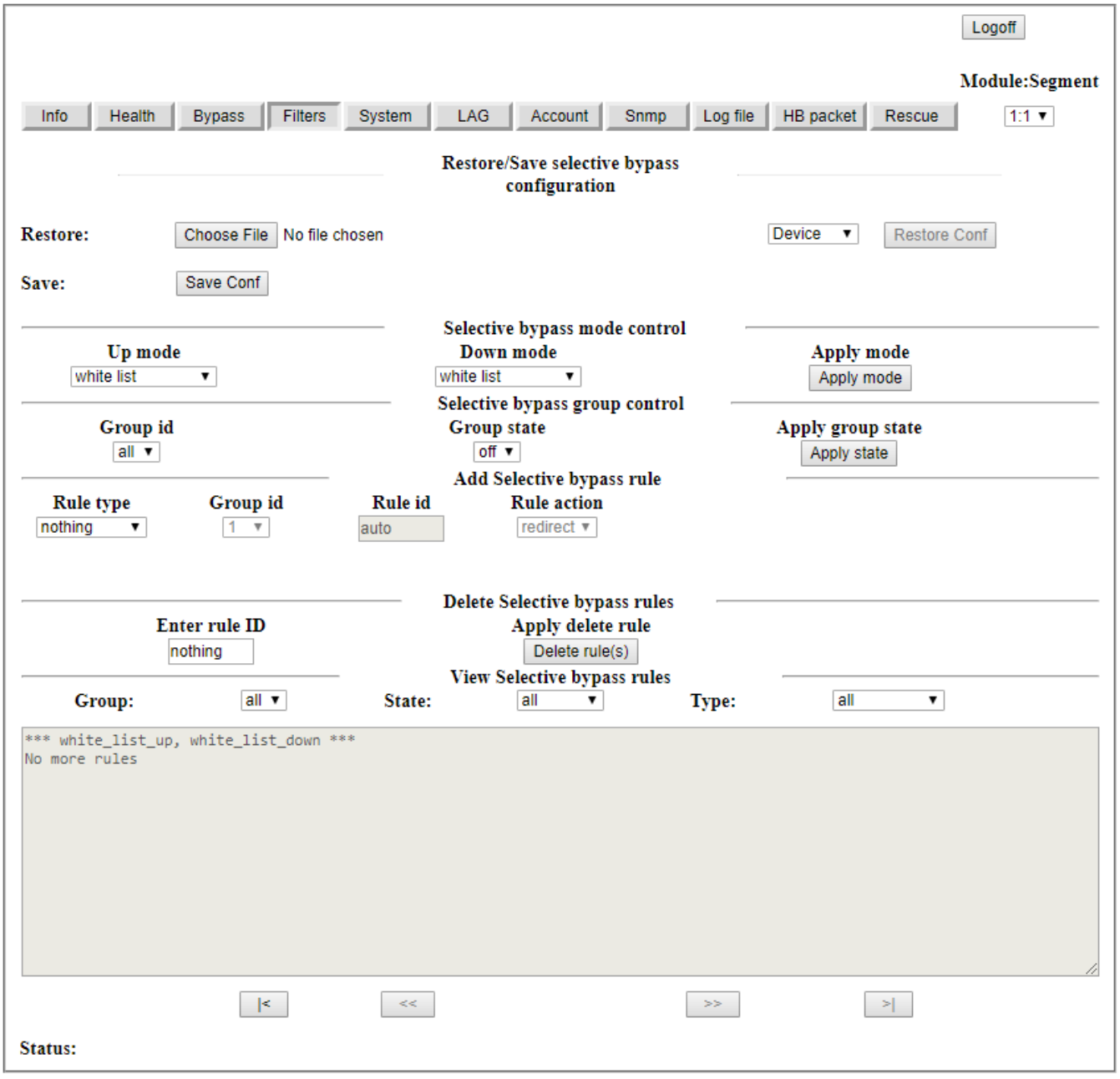
7.6.3.4 Net

Chang the Bypass mode to (none/linkdrop) when number of errors per second on NETx ports exceeds threshold

7.6.3.5 Rate threshold

RX/TX threshold : >0 (default - 10) err/sec

7.7 Filters



7.7.1.1 Restore/save configuration

The M40GBP supports option to restore/save the selective bypass configuration of the chassis of specific module.

7.7.1.2 Selective bypass mode control

Set the selective bypass up/down mode white/black list.

7.7.1.3 Selective bypass grupe control

The M40GBP support up to 16 groups of selective bypass filters.

