# **EdgeSafe**<sup>TM</sup> 10G Bypass Modular Network TAP

User Guide By Garland Technology

M10GMSBPv2 / M10GSSBPv2 / M10GESBPv2 / M10G1ACv2 / M10G1DCv2



For questions, please contact Garland Technology Support at: 8AM-9PM (CST) Monday - Friday (Except for observed US Holidays) Tel: 716.242.8500 Online: www.garlandtechnology.com/support

Garland Technology: Modular Bypass System Firmware Rev Level: 0.3.3.2

> Office: 716-242-8500 garlandtechnology.com/support garlandtechnology.com



Revision	Date	Change description
1.0	30-Nov-08	EdgeSafe Bypass TAP guide – Initial version
1.1	28-Dec-08	Added SNMP commands and trap
1.2		Added WEB interface, added additional SNMP commands, change CLI interface
1.3	17-Mar-09	Update keep_hb_act_mode explanation
1.4	24-Mar-09	Added Whoami command Added HTTP firmware update Added Management push button interface
1.5	28-Apr-09	Firmware 0.1.0.5 updates: Updates hb_interval , hb_holdtime and apply_snmp commands explanation
1.6	7-Jun-09	Add Safety Precautions section
1.7	6-Jul-09	Updates for firmware 1.06
1.8	6-Oct-09	Updates for firmware 1.10
1.9	23-Dec-09	Update for new firmware 2.0
2.0	23-Feb-10	Update section 8.1 – web interface
2.1	15-Apr-10	Updates for firmware 2.0.2 Updates for -48v products
2.2	28-Aug-11	Add show/set_rs232_speed command , set_link command
2.3	27-Sep-11	Add support for the different TAP modes
2.4	26-Oct-11	Add support for permitted IP Add support for product part number
2.5	8-Apr-12	Added support for TACACS multi users. Added support for SNMP multi trap destinations.
2.6	5-Aug-12	Added support for M2N mode. Added support for power supply monitoring. Added support for disabling WEB interface. Added support for security update. Added support for remote save/restore configuration. Added support for power off module
2.7	15-Sep-13	Update Spec and order information PN for IBSP – HW with power supply trap capabilities
2.8	17-Oct-13	Added support for Reporting of RX/TX errors in the Web interface / CLI. Added support for disconnect mode at power off



Revision	Date	Change description
2.9	24-Nov-13	Update for FW 0.3.0.5 Added commands (CLI, WEB SNMP): <pre>show_rx_tx_err_mode Set_rx_tx_err_mode Added to WEB, SNMP interface FAN status Added support for reporting good link is admin down due to 2PL/M2M Added support for reporting manual mode device change status events in log file Adding Copper version</pre>
3.0		Adding support for advanced_link and SSH state Update <b>show_dev_state</b> and <b>show_dev_alert</b> Added copper module IBSG-T
3.1		FW 3.1.1 - Add support for TACACS multi users, TACACS fallback. Add support for Internal vlan change Add support for M2M
3.2		FW 3.1.5 - Add support for Multi SNMP servers Add support for multi NTP servers
3.4		FW 3.1.7 - Add support for TACACS+ authorization read-only and read-write user Add support for TACACS+ for serial port Add support for Control and Info sessions for CLI and WEB users Add support for shell prompt show the user@hostname and will include in additional the permission level Add support for changing ssl certificate for the web UI
3.5		FW 3.2.0 - Add support for Selective Bypass Filters (VLAN/MPLS/IP) Added support for management port vlan Add support for cli tab to complete the command

Notes: Several new features supported only with new HW devices (EdgeSafe hardware version 0.3.0.0 and up).



# **Table of Contents**

1 INTRODUCTION	10
1.1 TARSHOW RELEASE	•••••

#### 10

2 FEATURES	11
2.1 GENERAL	11
2.2 BYPASS MODES	11
2.3 APPLICATION FAILURE (HEARTBEAT)	12
2.4 MONITOR LINK FAILURE	13
2.5 POWER FAILURE	13
2.6 TAPMODE	. 14
2.7 TAPI12 MODE	. 15
2.8 TAPA MODE	. 16
2.9 TAPAI1 MODE	. 17
2.10 TAPAI2 MODE	. 18
2.11 TAPAI12 MODE	. 19
2.12 LINKDROP MODE	. 20
2.13 TWO PORT LINK (2PL)	21
2.14 RESTORE FROM ACTIVE EXPIRE STATE	. 21
2.15 HEARTBEAT ACTIVE MODE	. 21
3 FRONT PANELS	. 22
3.1 IBS FIBER MODULE	. 22
3.2 IBS1U – IBS1U WITH 4 IBS MODULES	24
3.3 IBSSU – IBS STANDALONE UNIT - FRONT PANEL	24
4 REAR PANELS	25
4.1 IBS1U - IBS1U – REAR PANEL	25
4.2 IBSSU – IBS STANDALONE UNIT REAR PANEL	25
5 EdgeSafe Bypass TAP (IBS) INSTALLATION	
5.1 RACK MOUNT THE IBS	26
5.2 CONNECTING POWER TO THE AC IBS UNIT (230V/120V)	26
5.2.1 Verify that the power switch on the IBS unit is OFF.	26
5.2.2 Connect two power cables to the power supplies on to the back of the IBS. The PWR led's on	the
front panel of the IBS will illuminate when switching on the power switch power.	26
5.3 CONNECTING POWER TO THE DC IBS UNIT (-48VDC)	26
5.3.1 Use DC power source -48V DC with circuit breaker 5A	. 26
5.3.2 Verify that the power is OFF on the DC power source	. 26
5.3.3 Verify that the power switch on the IBS unit is OFF	. 26
5.3.4 Connect the DC input wires to the DC input terminal on the IBS as follows:	. 26
I. CONNECT WIRE TO GROUND TERMINAL IBS ( LEFT)	. 26
II. CONNECT 0V RETURN TO "+" TERMINAL IBS ( CENTER)	. 26
III. CONNECT -48V WIRE TO "-" TERMINAL ( RIGHT) IBS	26
IV. TURN ON THE DC POWER SOURCE THE PWR LEDS ON THE FRONT PANEL OF THE IBS WILL	
ILLUMINATE	. 26
5.4 CONNECTING THE RS232 DB9 MANAGEMENT CABLE	. 27
5.5 CONNECTING THE ETHERNET MANAGEMENT PORT	. 27



6 COMMAND LINE INTERFACE (CLI)	28
6.1 MAIN MENU	
6.2 COMMANDS LIST	
6.3 HEARTBEAT ACTIVE MODE. (HB_ACT_MODE)	30
6.4 ACTIVE BYPASS MODE	
6.5 POWER OFF STATE (PWOFF_STATUS)	
Version 3.5 Page 5 of 146	
6.6 HB_INTERVAL (HB_INTERVAL)	32
6.7 HB_HOLDTIME (HB_HOLDTIME)	33
6.8 KEEP HEARTBEAT ACTIVE MODE (KEEP_HB_ACT_MODE)	33
6.9 HEARTBEAT EXPIRATION STATE (HB_EXP_STATE)	
6.10 RESTORE FROM HEARTBEAT EXPIRATION EVENT (EN_ACT_HB_RESTORE)	35
6.11 CHANGE BYPASS STATE ON RX/TX ERROR DETECTION (RX_TX_ERR_MODE)	
6.12 SELECTIVE BYPASS FILTER	37
6.13 ADVANCED LINK MODES	39
6.13.1 Set link (available on the IBSG 1G Copper)	
6.13.1 Two port link	
6.13.2 M2N mode	40
6.13.1 M2M mode	
6.13.1 Advanced link (available on the IBS 1G/10G fiber)	
6.13.2 Set defualt advanced link (available on the IBS 1G/10G fiber).	
6.13.1 show/Set Internal VI AN ID	
41	•••••
6.14 ETHERNET MANAGEMENT PORT IP ADDRESS	
6.15 ETHERNET MANAGEMENT PORT NET MASK ADDRESS	
6.16 ETHERNET MANAGEMENT PORT GATEWAY IP ADDRESS	43
6 17 FTHERNET MANAGEMENT PORT VI AN ID	43
6 18 TIME	44
6 19 SYSTEM LISER (SET LISER)	45
6 20 DISPLAY CURRENT LISER	45
6 21 SYSTEM PASSWORD (SET PSW)	
6 22 LINIT NAME	
$6.22 \text{ WHO } \Delta M \mid (\text{WHO } \Delta M \text{I})$	,
6.24 DISPLAY IRS VERSIONS (SHOW, VER)	
6 25 DISPLAY IBS PARAMETERS (SHOW_VER)	40 17
6 26 DISPLAY IBS STATE (SHOW, DEV, STATE)	۲۴. ۱۸
6 27 DISPLAT DS STATE (SHOW_DEV_STATE)	40 ۱۵
6.28 DISPLAT DEVICE HAPDWARE VERSIONI (SHOW, HW, VER)	/19 /19
6 20 DISPLAT DEVICE TRACKING NUMBER (SHOW DEVICE)	
6.21 DISPLAT DEVICE FAR STATE (SHOW EAN STATUS)	
6.22 DISPLAT DEVICE FAIN STATE (SHOW_FAIN_STATUS)	
6.22 DISPLATING POWER SUPPLIES STATES.	
0.33 DISELAT AFFLICATION STATE (SHOW_AFFL_STATE)	
0.34 DISPLAT R5252 TERIVITINAL CONTRECTION STATE (SHOW_TERIVI_STATE)	
0.55 DISPLAT/CHAINGE K5232 TERIVITINAL PORT SPEED (SHOW/SET_K5232_SPEED)	ן כ בי
0.50 DISPLATETHERINET PORT ALTO NECOTIATION STATUS	
6.38 DISPLAY DEVICE LOG FILE (SHOW_LOG)	