7.7.1.4 Add selective bypass rule

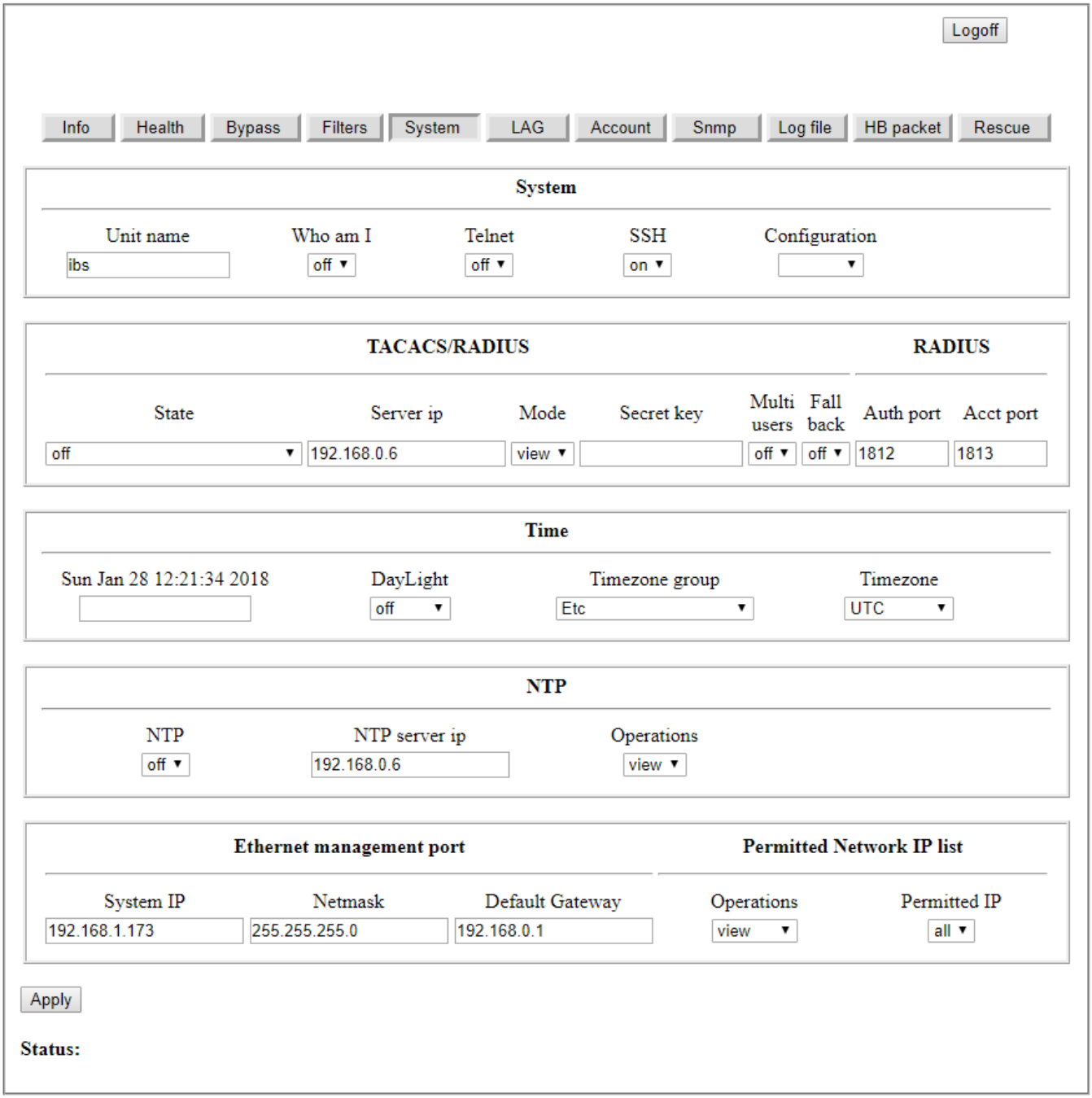
Add selective bypass, filter by :
mpls_lable
vlan_up|vlan_down
vlan_id
ip_up|ip_down
src_ip
dst_ip
src_port
dst_port
mac_up mac_down
proto_up
proto_down

7.7.1.5 Delet selective bypass rule

Delete selective bypass by filter id.

7.7.1.6 View selective bypass rules

7.8 System page



7.8.1 System configuration area

7.8.1.1 Unit name

The M40GBP supports individual name for each M40GBP unit on the network. The User can set the M40GBP unit name (default unit name: M40GBP). Unit name can be up to 25 symbols

7.8.1.2 Who am I

Blink the S.OK LED on currently controlled M40GBP unit in order to identify the relevant unit.

7.8.1.3 Telnet

The M40GBP supports Telnet protocol. The User can Enable/Disable the Telnet support (By default the Telnet support is: off).

7.8.1.4 Configuration

The M40GBP support multi configurations save and restore. Use the scroll down menu to save new configuration or to restore an existing configuration/
The M40GBP saves these different configurations on internal flash memory(~1 MB).

7.8.2 TACACS+ / RADIUS configuration area

The M40GBP support TACACS+ and RADIUS for remote access (WEB access, SNMP access, SSH access, Telnet access).

7.8.2.1 TACACS+ /RADIUS state

Set the TACACS+ / RADIUS state:

- default: off
- Tacacs on, clear text, snmp on
- Tacacs on, encrypted, snmp on
- Radius on, snmp on
- Tacacs on, encrypted, snmp off
- Tacacs on, encrypted, snmp off
- Radius on, snmp off

7.8.2.2 TACACS+ /RADIUS Server Ip

Set the TACACSS+ server IP address (default IP : 192.168.0.6)

7.8.2.3 TACACS+ mode

TACACS+ mode allow to view, add and remove additional TACACS+ server (up to 10 TACACS+ servers) and to set the main TACACS server.

7.8.2.4 TACACS+ / RADIUS secret key

Set the TACACS+ secret key (default: default_tac_key)

7.8.2.5 TACACS+ /RADIUS multi users

Multi users control allows enable/disable TACACS multi users mode.
When TACACS multi users flag is set device will not check the user account, it will rely on TACACS server.
When TACACS multi users flag is reset user can login if the M40GBP and TACACS server have this account.

7.8.3 Time configuration area

7.8.3.1 Time state

Time format: mm DD HH MM YYYY
Where:

- mm – month
- DD – day
- HH – hour
- MM – minute
- YYYY – year

7.8.3.2 Daylight state

Set the Daylight saving time mode ON/Off (default: OFF)

7.8.3.3 Timezone grope state

Set the time zone group. Select from the dropdown menu (default: etc).

7.8.3.4 Timezone state

Set the time zone. Select from dropdown menu (default: UTS)

7.8.4 NTP configuration area

The M40GBP clock can be synchronized from NTP servers on the network.
The M40GBP support Multi NTP servers

7.8.4.1 NTP

Set the NTP mode ON/OFF (default: OFF)

7.8.4.2 NTP Server Ip

Set the NTP server IP address (default IP: 192.168.0.6)

7.8.4.3 Operation

Enable to add/view/delete NTP server

7.8.5 Ethernet management port area

7.8.5.1 System IP address

The System IP address is the Ethernet management port IP address.
The New IP address will take effect only after performing device reboot
Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new IP address

7.8.5.2 Netmask

The System netmask IP address is Ethernet management port net mask address.
The new Netmask IP address will take affect only after device reboot.
Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new NETMASK IP address

7.8.5.3 Default gateway

The default gateway IP address is the Ethernet management port default gateway address .
The new default gateway IP address will take affect only after device reboot.
Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new gateway IP address

7.8.5.4 Permitted Network IP list

There are two fields which controls the permitted IP address:

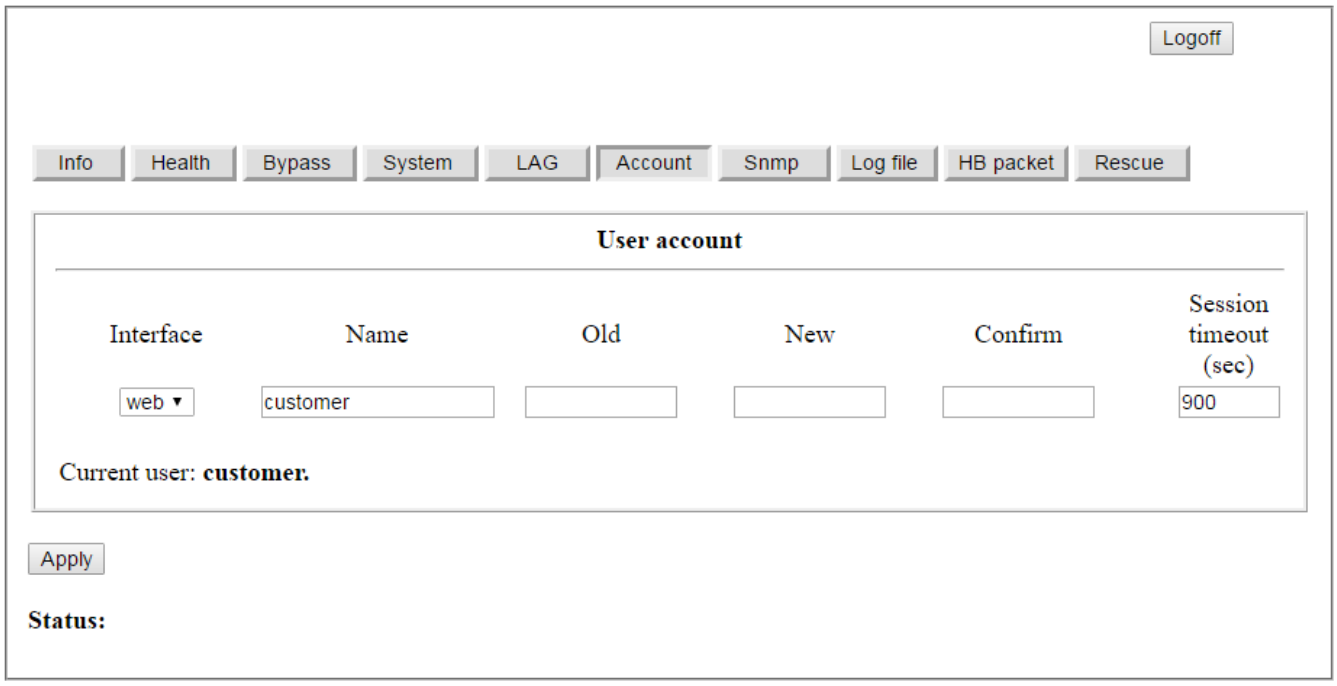
1) Operations
2) Permitted IP

The operation filed control the operation to be performed (view, set, remove)
When view" operation is selected, the "Permitted IP" window will displayed the current permitted IP ranges.
When "set" operation is selected, the "Permitted IP" will enable the user to enter new permitted IP range in the following format:
nnn.nnn.nnn.nnn/mask
For examples:
192.168.2.0/24
10.0.0.0/8
When "remove" operation is selected, the "Permitted IP" window will display the current permitted IP range that can be removed. The user can select one of the IP ranges to be removed or to select "all" ranges.

7.9 LAG

The M40GBP supports Link Aggregate Groups (LAG)
The LAG feature supported by the capabilies explained on section LAG configuration

7.10 Account page



7.10.1 Interface

Select the M40GBP interface for which you would like to change the user account (CLI, WEB, SNMP)

7.10.2 User/community name

Set the User name for the selected interface on the Interface dropdown menu

7.10.3 Password

The "old password" , "new password" and the "confirm new password" are required in order to set the Password for the selected interface on the Interface dropdown menu

7.10.4 Session timeout

The web_exp_time command sets the time that the WEB session can be passive (does not send requests to the M40GBP) before the session will be terminated by the M40GBP (default 900 sec).
In case that the WEB session was terminated the Login screen will be appear on the WEB browser.
If the main WEB interface window will be closed in any way other than by pressing on “Logoff” button, the WEB interface will be unavailable for the time defined by the web_expired_time (default 900 sec).
The first user that will be logged in to the WEB interface will get all the rights (Control /monitor) of the Web interface application, the next users will not able to control device, they will be able only to monitor the M40GBP parameters.
When first user will be logged off from the WEB interface, the next user will receive his rights and will be able to (Control /monitor) the WEB interface.

7.11 SNMP page

7.11.1 SNMP Entry

The M40GBP supports up to 11 different SNMP entries (Entry = user name/community).
Each entry support up to 8 different SNMP servers.
Each entry support different level of access (read only, read/write, trap only, read Only with Trap, read/write with Trap) and different SNMP version 1, 2c, and 3 (SHA and AES) and SNMP discovery.

7.11.2 SNMP server IP address

Using the IP operation select box and the current IP it is possible to view/add/delete the SNMP server IP
Each SNMP entry support up to 8 different SNMP servers

7.11.3 SNMP version

The M40GBP support SNMP versions 1, 2c and 3.
SNMP version select box destined to change the SNMP version.