6.39 RESET LOG FILE (RESET_LOG)	. 53
6.40 RESET ERROR CONDITION (RESET_ERR)	. 53
6.41 SET DEFAULT PARAMETERS (SET_DEFAULT)	. 54
6.42 FIRMWARE UPDATE	. 56
6.43 REBOOT	. 56
6.44 MODULE POWER OFF	56
6.45 SHOW/SET WEB HTTPS STATE (WEB HTTPS STATE)	57
6.46 REPLACING THE DEFAULT CERTIFICATE FOR THE WEB UI (SET CERT)	
6.46.1 Restore the factory default certificate for the web UI (set cert)	. 57
6.47 SHOW/SET MANAGEMENT SESSION TIMEOUT (SESSION EXP. TIME)	
6 48 SHOW/SET FTHERNET MANAGEMENT PORT STATUS (MGMT PORT STATE)	58
6.49 SHOW/SET ETHERNET MANAGEMENT PORT PARAMETERS (MGMT_ORT_PARAMS)	50
Version 3.5 Page 6 of $1/6$	
6 50 SHOW/SET SNIMD TRADS ENABLE STATE (SHOW/SET TRAD)	60
6.51 HEADTREAT DACKET	00
6.51.1 SHOW boartboat packet content	02 62
6.51.1 SHOW Healtbeat packet content	. 02
6.51.2 Lodu Hearlbeat packet content	. 62
6.51.3 Restore default heartbeat packet content	62
6.51.4 Snow/Set neartbeat packet transmit direction	63
6.51.5 Show/Set criteria for determining heartbeat packet failure	64
6.52 REMOTE LOG.	. 65
6.52.1 Show remote log state	65
6.52.2 Set remote log state	65
6.52.3 Show remote log server IP	65
6.52.4 Set remote log server IP	65
6.53 NTP (NETWORK TIME PROTOCOL)	. 66
6.53.1 Show NTP state	66
6.53.2 Set NTP state	66
6.53.3 Show NTP server IP	66
6.53.4 Set NTP server IP	66
6.53.1 Add NTP server IP	67
6.53.1 Delete NTP server IP	67
6.53.2 Send NTP request	67
6.54 TIMEZONE	68
6.54.1 Show timezone list	68
6.54.2 Show timezone	69
6.54.3 Set timezone	
6 54 4 Show daylight saving state	70
6 55 SHOW TECHNICAL SUPPORT INFORMATION	/ 0
71	••••
6 56 WEB LISER	73
6 56 1 Show WEB user name	72
6.56.2 Set WEB user name	72
6.56.3 Set WEB user password	כי 27
6.56.1 Disable/Enable WER interface	כו כד
	73
0.37 WULTI CUNFIGURATION WECHANISM	/4 7/
6.57.1 Display saved IBS configurations.	/4
0.57.2 Save IBS configuration.	. 74



6 E7 2 Dectare the IDC cauged configuration	74
6.57.4 Remove caved configuration	74 74
6.59 TELNET ACCESS	74
6.50 SCH ACCESS	75
6 60 STATISTICS COLINTERS	70
6.61 TACACS+ (TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTEM PLUS) SUPPORT	/ / 78
6 61 1 TACACS+ state	78
6 61 2 Set TACACS+ server IP	70 78
6 61 3 Add TACACS+ server IP	70
6 61 4 Del TACACS+ server IP	79
6.61.5 Show TACACS+ server IP	80
6.61.6 Set RS232 TACACS+ login	80
6.61.7 Show RS232 TACACS+ login	80
6.61.8 Set TACACS+ login fallback	81
6.61.9 Show TACACS+ login fallback	81
6.61.10 Set TACACS+ secret key	81
6.61.11 Set TACACS+ multi users flag.	82
6.61.1 Display TACACS+ multi users flag	82
Version 3.5 Page 7 of 146	
6.61.1 TACACS+ authorization	82
6.62 PERMITTED IP SUPPORT.	83
6.62.1 Set/delete permitted IP range	83
6.62.2 Display permitted IP range	83
6.62.3 Check permitted IP range	83
7 SNMP	84
7 SNMP	<b> 84</b> 84
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS show snmp entry To view the current SNMP entry or the view all entries use the command:	<b> 84</b> 84
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all]	<b> 84</b> 84 84
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry	<b> 84</b> 84 84 85
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries)	<b> 84</b> 84 84 85 85
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry	<b> 84</b> 84 85 85 86
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 84 85 85 86 87
7 SNMP 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry 7.1.3 Set/show_snmp_user set_snmp_user XXX - set snmp user name (5 - 30 symbols).	84 84 85 85 86 87 87
7 SNMP 7.1 SNMP_ENRTY COMMANDS show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry 7.1.3 Set/show_snmp_user set_snmp_user XXX - set snmp user name (5 - 30 symbols) 7.1.4 snmp version	84 84 85 85 85 86 87 88
7 SNMP 7.1 SNMP_ENRTY COMMANDS. show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry 7.1.3 Set/show_snmp_user set_snmp_user XXX - set snmp user name (5 - 30 symbols). 7.1.4 snmp version 7.1.5 snmp server ip	84 84 85 85 85 86 87 87 88 89
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 85 85 85 87 87 87 88 89 93
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS. show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry - 7.1.3 Set/show_snmp_user set_snmp_user XXX - set snmp user name (5 - 30 symbols) 7.1.4 snmp version 7.1.5 snmp server ip 7.1.6 snmp community access – show/set_snmp_access. 7.1.7 snmp password – set_snmp_user_psw	84 84 85 85 85 85 87 87 88 89 93 94
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 85 85 86 87 87 87 87 87 87 93 94
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 84 85 85 85 87 87 87 87 93 94 94 95
7 SNMP 7.1 SNMP_ENRTY COMMANDS. show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all]	
7 SNMP 7.1 SNMP_ENRTY COMMANDS. show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all]	
<b>7 SNMP</b> 7.1 SNMP_ENRTY COMMANDS. show_snmp_entry To view the current SNMP entry or the view all entries use the command: show_snmp_entry [entry_index all] 7.1.1 add_snmp_entry Add new SNMP entry (up to 11 different entries) 7.1.2 Select SNMP entry - sel_snmp_entry 7.1.3 Set/show_snmp_user set_snmp_user XXX - set snmp user name (5 - 30 symbols). 7.1.4 snmp version 7.1.5 snmp server ip 7.1.6 snmp community access – show/set_snmp_access. 7.1.7 snmp password – set_snmp_user_psw 7.1.8 snmp community status (show/set_snmp_status). 7.1.1 SNMP TRAP IP port - show/set_snmp_trap_port 7.1.2 SNMP MSG IP port - show/set_snmp_msg_port 7.2 SNMP VARIABLES 7.3 SNMP TRAPS.	
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 85 85 86 87 87 87 87 87 87 93 93 94 94 95 95 96 101
7 SNMP 7.1 SNMP_ENRTY COMMANDS	
7 SNMP 7.1 SNMP_ENRTY COMMANDS	84 84 85 85 85 85 87 87 87 87 93 93 94 94 95 95 96 103 103 103
7 SNMP         7.1 SNMP_ENRTY COMMANDS	84 84 85 85 85 86 87 87 87 87 97 93 94 95 95 96 103 103 103



# USER GUIDE EdgeSafe 10G Modular Bypass | Firmware Rev Level: 0.3.3.2

8.2 LOGIN	
8.3 INFORMATION PAGE	
8.3.1 Information page for device with hardware 0.3.0.11 and up	
Logoff	
8.3.3 Information area description.	
8.4 BYPASS PAGE	
8.4.1 Bypass configuration area description	
8.4.2 Selective bypass filter	110
8.4.3 Advanced features configuration area	
8.4.1 RX/TX errors processing	
8.5 SYSTEM PAGE	
8.5.1 configuration area	
8.5.2 TACACS+ configuration area	
8.5.3 Time configuration area	115
8.5.4 NTP configuration area	115
8.5.5 Ethernet management port area	115
8.6 ACCOUNT PAGE	117
8.6.1 Interface	117
8.6.2 User	
8.6.3 Password	117
8.6.4 Session timeout	
8.7 SNMP PAGE	
8.7.1 SNMP Entry	
8.7.2 Access	119
Version 3.5 Page 8 of 146	
8.7.1 Name	
8.7.1 Status	
8.7.2 SNMP control port	
8.7.3 SNMP trap account	119
8.7.4 SNMP trap control	
8.8 LOG FILE PAGE	
8.8.1 Remote log file control area	
8.9 HB PACKET PAGE	122, 123
8.10 RESCUE PAGE	
8.10.1 Device firmware update area	
8.10.2 System restore are	
8.10.3 Technical support area	
9 MANAGEMENT PUSH BUTTON INTERFACE	
9.1 MAIN MENU	
9.2 INFO MENU	
9.3 INFOMNF MENU:	
9.4 OP MENU	127
10 APPENDIXES	
10.1 KEY FEATURES	
10.2 BYPASS SPECIFICATIONS	129
10.3 PRODUCT DEFAULT SPECIFICATIONS	



10.4 TECHNICAL SPECIFICATIONS	129
10.4.1 IBSH	129
10.4.2 IBS10G-SR / IBS10G-SR	130
10.4.3 IBS10G-LR / IBS10GP-LR	131
1.1 IBSG –SX / IBSGP-SX	
1.1.1 Fiber Gigabit Ethernet Technical Specifications - (1000Base-SX) Adapters:	131
1.1.2 LED and Connector Specifications	
1.2 IBSG-LX / IBSGP-LX	
1.2.1 Fiber Gigabit Ethernet Technical Specifications - (1000Base-LX) Adapters:	133
1.2.2 LED and Connector Specifications	
10.5 APPENDIX D: ORDER INFORMATION:	
10.6 SAFETY PRECAUTIONS	
10.6.1 Safety considerations for the IBS rack mounting:	138
10.7 TFTP SERVER INSTALLATION AND CONFIGURATION.	139
10.7.1 Windows TFTP server installation and configuration	139
10.7.2 Linux TFTP server installation and configuration	139
10.8 MANAGEMENT SERIAL (RS232) CABLE DRAWING	
10.9 NET-SNMP COPYRIGHT	140
10.10 TACACS+ COPYRIGHT	145
LIST OF FIGURES	
Figure: 1. IBS Bypass Switch Normal Mode.	
Figure: 2. IBS Bypass Switch Passive Mode.	
Figure: 3. IBS Bypass Switch TAP Mode.	
Figure: 4 IBS Bypass Switch TAPI12 Mode	15

Figure: 4. IBS Bypass Switch TAPI12 Mode.	15
Figure: 5. IBS Bypass Switch TAPA Mode.	
Version 3.5 Page 9 of 146	
Figure: 6. IBS Bypass Switch TAPAI1 Mode.	
Figure: 7. IBS Bypass Switch TAPAI2 Mode.	
Figure: 8. IBS Bypass Switch TAPAI12 Mode.	
Figure: 9. IBS Bypass Switch Linkdrop Mode.	20
Figure: 10. IBS module front panel.	22
Figure: 11. IBS1U with 4 IBS modules	24
Figure: 12. IBSSG front panel	24
Figure: 13. IBS1U rear panel.	25
Figure: 14. IBSSG – Stand-alone unit rear panel.	25
Figure: 15. MCB#RS232- RJ11 to DB9 Management serial cable.	140



# 1 Introduction

EdgeSafe Bypass TAP (IBS) is an active external Bypass switch that protects network integrity from network failures and network maintenance. The IBS generates a heartbeat and supports several modes of operation.

The EdgeSafe Bypass TAP (IBS) includes two duplex LC ports for network ports, two SFP+ ports for the attached in-line network system and two management ports: serial port (RJ-11) and 1GB Ethernet port (RJ-45). The IBS supports 10 Gigabit Multimode Fiber (10GBase-SR) and 10 Gigabit single mode fiber (10GBase-LR) network standards.

The EdgeSafe Bypass TAP (IBS) supports 1 Gigabit Multimode Fiber (1000Base-SR) and 1 Gigabit single mode fiber (1000Base-LX) network standards.

The EdgeSafe Bypass TAP (IBS) is a 1U host system that supports up to four EdgeSafe Bypass TAPs. The Bypass switch host includes two redundant 110 – 220 V AC power supplies or two redundant -48V power supplies.

P/N	Description	Notes:
IBS10G-SR	10 Gigabit (MM) Fiber Intelligent Bypass Switch	10G - Multimode
IBS10G-LR	10 Gigabit (SM) Fiber Intelligent Bypass Switch	10G– Single mode
IBSG-SR	Gigabit (MM) Fiber Intelligent Bypass Switch	1G - Multimode
IBSG-LR	Gigabit (SM) Fiber Intelligent Bypass Switch	1G – Single mode
IBS1U	Intelligent Bypass Switch 1U host system	1U host system
IBS10GP-SR	10 Gigabit (MM) Fiber Intelligent Bypass Switch	10G - Multimode
		(with power supply trap capabilities)
IBS10GP-LR	10 Gigabit (SM) Fiber Intelligent Bypass Switch	10G– Single mode
		(with power supply trap
		capabilities) <b>e</b>
IBSGP-SR	Gigabit (MM) Fiber Intelligent Bypass Switch	1G - Multimode
		(with power supply trap capabilities)
IBSGP-LR	Gigabit (SM) Fiber Intelligent Bypass Switch	1G – Single mode
		(with power supply trap capabilities)
IBSGP-T	Gigabit Copper Intelligent Bypass Switch	1G – Copper
		(with power supply trap capabilities)
IBS1UP	Intelligent Bypass Switch 1U host system	1U host system
		(with power supply trap capabilities)

## 1.1 TarSHOW release



# 2 Features

# 2.1 General

The EdgeSafe Bypass TAP (IBS) supports four operation modes: **Inline, Bypass, Tap** and **Linkdrop** modes.

In **Inline** mode, the IBS diverts in-line network traffic to the attached in-line network system.

In **Bypass** mode, the IBS diverts in-line network traffic to the other network link only.

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 IBS disables the links on the network ports (NET0, NET1). The IBS simulates switch / router cable disconnection.

The EdgeSafe Bypass TAP (IBS) 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 IBS detects the heartbeat packet coming back it maintains the **Inline** mode state.

When the EdgeSafe Bypass TAP (IBS) does not detect the heartbeat packet from the Network / Monitor the IBS sets to **Bypass**. When the Network / Monitor appliance recovers, it transmits the heartbeat packet back and the IBS sets from **Bypass** to **Inline**.

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

The EdgeSafe Bypass TAP (IBS) can be configured via a management serial communication port and via management Ethernet port using telnet, SSH or SNMP.

# 2.2 Bypass Modes

The EdgeSafe Bypass TAP (IBS) 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 EdgeSafe Bypass TAP (IBS) 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 EdgeSafe Bypass TAP (IBS) 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 IBS 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 IBS will set to Normal / In-Line mode after detecting the heartbeat packets for a period set by the "hb\_holdtime" parameter.





Figure: 1. EdgeSafe Bypass Normal Mode.

#### 2.4 Monitor Link Failure

The IBS supports Monitor ports failure detection. In an event of Link failure on one of the monitor ports, the IBS 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 IBS will then set to Inline mode state after detecting the heartbeat packets for a 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 IBS supports Bypass on Power failure. In event of power loss the IBS 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 IBS 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 changed via management port from their initial default mode.





Figure: 2. EdgeSafe Bypass Passive Bypass Mode.

#### 2.6 Mode

The IBS supports 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.



## 2.7 TAPI12 mode

The IBS supports 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.





# 2.8 TAPA mode

The IBS supports 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.



# 2.9 TAPAI1 mode



The IBS supports 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.



### 2.10 TAPAI2 mode

![](_page_17_Picture_0.jpeg)

The IBS supports 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.

![](_page_17_Figure_3.jpeg)

# 2.11 TAPAI2 mode

The IBS supports 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.

![](_page_18_Picture_0.jpeg)

## Packets can be injected from each monitor port to both network ports.

![](_page_18_Figure_3.jpeg)

# 2.12 Linkdrop mode

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

![](_page_19_Picture_0.jpeg)

![](_page_19_Figure_2.jpeg)

# 2.13 Two Port Link (2PL)

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

# 2.15 Heartbeat active mode

![](_page_20_Picture_1.jpeg)

When heartbeat active mode is ON and the IBS does not detect the heartbeat packet received from the monitor port the IBS 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 IBS stops sending the heartbeats and the IBS 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.

![](_page_21_Picture_0.jpeg)

# 3 Front Panels

# 3.1 EdgeSafe IBS Fiber Module

![](_page_21_Figure_4.jpeg)

1. "Reset" (RST) button – reset the EdgeSafe Bypass TAP.

2. Ethernet monitor port #0 – port to connect a transparent network appliance (10G port on the IBS and 1G port on the IBSG).

3. Ethernet monitor port #1 – port to connect a transparent network appliance (10G port on the IBS and 1G port on the IBSG).

- 4. Watchdog timer (WDT) LED
- 5. ON indicate that Passive Bypass circuitry watchdog timer expired,
- 6. OFF indicate that Passive Bypass circuitry watchdog timer disabled,
- 7. BLINK indicate that heartbeat pulse sent to Passive Bypass circuitry.
- 8. Bypass mode (BYP) LED ON -indicate that:
- 9. Passive Bypass circuitry is set to Bypass OR
- 10. Active Bypass circuitry is set to Bypass or TAP or Linkdrop.
- 11. Ethernet network port 0 port to connect network device (10G port on the IBS10G and 1G port on the IBSG).

12. Ethernet network port 1 – port to connect network device (10G port on the IBS10G and 1G port on the IBSG).

13. Push button 1 – EdgeSafe Bypass TAP management button 1

- 14. Management 1G Ethernet network port EdgeSafe Bypass TAP management Ethernet port
- 15. Management RS232 port EdgeSafe Bypass TAP management serial port.
- 16. System OK (S.OK) LED indicate EdgeSafe Bypass TAP boot status.
- 17. Alarm (ALM) LED indicate serious hardware problem.Monitor port 0 activity (AC) LED indicate network activity for monitor port 0.
- 18. Monitor port 0 link (LK) LED indicate network link for monitor port 0.
- 19. Monitor port 1 activity (AC) LED indicate network activity for monitor port 1.
- 20. Monitor port 1 link (LK) LED indicate network link for monitor port 1.
- 21. Normal mode (NRM) LED indicate when ON that Normal mode is set.
- 22. Network port 0 activity (AC) LED indicate network activity for network port 0.
- 23. Monitor port 0 link (LK) LED indicate network link for network port 0.
- 24. Network port 1 activity (AC) LED indicate network activity for network port 1.
- 25. Network port 1 link (LK) LED indicate network link for network port 1.
- 26. LCD indicate EdgeSafe Bypass TAP current status.
- 27. Push button 0 EdgeSafe Bypass TAP management button 0
- 28. Power ON (PWR) LED indicate power ON.

![](_page_23_Picture_0.jpeg)

# 3.2 EdgeSafe IBS1U – IBS1U with 4 modules

![](_page_23_Picture_3.jpeg)

Figure: 11. EdgeSafe with 4 modules

3.3 IBSSU – IBS standalone unit - front panel

![](_page_23_Picture_6.jpeg)

Figure: 12. EdgeSafe IBSSG front panel

![](_page_24_Picture_0.jpeg)

# 4 Rear Panels

# 4.1 EdgeSafe IBS1U - IBS1U - rear panel

![](_page_24_Figure_4.jpeg)

![](_page_24_Figure_5.jpeg)

4.2 EdgeSafe IBSSU – IBS standalone unit rear panel

<b>•</b> ]		•	100
Ground Power entry 1	Power entry 2		

# Figure: 14. EdgeSafe IBSSG - Stand alone unit rear panel

![](_page_25_Picture_1.jpeg)

# 5 EdgeSafe Bypass TAP (IBS) Installation

5.1 Rack mount the EdgeSafe IBS

The IBS is a rack mounting ready box. To rack mount the IBS:

- 1. Attach the 2 mounting flanges to the IBS using 3 screws for each mounting flange.
- 2. Slide the IBS into 1U slot and screw the IBS to the rack using 2 screws on each mounting flange.

# 5.2 Connecting Power to the AC IBS unit (230V/120V)

- 5.2.1 Verify that the power switch on the IBS unit is OFF.
- 5.2.2 Connect two power cables to the power supplies on to the back of the IBS. The PWR led's on the front panel of the IBS will illuminate when switching on the power switch power.

# 5.3 Connecting Power to the DC IBS unit (-48VDC)

- 5.3.1 Use DC power source -48V DC with circuit breaker 5A
- 5.3.2 Verify that the power is OFF on the DC power source
- 5.3.3 Verify that the power switch on the IBS unit is OFF
- 5.3.4 Connect the DC input wires to the DC input terminal on the IBS as follows:
  - i. Connect wire to ground terminal IBS (left)
  - ii. Connect OV return to "+" terminal IBS ( center)
  - iii. Connect -48V wire to "-" terminal ( right) IBS
  - iv. Turn on the DC power source The PWR led that is on the front panel of the IBS will illuminate

![](_page_26_Picture_1.jpeg)

# 5.4 Connecting the RS232 DB9 management cable

- 1. Connect the RS232 DB9 cable supplied with the IBS to the IBS 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 IBS.
- 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 IBS
- 6. Login prompt will appear in the terminal window.
- 7. The login name: admin, the default password: gtadmin1
- 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 IBS
- 3. The following are the default IP and login parameters:
  - IP address: 192.168.0.100
  - Net mask: 255.255.255.0
  - Gateway: 192.168.0.1
  - 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

![](_page_27_Picture_0.jpeg)

# 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 a 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 a partial command the IBS will display all the commands which contain this part.