7.11.4 Access

Each entry support different level of access (read only, read/write, trap only, read Only with Trap, read/write with Trap)

7.11.5 Name

Define the entry name = SNMP user \community name

7.11.6 Status

Activate/deactivate the SNMP entry

7.11.7 SNMP control port

Message (min - 1, max - 49151, default - 161)
Trap port (min - 1, max - 49151, default - 162).

7.11.8 SNMP trap account

7.11.9 SNMP trap account allow to add/remove/view additional destinations for SNMP traps.SNMP trap control

SNMP trap control destined to enable/disable SNMP trap groups. SNMP traps are disabled by default. It can be enabled by checking the check box for the relevant trap group.

a) Appl fail enable/disable following traps:
- M40GBPTrapApplFail
- M40GBP TrapApplRecover.

b) Bypass enable/disable following traps:
- M40GBP TrapActBypassOn
- M40GBP TrapActInlineOn
- M40GBP TrapPasBypassOn
- M40GBP TrapPasBypassOff
- M40GBP TrapTapOn
- M40GBP TrapTapi12On
- M40GBP TrapTapaOn
- M40GBP TrapTapai1On
- M40GBP TrapTapai2On
- M40GBP TrapTapai12On

c) Mon link enable/disable following traps:
- M40GBP TrapMon0LinkDown
- M40GBP TrapMon0LinkUp
- M40GBP TrapMon1LinkDown
- M40GBP TrapMon1LinkUp.

d) Net link enable/disable following traps:
- M40GBP TrapNet0LinkDown
- M40GBP TrapNet0LinkUp
- M40GBP TrapNet1LinkDown
- M40GBP TrapNet1LinkUp.

e) Terminal enable/disable following traps:

- M40GBP TrapTermDisc
- M40GBP TrapTermCon.

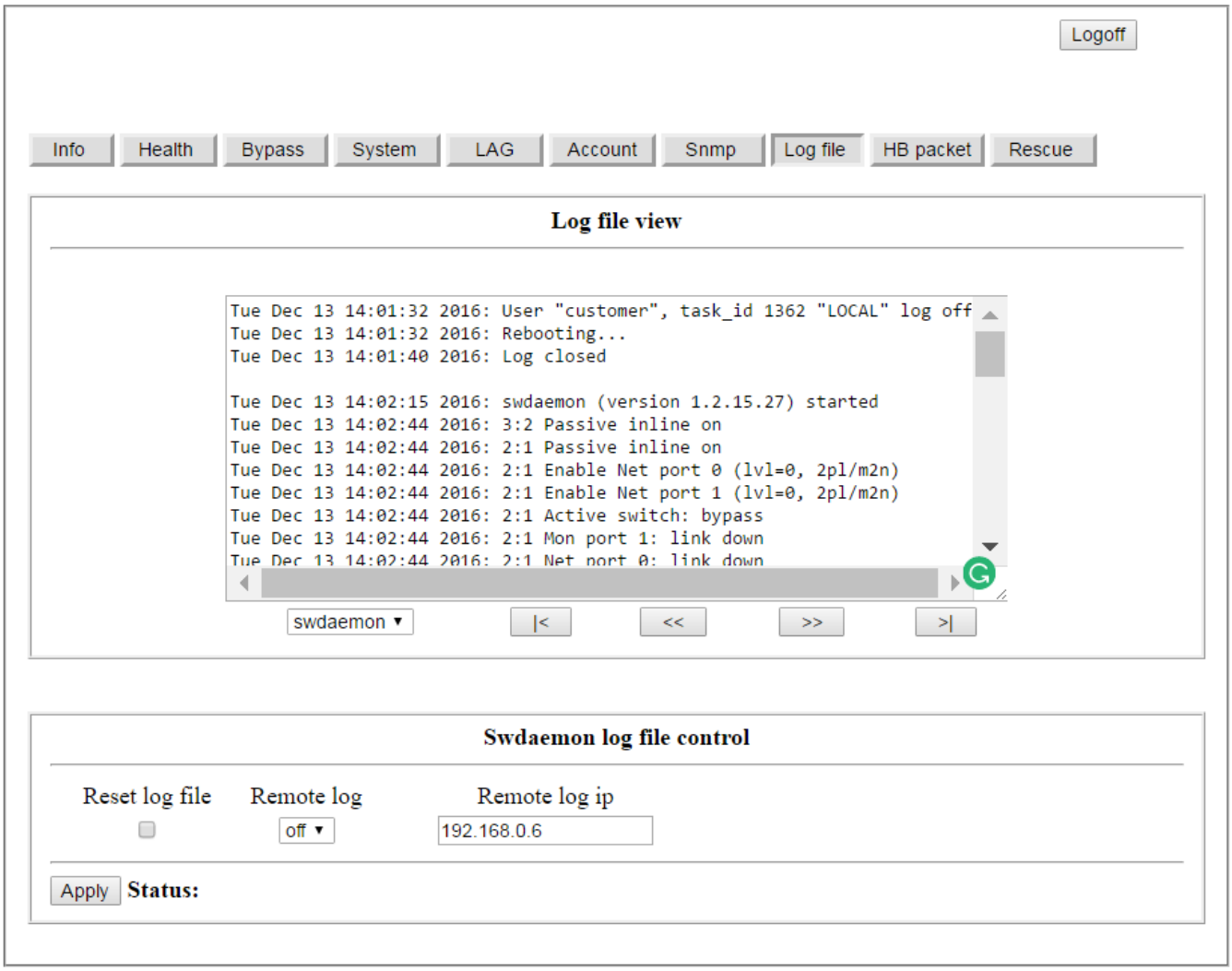
f) Error enable/disable following traps:

- M40GBP TrapErr
- M40GBPTrapPower1OK
- M40GBPTrapPower1OK
- M40GBPTrapRxTxError

g) Update

- M40GBP TrapUpdate
- M40GBP TrapUpdateReboot

7.12 Log file page



7.12.1 Log file control area

The default log file is stored in the internal FLASH memory. The log is saved also after reboot or power off. The log file is saved in 2 x 4096KB cyclic blocks. When two blocks are full, the older block is cleared and the new information is written in the location of the old block.