6.1 Main menu

IBS10G command line interface: help - this screen, help full - full help, exit - exit from CLI (logoff). IBS10G\$

![](_page_28_Picture_0.jpeg)

# 6.2 Commands list

```
M10GxSBP$ help
show/set hb emit,
                             show/set op mode,
                                                                  show/set lfp,
show/set_hb_interval,
                             show/set_hb_holdtime,
                                                                  show/set_preserve_hb_mode,
show/set_bypass_mode,
                             show/set_inline_restore,
                                                                  show_current_user,
show/set ip,
                             show/set netmask,
                                                                  show/set_gateway,
show/set time,
                             set username,
                                                                  set password,
show/set_device_name,
                             whoami,
                                                                  show_dev_alert,
show ver,
                             show_config,
                                                                  show status,
show hw ver,
                             show fw ver,
                                                                  show tk num,
show_fan_status,
                             show_appl_status,
                                                                  show_terminal,
show_link,
                             show_log,
                                                                  show/set_mgmt_port_params,
show/set_snmp_ver,
                             show/set_snmp_srv_ip,
                                                                  show/set_snmp_username,
set_snmp_password,
                             apply_snmp,
                                                                  show/set_trap,
reset_log,
                             set_default,
                                                                  update,
reboot,
                             clear_errors,
                                                                  show/set_web_https,
show_hb_pkt,
                             set_hb_defaults,
                                                                  show/set session exp time,
                             show/set hb dir,
show/set_mgmt_port,
                                                                  show/set hb fail mode,
show/set_remote_log_server_ip,
                                    show/set_remote_log_status,
show/set_ntp_status,
                             show/set_ntp_server_ip,
                                                                  send_ntp_request,
show timezone list,
                             show/set timezone,
                                                                  show_daylight_status,
                             show/set_web_username,
show_support_info,
                                                                  set_web_password,
save_conf,
                             restore_conf,
                                                                  show_list_conf,
remove_conf,
                             show/set_tacacs_multi_users,
show/set tacacs status,
                             set tacacs key,
                                                                  show/set tacacs server ip,
                             show/clear_stat,
show/set_telnet_status,
                                                                  show/set_rs232_speed,
set/del_mgmt_permit_ip,
                             show/check_mgmt_permit_ip,
show/set m2n,
show/set hb dst mac,
                             show/set hb src mac,
                                                                  set default hb macs,
show/set_web,
                             show/set_rx_tx_err_mode,
show/set_advanced_link,
                             show/set default advanced link,
show/set ssh status,
                             show/set int vlan,
                                                                  add/del_tacacs_server_ip,
show/set_tacacs_login_fallback,
                                                                  show/set_m2m,
add/del_ntp_server_ip,
                             show/sel_snmp_entry,
                                                                  add/del_snmp_entry,
show/set_snmp_access,
                             show/set_snmp_status,
                                                                  show/set_snmp_msg_port,
show/set_snmp_trap_port,
                             add/del_snmp_srv_ip,
                                                                  set/restore_cert,
                                    show/set_rs232_tacacs_login,
show/set_authorization_status,
                             add/del_slct_bypass,
show/set_slct_bypass,
                                                                  set/show_mgmt_vlan,
show/set_flow_control,
                             show/set_action_on_reboot,
show/set_radius_auth_port,
                                                                  show/set radius acct port,
show sessions,
                             stop_all_sessions,
                                                                  show/set_pas_bypass,
      - Exits from CLI and ends session (logoff).
Exit
```

![](_page_29_Picture_1.jpeg)

# 6.3 Heartbeat active mode. (hb\_act\_mode)

When heartbeat active mode is ON the IBS sends heartbeat packets on its monitor ports. If the IBS does not detect the heartbeat packet received from the monitor ports the IBS 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 IBS 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:

IBS\$ show\_hb\_act\_mode hb active mode: on. command succeeded. IBS\$ set\_hb\_act\_mode off command succeeded. IBS(manual)\$ show\_hb\_act\_mode hb active mode: off. command succeeded. IBS\$

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.

![](_page_30_Picture_1.jpeg)

# 6.4 Active Bypass mode

When heartbeat active mode is set to OFF the IBS 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 "show\_bypass\_mode" In order to change set the Active bypass circuitry use the command " set\_bypass\_mode".

Examples:

IBS(manual)\$ show_bypass_mode active state: inline command succeeded.
IBS (manual)\$ set_bypass_mode bypass command succeeded.
IBS (manual)\$ show_bypass_mode active state: bypass_command succeeded
IBS(manual)\$ set_bypass_mode tap command succeeded.
IBS(manual)\$ show_bypass_mode active state: tap. command succeeded.
IBS(manual)\$ set_bypass_mode linkdrop command succeeded.
IBS(manual)\$ show_bypass_mode active state: linkdrop. command succeeded.
IBS(manual)\$ set_bypass_mode tapi12 command succeeded.
IBS(manual)\$ set_bypass_mode tapa command succeeded.
IBS(manual)\$ set_bypass_mode tapai1 command succeeded.
IBS(manual)\$ set_bypass_mode tapai2 command succeeded.
IBS(manual)\$ set_bypass_mode tapi12 command succeeded.
IBS\$

# 6.5 Power off state (pwoff\_status)

The IBS supports Disconnect or Bypass mode at power off. When in Disconnect, in any event of power off the IBS will be in Disconnect mode - simulates switch / router cable disconnection on the two network ports. When in Bypass, in any event of power off the IBS

![](_page_31_Picture_0.jpeg)

will be in bypass mode.

Pwoff\_status is set to Bypass mode by default Bypass.Supported only with new HW devices (IBSP hardware version 0.3.2.0 and up).

Example:

IBS\$ show_pwoff_sta	atus		
Power off state : command succeeded	bypass . d.		
IBS\$ set_pwoff_state command succeeded	us disconnect d.		
IBS\$ show_pwoff_sta	atus		
Power off state : command succeeded	disconnect d.		
IBS\$			

# 6.6 hb\_interval (hb\_interval)

The IBS 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:

IBS\$ show_hb_interval
hb_interval: 5 ms.
command succeeded.
IBS\$ set_hb_interval 3
command succeeded.
IBS\$ show_hb_interval
hb_interval: 3 ms.
command succeeded.
IBS\$

![](_page_32_Picture_0.jpeg)

# 6.7 hb\_holdtime (hb\_holdtime)

The IBS monitors the received packets on monitor port1, if heartbeat packets do not arrive within "hb\_holdtime" msec, the IBS will set the Active Bypass to Bypass/TAP/Linkdrop mode, depending 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:

IBS\$ show_hb_holdtime
hb_holdtime: 20 ms. command
succeeded.
command succeeded.
IBS\$ show_hb_holdtime
hb_holdtime: 10 ms. command succeeded.
IBS\$

# 6.8 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:

IBS\$ show\_keep\_hb\_act\_mode keep\_hb\_act\_mode: off. command succeeded.
IBS\$ set\_keep\_hb\_act\_mode on command succeeded.
IBS\$ set\_keep\_hb\_act\_mode off command succeeded.
IBS\$

![](_page_33_Picture_0.jpeg)

# 6.9 Heartbeat expiration state (hb\_exp\_state)

When the IBS 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).

#### Example:

IBS\$ show_hb_exp_state	e
hb expired state: command succeeded.	bypass.
IBS\$ set_hb_exp_state ta command succeeded.	ар
IBS\$ show_hb_exp_state	e
hb expired state: command succeeded.	tap.
IBS\$ set_hb_exp_state li command succeeded.	inkdrop
IBS\$ show_hb_exp_state	e
hb expired state: command succeeded.	linkdrop.
IBS\$ set_hb_exp_state ta command succeeded.	api12
IBS\$ set_hb_exp_state ta command succeeded.	ара
IBS\$ set_hb_exp_state ta command succeeded.	apail
IBS\$ set_hb_exp_state ta command succeeded.	apai2
IBS\$ set_hb_exp_state ta command succeeded.	apai12
IBS\$	

![](_page_34_Picture_1.jpeg)

# 6.10 Restore from Heartbeat expiration event (en\_act\_hb\_restore)

The IBS supports 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 IBS 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 IBS preserves its state and no heartbeat packets are generated.

The following actions should be taken to restore the normal operation:

- Restore the external environment to normal work.
- Send command "set\_bypass\_mode inline"
- Send command "set\_hb\_act\_mode on"

#### Example:

IBS\$ show\_en\_act\_hb\_restore restore active state: on. command succeeded. IBS\$ set\_en\_act\_hb\_restore off command succeeded. IBS\$ show\_en\_act\_hb\_restore restore active state: off. command succeeded. IBS\$

![](_page_35_Picture_1.jpeg)

# 6.11 Change Bypass state on RX/TX error detection (rx\_tx\_err\_mode)

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.

#### Example:

IBSG\$ show_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.
IBSG\$ set_rx_tx_err_mode trap timeout mon net threshold
<ul> <li>set rx and tx error processing mode</li> </ul>
<b>trap</b> : on off - enable/disable trap timeout: >0 - minimal time between traps <b>mon</b> :
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) IBSG\$
set_rx_tx_err_mode on 4 linkdrop linkdrop 20


### 6.12 Selective Bypass Filter

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) For MLPS and IP - it is possible to set the upstream (net0 to Net1) or/and downstream (Net1 to Net0).

Selective bypass commands: set\_slct\_bypass - enable/disable , show\_slct\_bypass , add\_slct\_bypass , del\_slct\_bypass

BS10GP5 set_sict_bypass
et_slct_bypass mpls vlan 1p on off
<ul> <li>set selective bypass.</li> </ul>
When ON, all filtered traffic goes
from NET0 to NET1 and vice versa
BS10GP\$ set_slct_bypass mpls on command succeeded. BS10GP\$ set_slct_bypass vlan on command succeeded. BS10GP\$ set_slct_bypass ip on command succeeded. BS10GP\$ add_slct_bypass add_slct_bypass mpls_up mpls_down vlan data mask add_slct_bypass mpls_up mpls_down vlan data mask add_slct_bypass ip_up ip_down ip_src/mask n/a ip_dst/mask n/a - add selective bypass. When using n/a, correspondent parameter
not applicable.
BS10GP\$ add_slct_bypass mpls_up 44443 33333 command succeeded. BS10GP\$ get_slct_bypass mpls
MPLS: off
Upload
lata/mask: 0x0ad9b(44443) 0x08235(33333)
Download
command succeeded.
BS10GP\$ add_slct_bypass vlan 20 0xfff
DS10CS act alst harves also
D STOGD get_sict_bypass vian
lots/mastr: 0x00014/20\ 0x000002/4005\
1 $1$ $1$ $1$ $1$ $1$ $1$ $1$ $1$ $1$
command succeeded.