7.12.2 Remote log file control area

The M40GBP is capable to send the log messages to remote log server (factory default = disable)
The Remote log should be enabled on remote server to receive messages from device.

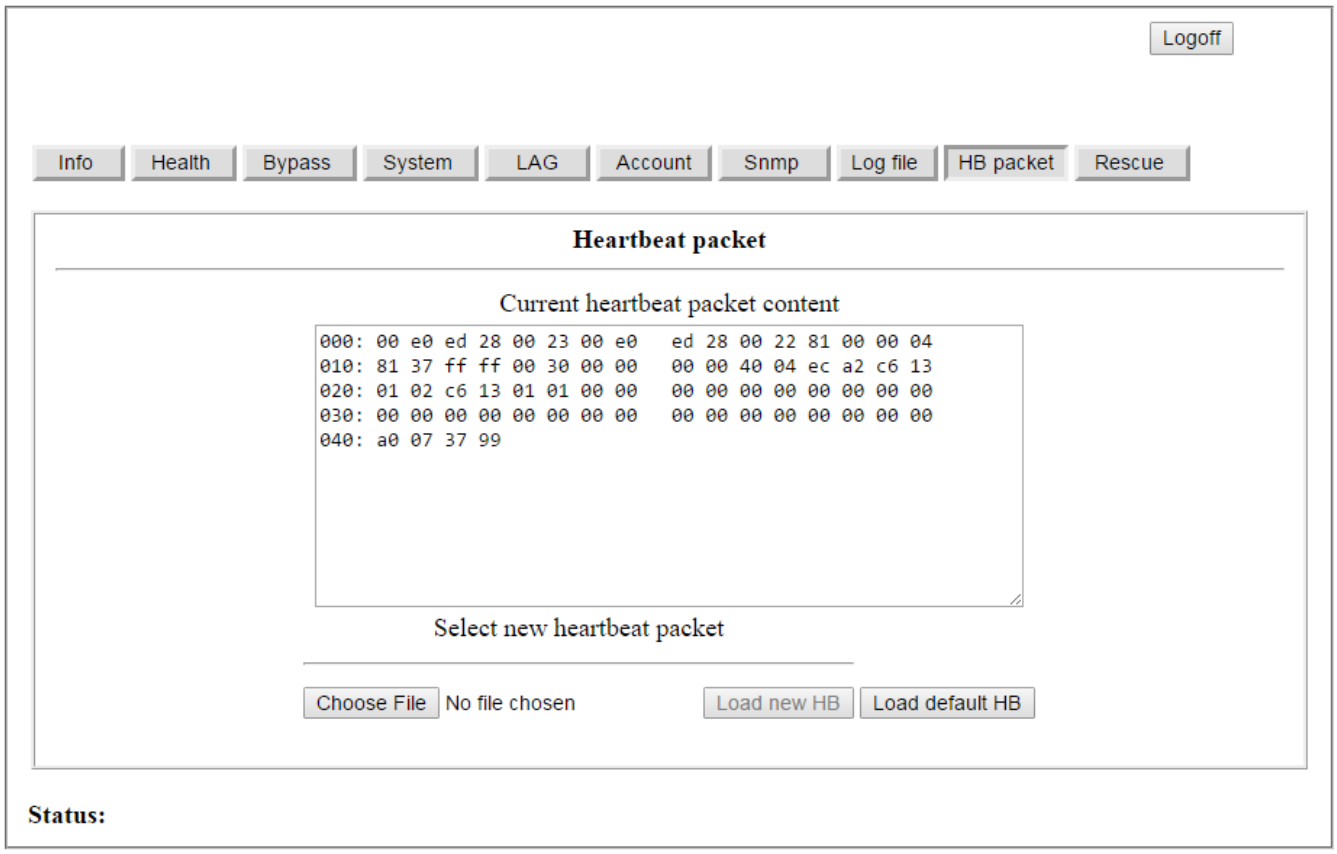
7.12.2.1 Remote log

Set the remote log ON/OFF (default: OFF)

7.12.2.2 Remote log Server Ip

Set the Remote log server IP address (default IP: 192.168.0.6)

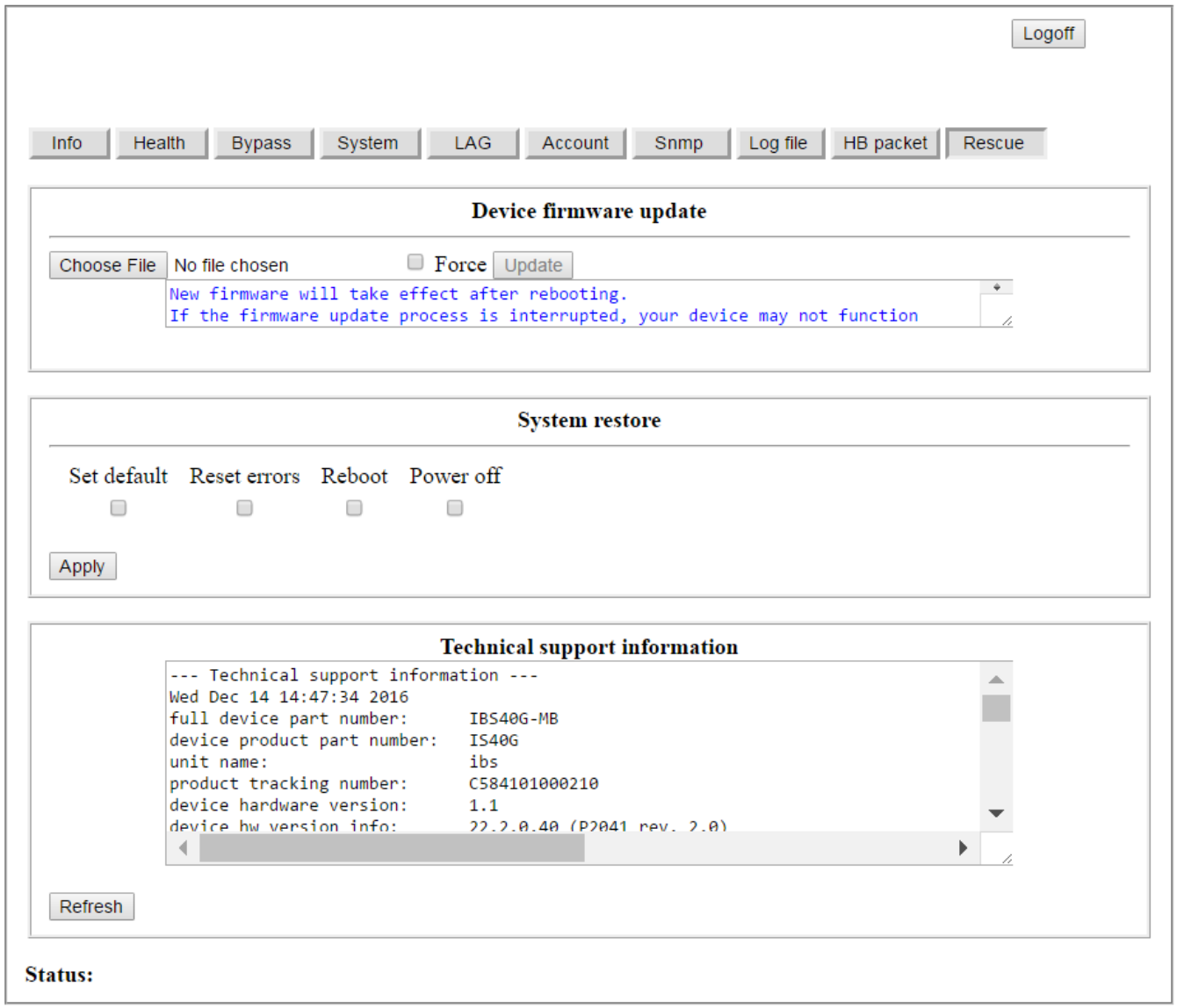
7.13 HB Packet page



This page enables the user to change or to load new Heartbeat packet content.

,

7.14 Rescue page



7.14.1 Device firmware update area

The Update command updates the M40GBP firmware's:
Follow the FW update user guide to load the new Firmware

NOTE: If the firmware update process is interrupted, your M40GBP may not function properly. We recommend the process be done in an environment with a steady power supply (preferably with UPS).

7.14.2 System restore are

7.14.2.1 Set default parameters

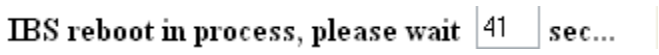
Restore the factory default settings for all parameters including system user name and password.

7.14.2.2 Reset errors

Reset the M40GBP errors.
The M40GBP displays on the LCD the first error only, after resetting the error the M40GBP will display the next error if exist.

7.14.2.3 Reboot

Checking Reboot check box force the M40GBP to reboot



The following screen appears during the M40GBP reboot progress, when the M40GBP will load again the main screen will appear.

7.14.2.4 Power off (only for hardware 0.3.0.11 and up)

Module power will be off after select check box "Power off" and click "Apply" button.

7.14.3 Technical support area

The command gathers all the necessary information needed for the Technical Support team in order to help resolving technical problems.

8 Appendixes

Key features

- Self generating heartbeat pulses – No driver or management port is required to generate pulses.
- Sets to Bypass when it detects in-line system failure.
- Sets to Bypass when it detects in-line system link failure
- Sets to Bypass when it detects in-line software application system hang.
- Sets to Bypass on Power failure.
- Sets to Normal when it detects in-line system recovery.
- Double Safe Bypass architecture with two routing circuitries.
- Centralized managements.
- Two on Board Watch Dog Timer (WDT) Controllers.
- Software programmable time out interval.
- Software Programmable WDT Enable / Disable.
- Independent Bypass / Normal / Tap /Linkdrop operation in every module.
- Supports up to three 40G Bypass segment in a 1U chassis.
- Supports up to six dual rate 10G/1G Bypass segment in a 1U chassis.
- Supports TAP mode of operation.
- Simple CLI configuration management via serial port.
- Telnet management interface via network management port.
- SSH management interface via network management port.
- Supports SNMP version 1, 2c, 3 (SHA, AES)
- Supports remote log
- Supports TACACS+
- Support RADIUS
- Supports NTP
- Supports time zone
- Supports multi configuration backup
- Support Two ports link feature - if one of the network ports link fails it will drop the link on the other network port as well.
- Two redundant power supplies
- Optional -48V DC power supplies

M40GMSBP

- Supports Short Range Fiber 40 Gigabit Ethernet (40GBase-SR4 50um).

M40GSSBP

- Supports Long Reach Fiber 40 Gigabit Ethernet (40GBase-LR4).

M10GMS2BP

- Supports Short Range Fiber 10 Gigabit Ethernet (10GBase-SR).
- Supports Short Range Fiber Gigabit Ethernet (1000Base-SX).

M10GSS2BP

- Supports Long Reach Fiber 10 Gigabit Ethernet (10GBase-LR).
- Supports Long Range Fiber Gigabit Ethernet (1000Base-LX).