IBS10GP\$ add\_slct\_bypass ip\_up 192.168.1.40/32 192.168.1.32/32 command succeeded. IBS10GP\$ get\_slct\_bypass ip IP: off ------ Upload ----- Src ----- Dst ----ip/mask: 192.168.1.40/32 192.168.1.32/32 ------ Download ---- Src ----- Dst ----command succeeded.



### 6.13 Advanced LINK modes

#### 6.13.1 Set link (available on the IBSG 1G Copper)

The IBS supports link speed 10, 100 and 1000 Full Duplex and Half Duplex, Enable/Disable Autonegotiation.

Default link speed is 1G Auto-negotiation. Please note that both Network and Monitor ports should use the same Network speed in order to avoid packet loss.

#### Example:

IBSGP-T\$ get_lin	k
get_link XXX	- get port link (MON0, MON1, NET0,
NET1).	
IBSGP-T\$ set_lin1	k MON0 on fd 100m
command succeed	ed.
IBSGP-T\$ get_lin	k MON0
monitor port 0:	link up (speed: 100 megabits/sec, full-duplex).
aut	oneg on

#### 6.13.1 Two port link

The IBSG (Copper and Fiber ) 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.

IBS\$ get_2pl	
two port link:	off.
command succeeded.	
IBS\$ set_2pl on	
command succeeded.	
IBS\$ get_2p1	
two port link:	on.
command succeeded.	
IBS\$ set_2pl off	
command succeeded.	
IBS\$ get 2pl	
two port link:	off.
command succeeded.	
IBS\$	

### 6.13.2 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.

Example:

IBS10G\$ get_m2n		
m2n (Mon port 0):	off.	
m2n (Mon port 1):	off.	
command succeeded.		
IBS10G\$ set m2n MO	N0 on	
command succeeded.		
IBS10G\$ get_m2n		
m2n (Mon port 0):	on.	
m2n (Mon port 1):	off.	
command succeeded.		
IBS10G\$ set_m2n MO	N1 on	
command succeeded.		
IBS10G\$ get_m2n		
m2n (Mon port 0):	on.	
m2n (Mon port 1):	on.	
command succeeded.		
IBS10G\$ set_m2n MO	N1 off	
command succeeded.		
IBS10G\$ get_m2n		
m2n (Mon port 0):	on.	
m2n (Mon port 1):	off.	
command succeeded.		
IBS10G\$		

### 6.13.3 M2M mode

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

Example:

IBS10GP\$ get\_m2m m2m: off. command succeeded. IBS10GP\$ set\_m2m on command succeeded. IBS10GP\$ get\_m2m m2m: on. command succeeded. IBS10GP\$



### 6.13.4 Advanced\_link (available on the IBS 1G/10G fiber)

Advanced link mode enables the IBS ability to detect Network and Monitor link failure based on RXdisconnection on the link partner. By default the advanced link is disabled (off).

Example:

IBSG10P\$ get_advanced_link
advanced link discover: off.
Command succeeded.
IBSG10P5 set_advanced_link on
IDSC100\$ act advanced link
IBSG10P3 get_advanced_link
advanced link discover: on.

### 6.13.5 Set\_default\_advanced\_link (available on the IBS 1G/10G fiber)

Advanced link mode enables the IBS ability to detect Network and Monitor link failure based on RX disconnection on the link partner. By default the advanced link is disabled (off). It is possible to change the default state of the advanced\_link feature using the command:

set\_default\_adavnced \_link

Example:

IBSG10P\$	
get_default_advanced_link	
default of advanced link: off.command succeeded.	
IBSG10P\$	
set_default_advanced_link on	
command succeeded.IBSG10P\$	
get_default_advanced_link	
default of advanced link: on.	
command succeeded.	

#### 6.13.6 Show/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 show\_int\_vlan\_id display the current internal vlan id Example:

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



## 6.14 Ethernet management port IP address

The Ethernet management port default IP address: 192.168.0.100 The IP address can be set to a different IP address using the command set\_ip . Example:

IBS\$ get ip	
device ip address: command succeeded.	192.168.0.100
IBS\$ set_ip 192.168.0.	101
New system IP will tak	e effect after reboot.
command succeeded. IBS\$ get ip	
device ip address: command succeeded. IBS\$	192.168.0.101

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.

### 6.15 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:

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

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



### 6.16 Ethernet management port gateway IP address

The Ethernet management port default gateway IP address is 192.168.0.1.

The net default gateway IP address can be set to different IP address using the command: set\_gateway

Example:

IBS\$ get\_gateway default gateway ip address: 192.168.0.1 command succeeded. IBS\$ set\_gateway 192.168.0.2 New default gateway will take effect after reboot. command succeeded. IBS\$ get\_gateway default gateway ip address: 192.168.0.2 command succeeded. IBS\$

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 addresses.

## 6.17 Ethernet management port VLAN ID

The VLAN id for the Ethernet management port can be modified show/set\_mgmt\_vlan. Example:



### 6.18 Time

To change the IBS 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:

IBS\$ get\_time Time: Thu Feb 5 13:10:00 2009 command succeeded. IBS\$ 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. IBS\$ get\_time Time: Fri Feb 5 13:10:02 2010 command succeeded. IBS\$



### 6.19 System user (set\_user)

To change the IBS user name (factory default user name is: "admin") use the command "set\_user". The new username will take effect after the next login.

Example:

IBS\$ set\_user Tomcat System user name changed, this operation requires logoff. Continue? (Y/n). n command succeeded. IBS\$

### 6.20 Display current user

Current user can be displayed by command "show\_current\_user". Example:

IBS10G\$ get\_current\_user current user: customer IBS10G\$

### 6.21 System password (set\_psw)

To change the IBS system password (factory default is "gtadmin1" ) Use the command "set\_psw". The new password will take effect after the next login.

IBS\$ 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.
IBS\$



### 6.22 Unit name

The IBS supports individual names for each IBS unit on the network. The User can set the IBS unit name (default unit name: ibs) using the command: set\_unit\_name. Unit name can be up to 25 symbols.

Example:

IBS\$ get_unit_name
unit name: ibs
command succeeded.
IBS\$ set_unit_name first
command succeeded.
IBS\$

### 6.23 Who am I (whoami)

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

IBS\$ whoami on command succeeded. I BS\$ whoami off command succeeded. IBS\$

### 6.24 Display IBS versions (show\_ver)

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

IBS\$ get ver	
hardware version:	0.2.0.0
firmware version:	0.2.0.0
swdaemon version:	1.0.2.24
swctl version:	1.0.2.24
u-boot version:	U-Boot 1.3.0, Dec 7 2009, 09:05:02
kernel version: command succeeded.	2.6.23-S-001, #29 Thu Dec 3 16:57:36 IST 2009
IBS\$	



# 6.25 Display IBS parameters (show\_params)

Show the current IBS parameters values.

IBS\$ get_params	
Time: Thu Fel	5 13:12:08 2009
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:	bidirectional.
hb_fail:	unidirectional.
device ip address:	192.168.0.100
netmask:	255.255.255.0
gateway ip address:	192.168.0.1
log file destination:	flash.
https:	off.
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:	"tftpboot".
eth management port param IBS\$	s:speed:auto, duplex:auto



# 6.26 Display IBS state (show\_dev\_state)

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

IBSGP\$ get dev s	tate
Time: Sun Ju	1 27 10:46:46 2014
DEVICE STATUS	and the standard out that "In " In Section 1" Exc.
Box fan 1 status:	operate.
Box fan 2 status:	operate.
Box fan 3 status:	operate.
Box fan 4 status:	operate.
Box fan 5 status:	operate.
Box fan 6 status:	operate.
Power 1:	FAIL
Power 2:	OK
Memory status:	OK
NTP status:	OFF
CPU status:	OK
eth management po	ort: on.
SYSTEM EVENT	STATUS:
active state:	inline.
passive state:	inline.
application:	alive.
rs232 terminal:	disconnected.
network port 0:	link down.
	autoneg on
network port 1:	link down.
	autoneg on
monitor port 0:	link up.
	autoneg on
monitor port 1:	link up.
	autoneg on
command succeede	ed.



## 6.27 Display device alert status

Show the current IBS Alarm status .

#### Example:

```
IBSGP$ get_dev_alert

Time: Sun Jul 27 10:46:17 2014

DEVICE ALARM LIST:

Power 1: FAIL

SYSTEM ALERT STATUS:

network port 0: link down.

network port 1: link down.

command succeeded.

IBSGP$
```

6.28 Display device hardware version (show\_hw\_ver)

Example:

```
IBSG$ get_hw_ver
hardware version: 1..1
command succeeded.
IBSG$
```

## 6.28 Display device firmware version (show\_fw\_ver)

Device firmware version is the generalized version that allows you to determine versions of all software components.

Example:

```
IBS$ get_fw_ver
firmware version: 0.0.99.2
command succeeded.
IBS$
```

6.30 Display device Tracking number (show\_dev\_tk\_num)

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



# 6.31 Display device fan state (show\_fan\_state)

Fan status displayed if hardware version is 0.1.0.0 or higher.