8.1 Bypass Specifications

WDT Interval (Software Programmable):	Routing Transmit heart beat packet every 3mS – 10Sec. Default 5mS Verification packets received every 10mS – 50Sec. Default 20mSec Double Bypass Transmit heart beat packet every 300mS – 60Sec. Default 7Sec Verification packets received every 1S – 253Sec. Default 20Sec

8.2 Production Default configuration

Mode at Power up:	Bypass
Heartbeat:	Activated
Bypass Switch is ready and in-line device responds to heartbeat:	Change to Normal
In-line device responds to heartbeat:	Normal
In-line device does not respond heartbeat:	Bypass
Mode at Power 0ff:	Bypass
Heartbeat Packet:	Internetwork Packet Exchange

9 Technical Specifications:

9.1 M40GBP1U

9.1.1 M40GBP1U: Bypass Switch 1U Host System Technical Specifications

Dockings:	Front holders
Voltage Input:	AC: 90-240 VAC Auto-Select -48 (-75 - -36) VDC
Size:	438mm x 586 mm x 44 mm (17.24” x 23.07” x 1.73”) Wide x Depth x Height
Operating Humidity:	0%–90%, non-condensing
Operating Temperature:	0°C – 40°C (32°F - 104°F)
Storage Temperature:	-20°C–65°C (-4°F–149°F)
Fans	4 hot swap Fans 4 wires connections on each fan (12V,GND,TACH and PWM) Specifications (maximum operation condition) of one Fan SPL- 61dB(A) Current – 0.92A Air flow - 28.6 CFM
EMC Certifications:	Class B FCC / CE / VCCI
MTBF*:	> 150,000 hours

9.1.2 M40GBP1U: Bypass Switch 1U Host System LEDs & Switches Specifications

LEDs:	----------FRONT---------- Two Power LEDs: PS1, PS2 3. PS1: Green LED will light when power is on and off if there is a failer in power supply module or when extracting the power supply module from the system. 4. PS2: Green LED will light when power is on and off if there is a failer in power supply module or when extracting the power supply module from the system. System Status LEDs: 3 LEDs 4. Sys OK: System Normal Operation – Light Green. Who I'm: in rack identification – Blinking Green. 5. Sys UP: System Init during power up and during shutdown – Light Yellow. 6. ALM: System Alarm – Light Red. Module Power LEDs: 3. M1: module1 power on – Light Green.M2: module2 power on – Light Green. 4. M3: module3 power on – Light Green. ----------BACK---------- One bi-color LED indication that integrated on each power supply module: Power Switch On – Green color. Standby(AC/DC In,Only +5VSB output) - Blinking Green color. Power Fail – Red color. Internal Fan Fail – Blinking Red.
Switches	Push button to power the system (PWR). From ON to OFF – Press and hold this push button during 4 second will perform firmware shutdown press and hold this push button during 8second will perform power shutdown. From OFF to ON – simple push will turn system on. Reset (RST): Small micro-switch stand behind hidden hole : Press and hold for more than 1 sec will perform restart to the system.

Connectors:	Management Ports: RJ-45 Ethernet (MGNT ETH) RJ-45 serial port (RS-232) USB port (RS-232)

9.2 M40GMSBP(50um)

9.2.1 Fiber Gigabit Ethernet Technical Specifications - (40GBase-SR4) Adapters:

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, 40GBase-SR4 (850nM)
Data Transfer Rate:	40G per port
Cables and Operating distance:	Multimode fiber:50um *50m maximum on OM3 MMF *75m maximum on OM4 MMF Theoretical Distance – Defined as half a distance
Size:	102.2mm x161.9 mm x 40.5 mm (4.02” x 6.37” x 2”) Wide x Depth x Height
Operating Humidity:	0%–90%, non-condensing
Operating Temperature:	0°C – 40°C (32°F - 104°F)
Storage Temperature:	-20°C–65°C (-4°F–149°F)
EMC Certifications:	Class B / FCC / CE / VCCI
Safety:	UL
MTBF*:	> 150,000 hours

9.2.2 M40GMSBPand : LED and Connector Specifications

LEDs:	Green LED per port (Network / Monitor) Activity : LED will blink. Link : LED will turn on. Two LED: Inline Mode – Green LED. Non Inline Mode :Bypass, TAP, Disconnect – Yellow (Orange) LED. HB Status LED Blinking Green LED – HB is active. LED is off – HB not active.
Connectors:	Network: 2 MPO Monitor: 2 QSFP+

9.3 M40GSSBP

9.3.1 Fiber 40Gigabit Ethernet Technical Specifications - (40GBase-LR4) Adapters:

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, 40GBase-LR4 (1310nM)
Data Transfer Rate:	40Gbit/s per port
Network ports Cables and Operating distance:	Single mode fiber: 5000m maximum at 9 um ** **Theoretical Distance – Defined as half a distance
Insertion Loss (Passive: Normal Mode)	Typical: 1.2 dB Maximum: 1.6dB
Insertion Loss (Passive: Bypass Mode)	Typical: 1.2 dB Maximum: 1.6dB
Voltage:	12V +/-5%, 5VSB+/-5%, 5V +/-5%
Size:	102.2mm x161.9 mm x 40.5 mm (4.02” x 6.37” x 2”) Wide x Depth x Height
Operating Humidity:	0%–90%, non-condensing
Operating Temperature:	0°C – 40°C (32°F - 104°F)
Storage Temperature:	-20°C–65°C (-4°F–149°F)
EMC Certifications:	Class B FCC / CE / VCCI /
Safety:	UL
MTBF*:	> 150,000 hours

9.3.2 M40GSSBP and : LED and Connector Specifications

LEDs:	Green LED per port (Network / Monitor) Activity : LED will blink. Link : LED will turn on. Two LED: Inline Mode – Green LED. Non Inline Mode :Bypass, TAP, Disconnect – Yellow (Orange) LED. HB Status LED Blinking Green LED – HB is active. LED is off – HB not active.
Connectors:	Network: 2 LC Monitor: 2 QSFP+

9.4 M10GMS2BP

9.4.1 Dual rate Fiber 10G/1G Ethernet Technical Specifications - (10GBase-SR / 1000Base-SX) Adapters:

IEEE Standard / Network topology:	1000Base-SX, 10GBase-SR (850nM)
Data Transfer Rate:	20Gbit/s in full duplex mode per port
Cables and Operating distance:	Multimode fiber:62.5um 16.5m maximum at 62.5 um ** Theoretical Distance – Defined as half a distance as stated by the IEEE 802.3 standard
Insertion Loss (Passive: Normal Mode)	Typical: 0.8 dB Maximum: 1.9 dB
Insertion Loss (Passive: Bypass Mode)	Typical: 0.8 dB Maximum: 1.9 dB
Voltage:	12V +/-5%, 5VSB+/-5%, 5V +/-5%
Size:	102.2mm x161.9 mm x 40.5 mm (4.02” x 6.37” x 2”) Wide x Depth x Height
Operating Humidity:	0%–90%, non-condensing
Operating Temperature:	0°C – 40°C (32°F - 104°F)
Storage Temperature:	-20°C–65°C (-4°F–149°F)
EMC Certifications:	Class B / FCC / CE / VCCI
Safety:	UL
MTBF*:	> 150,000 hours

9.5 M10GSS2BP

9.5.1 Dual rate Fiber 10G/1G Ethernet Technical Specifications - (10G Base-LR / 100BaseLX) Adapters:

IEEE Standard / Network topology:	1000Base-LX, 10GBase-LR (1310nM)
Data Transfer Rate:	20Gbit/s in full duplex mode per port
Network ports Cables and Operating distance:	Single mode fiber: 5000m maximum at 9 um **
Insertion Loss (Passive: Normal Mode)	Typical: 1.2 dB Maximum: 1.6dB
Insertion Loss (Passive: Bypass Mode)	Typical: 1.2 dB Maximum: 1.6dB
Voltage:	12V +/-5%, 5VSB+/-5%, 5V +/-5%
Size:	102.2mm x161.9 mm x 40.5 mm (4.02” x 6.37” x 2”) Wide x Depth x Height
Operating Humidity:	0%–90%, non-condensing
Operating Temperature:	0°C – 40°C (32°F - 104°F)
Storage Temperature:	-20°C–65°C (-4°F–149°F)
EMC Certifications:	Class B FCC / CE / VCCI /
Safety:	UL
MTBF*:	> 150,000 hours

9.5.2 M10GSS2BP/SRD: LED and Connector Specifications

LEDs:	Green LED per port (Network / Monitor) Activity : LED will blink. Link : LED will turn on. Bi-color LED: Inline Mode – Green color Non Inline Mode :Bypass, TAP, Disconnect – Yellow (Orange) color. HB Status LED Blinking Green LED – HB is active. LED is off – HB not active.
Connectors :	Network: 4 LC Duplex Monitor: 4 SFP+

10 Safety Precautions

CAUTION:

- **The battery requires special handling at end-of-life. The battery can explode or cause burns if disassembled, charged, or exposed to water, fire or high temperature. After replacing the battery, properly dispose of used battery according to instructions.**
- **There is a risk of explosion if the battery is replaced by an incorrect type. Ensure to replace the battery with the same type.**
- **To avoid the possibility of electric shock, all power cords must be disconnected from the switch before starting this procedure.**

CAUTION:

The fiber optic ports contain a Class 1 laser device. When the ports are disconnected, always cover them with the provided plug. If an abnormal fault occurs, skin or eye damage may result if in close proximity to the exposed ports.

- **Remove and save the fiber optic connector cover.**
- **Insert a fiber optic cable into the ports on the network adapter bracket as shown.**

10.1.1 Safety considerations for the M40GBP rack mounting:

A. Verify that the maximum operating ambient temperature inside a rack assembly does not exceed 50°C.

B. Verify that a sufficient clear space is provided around the M40GBP unit to allow sufficient amount of air flow for safe operation of the product. Keep 25 mm clearance on the sides of the unit.

C. Serious injury could result due to improper handling and uneven mechanical loading. Use proper techniques to mount and secure to the rack to avoid uneven mechanical loading.

D. An external circuit breaker rated max. 20A should be provided in the building installation (end user's responsibility).

E. Verify that the M40GBP unit is reliably connected to protective grounding. Connect the product only to a grounded type socket-outlet in the building installation or in a rack. Use the grounding stud on the rear panel to connect the product to the rack.

10.2 TFTP server installation and configuration.

10.2.1 Windows TFTP server installation and configuration

Use any TFTP server utility to create TFTP server (for example: tftpd32 which is a free utility):

1) Create \tftp directory
2) Create \tftp\tftpboot directory. (The working directory for the TFTP software should be the \tftp)

10.2.2 Linux TFTP server installation and configuration

1) Connect the host computer to Internet
2) Install tftp-server (yum –y install tftp-server)
3) Disconnect the host computer from the Internet
4) Turn off firewall. Run the following command: iptables -F or type "setup"
5) Create the tftboot directory: `mkdir /tftpboot`
6) For FC4 edit file /etc/sysconfig/selinux: SELINUX=PERMISSIVE
7) Disable iptable and ip6table in services
8) Edit /etc/xinetd.d/tftp to enable tftp:

```
{
    disable = no
    socket_type = dgram
    protocol = udp
    wait = yes
    user = root
    server = /usr/sbin/in.tftpd
    server_args = /tftpboot
}
```

9) Restart the tftp servers on your host: `/etc/init.d/xinetd restart`

10.3 NET-SNMP Copyright.

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2006, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
  brand or product names may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

10.4 TACACS+ copyright.

Copyright 2000,2001 by Roman Volkov

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The names of its contributors may not be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS

IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Next LICENSE text MUST be here:

The MD5 Message-Digest Algorithm was derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm with next copyright:

> Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
>
> License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.
>
> License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.
>
> RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.
>
> These notices must be retained in any copies of any part of this documentation and/or software.

1.1 RADIUS copyright.

documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc.
Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.

Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

[C] The Regents of the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995 All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided

that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.