Example:

For the IBSG10:

IBS10G\$ get fan	state	
Module fan status:	operate.	
IBSGP-RW\$ get_f	an_state	
Box fan 1 status:	operate.	
Box fan 2 status:	operate.	
Box fan 3 status:	operate.	
Box fan 4 status:	operate.	
Box fan 5 status:	operate.	
Box fan 6 status:	operate.IBS10G\$	

For the IBSG (1G Copper and 1G Fiber):

IBSGP\$ get_fan_st	tate
Box fan 1 status:	operate.
Box fan 2 status:	operate.
Box fan 3 status:	operate.
Box fan 4 status:	operate.
Box fan 5 status:	operate.
Box fan 6 status:	operate.
IBSP\$	

6.32 Displaying power supplies states.

The command show\_power\_state displays the status of the 1U chassis power supplies This command is supported only with hardware version 0.3.0.0.11 and up. Example:

IBS10G\$ get\_power\_state Power 1: OK Power 2: OK PASS IBS10G\$ get\_power\_state Power 1: FAIL Power 2: OK PASS



# 6.33 Display application state (show\_appl\_state)

The command show\_appl\_state display the current status of the application installed on the monitor appliance that is connected to the IBS monitor ports:

- Alive The link on the monitor ports are ON and the IBS receives the heartbeat packets
- Fail The link on the monitor ports are ON and the IBS does not receive the heartbeat packets
- Unknown The link on the monitor ports are OFF

Example:

IBS\$ get\_appl\_state application: alive. command succeeded. IBS\$

## 6.34 Display rs232 terminal connection state (show\_term\_state)

Example:

IBS\$ get_term_sta	ite	
rs232 terminal:	connected.	
command succeed	ed.	
IBS\$		

## 6.35 Display/change rs232 terminal port speed (show/set\_rs232\_speed)

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

s232_speed
115200
eeded.
s232_speed 9600
rs232 speed settings requires a reboot of the device.
)



# 6.36 Display Ethernet port state (show\_link)

The command "show\_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:

IBS\$ get_link MC	N0	
monitor port 0: command succeed IBS\$	link up. led.	

## 6.37 Change Ethernet port auto-negotiation status

The command "set\_link XXX enable\_autoneg|disable\_autoneg is used to set Ethernet port auto negotiation mode. By default auto-negotiation is enabled. This command is supported only by IBSG devices.

Where XXX:

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

Example:

IBSG\$ set\_link MON0 disable\_autoneg command succeeded. IBS\$

# 6.38 Display device log file (show\_log)

The command show\_log displays the IBS log file. Example:

IBS\$ get_log		
log file destination:	flash.	
swdaemon (version 1.	0.0.4) started: Thu Feb 513	:02:40 2009
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.		
IBS\$		



# 6.39 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:

IS40G\$ reset_log	
command succeeded.	
154065	

Example:

IBS\$ reset\_log command succeeded. IBS\$

### 6.40 Reset error condition (reset\_err)

The Command "reset\_err" is used to reset error conditions in the IBS.

IBS\$ reset_err	
command succeeded.	
IBS\$	



## 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:

IBS\$ set_default	
command succeeded.	
IBS\$	

The factory default settings are:

- IP address: 192.168.0.100
- Net mask: 255.255.255.0
- Gateway: 192.168.0.1
- hb\_act\_mode: on
- hb\_exp\_state: bypass
- Keep heartbeat active mode: disabled
- hb\_interval : 5 ms
- hb\_holdtime: 20 ms
- hb\_tx\_dir: mon0
- hb\_fail: unidir
- enable snmp traps: disabled all snmp trap -
- snmp server ip: 192.168.0.6
- snmp version: 1
- WEB expired time: 900 sec
- WEB https: disabled
- TFTP server ip: 192.168.0.6
- SNMP user: admin
- SNMP password: gtadmin1
- Unit name: ibs
- TFTP root: tftpboot
- Two port link: disabled
- M2N: off
- Advanced link: off
- Expire state: Bypass
- 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: on
- 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
- Tacacs fallback: off
- Tacacs multi users: off
- WEB user name: admin
- WEB user password: gtadmin1
- Tacacs secret key: default\_tac\_key



# 6.42 Firmware Update

Follow the instructions on the firmware update user guide to perform the firmware update:

- ibs10g.ppc1\_fw\_update\_xxxdoc IBS10G with PPC rev 1.0
- ibs10g.ppc2\_fw\_update\_xxx.doc IBS10G with PPC rev 2.1
- ibsg.ppc1\_fw\_update\_xxx.doc IBSG with PPC rev 1.0
- ibsg.ppc2\_fw\_update\_xxx.doc IBSG with PPC rev 2.1

SCP protocol supported by firmware update:

update user@ScpSrvIP:[Path\_to\_fw\_update] [force]

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

## 6.43 Reboot

The reboot command forces a reboot of the IBS.

Example:

IBS\$ reboot	
rebooting	

## 6.44 Module power off

The command power\_off, causing the individual IBS module to be powered off.

It enable the user to replace individual IBS module while the rest of the IBS modules on the same 1U chassis are powered on up and running.

This command is supported only with hardware version 0.3.0.0.11 and up.

IBS10G\$ power_off Shutdown	



# 6.45 Show/Set WEB HTTPS state (web\_https\_state)

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

IBS\$ get_w	eb_https_state	
https:	off.	
command su	acceeded.	
IBS\$ set_we	eb_https_state on	
command su	acceeded.	
IBS\$ get_w	eb_https_state	
https:	on.	
command su	acceeded.	
IBS\$		

6.46 Replacing the default certificate for the web UI (set\_cert)

For HTTPS connections with the web UI, the IBS has its certificate. By default, the IBS "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

Example:

IBS10G\$ set\_cert 192.168.0.06 tftpboot command succeeded.

**6.46.1** Restore the factory default certificate for the web UI (set\_cert)

To restore the factory default certificate use the command restore\_cert. Example:

IBS10G\$ restore\_cert command succeeded.



### 6.47 Show/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 IBS) before the session will be terminated by the IBS (default 900 sec).

In case that the WEB session was terminated the Login screen will appear on the WEB browser.

Example:

IBS\$ get_session_expired_time	
session timeout: 900 sec.	
command succeeded.	
IBS\$ set_session_expired_time 1000 command succeeded.	
IBS\$ get_session_expired_time	
session timeout: 1000 sec. command succeeded. IBS\$	

### 6.48 Show/Set Ethernet management port status (mgmt\_port\_state)

The IBS 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.

IBS\$ get_mgmt_port_state
eth management port: on.
command succeeded.
IBS\$ set_mgmt_port_state off
command succeeded.
IBS\$ get_mgmt_port_state
eth management port: off.
command succeeded.
IBS\$



## 6.49 Show/Set Ethernet management port parameters (mgmt\_port\_params)

The IBS Ethernet management port can set to auto negotiation mode or to force 10 Mbit/s half duplex mode (factory default = auto)

IBS\$ get_mgmt_port_params
eth management port params: speed:auto, duplex:auto.
command succeeded.
IBS\$ set_mgmt_port_params 10h
command succeeded.
IBS\$ get_mgmt_port_state
eth management port params: speed:10, duplex:half.
command succeeded.
IBS\$ set_mgmt_port_params auto
command succeeded.
IBS\$ get_mgmt_port_state
eth management port params: speed:auto, duplex:auto.
command succeeded.
IBS\$



## 6.50 Show/Set snmp traps enable state. (show/set\_trap)

SNMP traps can be enabled or disabled from CLI interface by using set\_trap command.

Default – all traps disabled.

Command SHOWs 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.
  - $\circ~$  all all traps.

SNMP trap enable state can be obtained by the show\_en\_trap command. Command does not Show parameters.



IBS10G\$ get_trap	
trap status: 0x00000000	
trap ibs10gTrapApp1Failed	: off
trap ibs10gTrapApp1Recovered	: off
trap ibs10gTrapMon0LinkDown	: off
trap ibs10gTrapMon0LinkUp	: off
trap ibs10gTrapMon1LinkDown	: off
trap ibs10gTrapMon1LinkUp	: off
trap ibs10gTrapNet0LinkDown	: off
trap ibs10gTrapNet0LinkUp	: off
trap ibs10gTrapNet1LinkDown	: off
trap ibs10gTrapNet1LinkUp	: off
trap ibs10gTrapTermDisc	: off
trap ibs10gTrapTermConnect	: off
trap ibs10gTrapError	: off
trap ibs10gTrapPasBypassOff	: off
trap ibs10gTrapPasBypassOn	: off
trap ibs10gTrapActNormalOn	: off
trap ibs10gTrapActBypassOn	: off
trap ibs10gTrapActTrapOn	: off
trap ibs10gTrapUpdate	: off
trap ibs10gTrapLinkDropOn	: off
trap ibs10gTrapUpdateReboot	: off
trap ibs10gTrapTapi12On	: off
trap ibs10gTrapTapaOn	: off
trap ibs10gTrapTapai1On	: off
trap ibs10gTrapTapai2On	: off
trap ibs10gTrapTapai12	: off
trap ibsTrapPower1OK	: off (only for hw 0.3.0.11 and up)
trap ibsTrapPower2OK	: off (only for hw 0.3.0.11 and up
trap ibsTrapCpuFanOK	: off (only for hw 0.3.0.11 and up)
PASS	
IBS10G\$	

IBS10G\$ set\_trap on all PASS IBS10G\$ IBS10G\$ set\_trap off appl bp mon PASS IBS10G\$



### 6.51 Heartbeat packet

#### 6.51.1 SHOW heartbeat packet content

Display the current heartbeat packet content:

#### 6.51.2 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 XX	This value will be replaced by the IBS to the IBS port0/port1 MAC address
Source MAC	XX XX XX XX XX XX XX	This value will be replaced bythe IBS to the IBS 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.

IBS\$ load_hb_pkt 192.168.0.2 tftpboot	
command succeeded.	
IBS\$	



### 6.51.3 Restore default heartbeat packet content

Default heartbeat packet content can be restored by command:

IBS\$ set\_default\_hb\_pkt command succeeded. IBS\$

### 6.51.4 Show/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.

BS\$ get_hb_tx_dir	
b_dir: mon0. ommand succeeded.	
BS\$	
BS\$ set_hb_tx_dir mon1 command succeeded.	
BS\$ set_hb_tx_dir bidir	
ommand succeeded.	
BS\$ set_hb_tx_dir mon0	
ommand succeeded.	
BS\$	



### **6.51.5** Show/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.

<u>Unidirectional</u>: The IBS will change its state if one of the monitor ports does not receive heartbeat packets. The IBS will restore to its default state when both monitor ports receive the heartbeat packets.

**<u>Bidirectional</u>**: The IBS will change its state if both monitor ports do not receive the heartbeat packets. The IBS will restore to its default state if at least one of the monitor ports receives the heartbeat packets.

IBS\$ get\_hb\_fail hb\_fail: unidirectional. command succeeded. IBSG\$ IBS\$ set\_hb\_fail bidir hb\_dir: bidirectional. command succeeded. IBS\$



### 6.52 Remote log

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

#### 6.52.1 SHOW remote log state

The IBS remote log state can be retrieved by command "show\_remote\_log\_state". Example:

BS10G\$ get_remote_log_state	
remote log state: off.	
command succeeded.	
BS10G\$	

### **6.52.2** Set remote log state

The IBS remote log state can be set by command "set\_remote\_log\_state".

#### Example:

IBS10G\$ set_remote_log_state on
command succeeded.
IBS10G\$ get_remote_log_state
remote log state: on.
command succeeded.
IBS10G\$ set_remote_log_state off
command succeeded.
IBS10G\$

### 6.52.3 SHOW remote log server IP

The Remote log server IP can be retrieved by command "show\_remote\_log\_server\_ip".

Default remote log server IP: 192.168.0.6.

Example:

```
IBS10G$ get_remote_log_server_ip
remote log server ip: 192.168.0.6
command succeeded.
IBS10G$
```

#### 6.52.4 Set remote log server IP

The IBS remote log server IP can be set by command "set\_remote\_log\_server\_ip".

IBS10G\$ set\_remote\_log\_server\_ip 192.168.0.6 command succeeded. IBS10G\$



## 6.53 NTP (Network Time Protocol)

The IBS clock can be synchronized using the NTP protocol. The IBS support multi NTP servers –up to 10. NTP can be enabled or disabled (default: disable).

#### 6.53.1 SHOW NTP state

The IBS NTP state can be retrieved by command "show\_ntp\_state".

IBS10G\$ get\_ntp\_state NTP state: off. command succeeded. IBS10G\$

#### 6.53.2 Set NTP state

The IBS NTP can be enabled or disabled by command "set\_NTP\_state".

IBS10G\$ set\_ntp\_state on command succeeded. IBS10G\$ get\_ntp\_state NTP state: on. command succeeded. IBS10G\$ set\_ntp\_state off command succeeded. IBS10G\$

#### 6.53.3 SHOW NTP server IP

The NTP server IP can be retrieved by command "show\_ntp\_server\_ip".

Default NTP server IP: 192.168.0.6.

IBS10G\$ get_ntp_s	erver_ip
NTP server ip:	192.168.0.6
command succeede	d.
IBS10G\$	

#### 6.53.4 Set NTP server IP

The IBS main NTP server IP can be set by command "set\_ntp\_server\_ip".

IBS10G\$ set\_ntp\_server\_ip 192.168.0.6 command succeeded. IBS10G\$ 6.53.5 Add NTP server IP

Add NTP server IP

IBS10GP\$ get\_ntp\_server\_ip NTP server ip: 192.168.0.6 command succeeded. IBS10GP\$ add\_ntp\_server\_ip 192.168.0.55 command succeeded. IBS10GP\$ get\_ntp\_server\_ip NTP server ip: 192.168.0.6 192.168.0.55

#### 6.53.6 Delete NTP server IP

IBS10GP\$ get\_ntp\_server\_ip NTP server ip: 192.168.0.6 command succeeded. IBS10GP\$ add\_ntp\_server\_ip 192.168.0.55 command succeeded. IBS10GP\$ get\_ntp\_server\_ip NTP server ip: 192.168.0.6 192.168.0.55 command succeeded. IBS10GP\$ del\_ntp\_server\_ip 192.168.0.55 command succeeded. IBS10GP\$ get\_ntp\_server\_ip

### 6.53.7 Send NTP request

Force NTP request using the command send\_ntp\_request



## 6.54 Timezone

### 6.54.1 SHOW timezone list

The Command "show\_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 zones 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").

IBS10G\$ 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.
IBS10G\$



IBS10G\$ 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" IBS10G\$

#### 6.54.2 SHOW timezone

Command "show\_timezone" retrieves current time zone. Default time zone is UTC (GMT+0) time zone.

IBS10G\$ get_tit	mezone
timezone:	Etc/UTC (GMT-0).
command succe	eded.
IBS10G\$	

### 6.54.3 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).
```



IBS10G\$ set\_timezone off Mountain Timezone group: Canada Mountain (GMT-7) Is the above information OK? (Y/n)y command succeeded. IBS10G\$ 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. IBS10G\$

### 6.54.4 SHOW daylight saving state

Daylight saving state can be retrieved by command "show\_daylight\_state".

IBS10G\$ get\_daylight\_state daylight saving state: off. command succeeded. IBS10G\$



## 6.55 SHOW technical support information

The command gathers all the necessary information needed for the Technical Support team in order to help resolve 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.	
kem 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.	

IBS10G\$ get_support_info	
Tue Apr 13 22:29:45 2010	
full device part number:	IB10G-SR
device product part number:	IBS10G
Unit name:	ibs
product tracking number:	C164301300011
device hardware version:	0.2.0.0
device firmware version:	0.2.0.2
device swdaemon version:	1.0.2.60
device swctl version:	1.0.2.60
u-boot version and date:	U-Boot 1.3.0, Jan 19 2010, 12:39:21
kernel version and date:	2.6.23-S-001, #171 Wed Mar 10 17:28:38 IST 2010
swdaemon build date:	Wed Mar 24 10:30:05 2010
swctl build date:	Wed Mar 24 10:30:05 2010
badas build date:	Wed Mar 24 10:30:05 2010
snmpd build date:	Wed Mar 24 10:30:06 2010
passive bypass build date:	Wed Mar 24 10:30:04 2010
kernel bde driver build date:	Wed Mar 24 10:30:04 2010
user bde driver build date:	Wed Mar 24 10:30:04 2010
Configuration information	

IBS10G\$



IBS10G\$ get support info kern log 20 Freescale eLBC NAND Driver (C) 2006-2007 Freescale NAND device: Manufacturer ID: 0xec, Chip ID: 0x75 (Samsung NAND 32MiB 3,3V 8-bit) Scanning device for bad blocks fsl-elbc fsl-elbc.0: Using OF partition information Creating 3 MTD partitions on "nand": 0x0000000-0x00100000 : "log" 0x00100000-0x00200000 : "params" 0x00200000-0x02000000 : "fs" i2c /dev entries driver rtc-ds1307 0-0068: rtc core: registered ds1339 as rtc0 TCP cubic registered NET: Registered protocol family 1 NET: Registered protocol family 17 turn off boot console udbg0 rtc-ds1307 0-0068: setting the system clock to 2010-04-14 04:36:52 (1271219812) RAMDISK: Compressed image found at block 0 VFS: Mounted root (ext2 filesystem). Freeing unused kernel memory: 140k init command succeeded. IBS10G\$


## 6.56 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.

#### 6.56.1 SHOW WEB user name

WEB user name can be retrieved by command "show\_web\_user".

IBS10G\$ get\_web\_user web user: customer command succeeded. IBS10G\$

#### 6.56.2 Set WEB user name

WEB user name can be set by command "set\_web\_user".

IBS10G\$ set\_web\_user customer command succeeded. IBS10G\$

#### 6.56.3 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).

#### 6.56.4 Disable/Enable WEB interface

The command set\_web is used to disable/enable WEB interface.

The command show\_web is used for displaying WEB interface state.

IBS10G\$ get\_web WEB interface: on. command succeeded. IBS10G\$ set\_web off command succeeded. IBS10G\$ get\_web WEB interface: off. command succeeded.



## 6.57 Multi configuration mechanism

The user can save and restore several (~100) different configurations of the IBS parameters.

The IBS saves these different configurations on internal flash memory (~1 MB).

Configuration can be saved locally or on a remote server by SCP protocol.

To work with remote server should be used additional parameter:

user@ScpSrvIP:[Path/][ConfName]

#### 6.57.1 Display saved IBS configurations

Command "show\_list\_conf" used for displaying the local saved IBS configurations.

IBS10G\$ get_list_conf	
saved configurations:	
cust1_03	
cust2_31	
command succeeded.	
IBS10G\$	

### 6.57.2 Save IBS configuration

Command "save\_conf' used for local and remote saving the IBS configurations.

```
IBS10G$ save_conf cust2_31
command succeeded.
IBS10G$
```

### 6.57.3 Restore the IBS saved configuration

To restore the saved configuration the command "restore\_conf" should be used (to display saved configurations run "show\_list\_conf").

After restoring configuration the IBS must be rebooted.

```
IBS10G$ restore_conf cust2_31
Restoring configuration require reboot device.
Continue? (Y/n)
y
rebooting...
```

#### 6.57.4 Remove saved configuration

The command "remove\_conf" is used to remove saved configuration from the Flash memory.

```
IBS10G$ remove_conf cust1_03
command succeeded.
IBS10G$
```



## 6.58 Telnet access

The IBS supports the Telnet protocol. By default the Telnet access is enabled. The Command "show\_telnet\_state" is used to retrieve telnet access state. The Command "set\_telnet\_state" is used to enable or disable telnet access.

IBS10G\$ get\_telnet\_state telnet state: on. command succeeded. IBS10G\$ set\_telnet\_state off command succeeded. IBS10G\$ get\_telnet\_state telnet state: off. command succeeded. IBS10G\$ set\_telnet\_state on command succeeded. IBS10G\$



## 6.59 SSH access

The IBS supports SSH protocol. By default the SSH access is enabled. The Command "show\_ssh\_state" is used to retrieve ssh access. The Command "set\_ssh\_state" is used to enable or disable ssh access.

IBS10G\$ get\_ssh\_state sshstate: on. command succeeded. IBS10G\$ set\_ssh\_state off command succeeded. IBS10G\$ get\_ss\_state ssh state: off. command succeeded. IBS10G\$ set\_ssh\_state on command succeeded. IBS10G\$



## 6.60 Statistics counters

The IBS supports several statistics counters. Statistics can be displayed and cleared.

IBS10G\$ clear_stat command succeeded	L				
1031000					
IBS10G\$ get stat					
	SUM	Mon0	Mon1	Net0	Netl
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 IBS10G\$			100	• • • • •	

Statistic description:

#	Name in IBS statistic	Name	RFC
1	RxPkts	snmpEtherStatsPkts	RFC 1757
2	RxOctets	snmplflnOctets	RFC 1213
3	TxOctets	snmplfOutOctets	RFC 1213
4	RxPktGood	snmpEtherStatsRXNoErrors	RFC 1757
5	RxUnicastPkts	snmplflnUcastPkts	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	snmplfHCOutBroadcastPckts	RFC 2233
12	RxDiscards	snmplflnDiscards	RFC 1213
13	TxDiscards	snmplfOutDiscards	RFC 1213



6.61 TACACS+ (Terminal Access Controller Access Control System Plus) support.

The IBS supports TACACS+ for remote access (WEB access, SNMP access, SSH access, Telnet access).

The IBS TACACS+ supports:

- clear and encrypted mode.
- Authentication , authorization and Accounting (tac\_plus.rfc.1.78.txt).
- Inbound PAP Login (Password Authentication Protocol).

TACACS+ disabled by default.

TACACS+ secret key length can be from 8 to 127 characters.

Default secret key: default\_tac\_key.

Support Multi TACACS+ servers, default TACACS 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.

#### 6.61.1 TACACS+ state

TACACS+ can be enabled or disabled by command "set\_tacacs\_state".

The command also controls the encryption of the session and the SNMP sessions will be authenticated by the TACACS+ server.

TACACS+ state can be retrieved by command "show\_tacacs\_state".

```
set_tacacs_state XXX snmp - set TACACS state (off - default,
on_clear, on_encrypted).
snmp - on: enable tacacs for snmp.
snmp - off: disable tacacs for snmp.
IBS10G$ set_tacacs_state off off
command succeeded.
IBS10G$ set_tacacs_state on_clear off
command succeeded.
IBS10G$ set_tacacs_state on_clear on
command succeeded.
IBS10G$ set_tacacs_state on_encrypted on
command succeeded.
```

#### 6.61.2 Set TACACS+ server IP

The IBS supports multi TCACS servers, the command set\_tacacs\_server\_ip sets the main TACACS+ server.

```
IBS10G$ set_tacacs_server_ip 192.168.0.6
command succeeded.
IBS10G$
```



#### 6.61.3 Add TACACS+ server IP

The IBS support multi TACACS+ servers (up to 10 servers), additional TACACS+ server can be added to the TACACS+ servers using the command add\_tacacs\_server\_ip

IBS10G\$ add\_tacacs\_server\_ip 192.168.1.159 command succeeded. IBS10G\$

#### 6.61.4 Del TACACS+ server IP

TACACS+ server IP can be deleted from the TACACS+ server list using the command :

del\_tacacs\_server\_ip (Main TACACS+ server cannot be deleted).

IBS10G\$ del\_tacacs\_server\_ip 192.168.1.159 command succeeded. IBS10G\$



#### 6.61.5 SHOW TACACS+ server IP

TACACS+ server IP can be retrieved by command "show\_tacacs\_server\_ip"

IBS10G\$	
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	
IBS10G\$	

#### 6.61.6 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

IBS10G\$
set rs232 tacacs login on off
- set rs232 login via tacacs.IBS10G\$ set rs232 tacacs login on
IBS10G\$ set_rs232_tacacs_login on
command succeeded.
IBS10G\$ set rs232 tacacs login off

command succeeded.

#### 6.61.7 SHOW RS232 TACACS+ login

The TACACS+ RS232 access status can be retrieved by command: "show\_rs232\_tacacs\_login"

IBS10G\$ get\_rs232\_tacacs\_login rs232 tacacs login: off command succeeded. IBS10G\$



#### 6.61.8 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/disables the login fallback to the local IBS credentials in case that no TACACS+ server is available.

IBS10G\$ set\_tacacs\_login\_fallback on command succeeded. IBS10G\$

#### 6.61.9 SHOW TACACS+ login fallback

TACACS+ login fallback status can be retrieved by command "set\_tacacs\_login\_fallback"

IBS10G\$ get\_tacacs\_login\_fallback TACACS login fall back: off command succeeded. IBS10G\$

6.61.10 Set TACACS+ secret key

TACACS+ secret key can be set by command "set\_tacacs\_key"

IBS10G\$ set\_tacacs\_key default\_key command succeeded. IBS10G\$



#### 6.61.11 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 IBS and TACACS server have this account.

TACACS+ multi users flag can be set by command "set\_tacacs\_multi\_users" (default: on)

IBS10G\$ set\_tacacs\_multi\_users off|on command succeeded. IBS10G\$

#### 6.61.12 Display TACACS+ multi users flag

The state of TACACS+ multi users flag can be displayed by command "show\_tacacs\_multi\_users"

IBS10G\$ get\_tacacs\_multi\_users TACACS multi-users: off. command succeeded. IBS10G\$

#### 6.61.13 TACACS+ authorization

When TACACS+ authorization is enabled, the IBS uses information retrieved from the user profile, which is located either in the local user database or on the TACACS+ server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

The IBS TACACS+ Authorization defines 2 user levels.

Read only. Read/write

6.61.13.1 set\_authorization\_state

By default the TACACS+ authorization is disabled. The command set\_authorization state on/off enable/disable the TACACS+ Authorization.

IBS10G\$ set\_authorization state on command succeeded. IBS10G\$



## 6.62 Permitted IP support

The IBS supports SSH protocol. By default the SSH access is enabled.

The IBS supports 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.

6.62.1 Set/delete permitted IP range

New permitted IP range can be added by command "set\_ mgmt\_permit\_ip"

IBS10G\$ set\_mgmt\_permit\_ip 192.168.0.0/24 command succeeded. IBS10G\$

Permitted IP range can be removed by command "del\_ mgmt\_permit\_ip".

Command Show parameters Netlp/NetMask or "all".

With parameter "all" command remove all permitted IP ranges and the device will receive commands from all IP.

IBS10G\$ del\_mgmt\_permit\_ip 192.168.0.0/24 command succeeded. IBS10G\$

#### 6.62.2 Display permitted IP range

Permitted IP range can be displayed by command "show\_ mgmt\_permit\_ip"

```
IBS10G$ get_mgmt_permit_ip
permitted ip: 192.168.0.0/24
command succeeded.
IBS10G$
```

#### 6.62.3 Check permitted IP range

Permitted IP range can be checked by command "check\_mgmt\_permit\_ip"

IBS10G\$ check\_mgmt\_permit\_ip 192.168.0.0/24 All management servers can be accessed. command succeeded. IBS10G\$



# 7 SNMP

The IBS supports up to 11 different SNMP entries (Entry = user name/community). Each entry supports up to 8 different SNMP servers.

Each entry supports 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.

## 7.1 SNMP\_Entry commands

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

- Show\_snmp\_entry:

To view the current SNMP entry or the view all entries use the command:show\_snmp\_entry [entry\_index | all] -

- show current snmp entry,
- all show all entries,
- 1 11 show correspondent entry

get snmp entry [entry index all] get current snmp entry, all - get all entries, 1 - 11 - get correspondent entry. IBS10GP\$ get snmp entry all snmp msg port: 161 snmp trap port: 162 TACACS state: off TACACS state for snmp: off all permitted ip: snmp user: customer 1 snmp version: 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. IBS10GP\$



#### 7.1.1 add\_snmp\_entry -

Add new SNMP entry (up to 11 different entries)

IBS10GP\$ add snmp entry snmp entry 2 was created New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get snmp entry all snmp msg port: 161 snmp trap port: 162 TACACS state: off. TACACS state for snmp: off. permitted ip: all customer snmp user: 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: snmp user: snmp version: 1 snmp community status: off snmp community access: read. snmp server ip address: snmp password: command succeeded. IBS10GP\$



#### 7.1.2 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 show\_snmp\_entry

sel\_snmp\_entry entry\_index - select snmp entry (1 - 11)

IBS10GP\$ sel snmp entry 2 command succeeded. IBS10GP\$ IBS10GP\$ get snmp entry ===== entry index 2 == snmp user: snmp version: 1 off snmp community status: snmp community access: read. snmp server ip address: snmp password: command succeeded. IBS10GP\$



#### 7.1.3 Set/show\_snmp\_user

set\_snmp\_user XXX - set snmp user name (5 - 30 symbols).

IBS10GP\$ set\_snmp\_user test1 New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get snmp user snmp user: test1 command succeeded. IBS10GP\$ IBS10GP\$ get\_snmp\_entry ======= entry index 2 == test1 snmp user: 1 snmp version: snmp community status: off snmp community access: read. snmp server ip address: snmp password: command succeeded. IBS10GP\$ IBS10GP\$ IBS10GP\$ get snmp entry all snmp msg port: 161 snmp trap port: 162 TACACS state: off. TACACS state for snmp: off. permitted ip: a11 = === 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 = test1 snmp user: 1 snmp version: snmp community status: off snmp community access: read. snmp server ip address: snmp password: command succeeded.



7.1.4 snmp version

set\_snmp\_ver XXX - set snmp version (1, 2c, 3, default - 1)
show\_snmp\_ver

IBS10GP\$ get snmp ver snmp version: 1 command succeeded. IBS10GP\$ set snmp ver 3 New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get snmp ver snmp version: 3 command succeeded. IBS10GP\$ BS10GP\$ get snmp entry ===== entry index 2 = test1 snmp user: 3 snmp version: snmp community status: off snmp community access: read. snmp server ip address: snmp password: command succeeded. IBS10GP\$



#### 7.1.5 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:

- show\_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

#### 7.1.5.1 show\_snmp\_srv\_ip

Show the SNMP servers IP for the current selected entry

IBS10GP\$ get snmp srv ip snmp server ip address: 192.168.0.44 command succeeded. IBS10GP\$ sel snmp entry 1 command succeeded. IBS10GP\$ get snmp srv ip snmp server ip address: 192.168.0.44 192.168.0.111 192.168.0.33 command succeeded. IBS10GP\$ sel snmp entry 2 command succeeded. IBS10GP\$ get snmp srv ip snmp server ip address: 192.168.0.44 command succeeded. IBS10GP\$



7.1.5.2 add\_snmp\_srv\_ip

IBS10GP\$ get\_snmp\_srv\_ip snmp server ip address: 192.168.0.44 192.168.0.111 command succeeded. IBS10GP\$ del\_snmp\_srv\_ip 192.168.0.111 New SNMP setting will take effect after apply\_snmp. command succeeded. IBS10GP\$ apply\_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get\_snmp\_srv\_ip snmp server ip address: 192.168.0.44 command succeeded. IBS10GP\$



7.1.5.3 del\_snmp\_srv\_ip

Note: The main SNMP srv\_ip cannot be deleted.

IBS10GP\$ get snmp entry customer snmp user: 1 snmp version: 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. IBS10GP\$ del snmp srv ip 192.168.0.33 New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get snmp entry ======= entry index 1 == customer snmp user: 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. IBS10GP\$



7.1.5.4 set\_snmp\_srv\_ip - modify the IP address of the main SNMP server set\_snmp\_srv\_ip xxx.xxx.xxx

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

IBS10GP\$ sel snmp entry 2 command succeeded. IBS10GP\$ get snmp entry ======= entry index 2 == snmp user: test1 3 snmp version: snmp community status: off snmp community access: read. snmp server ip address: 192.168.0.7 192.168.0.33 snmp password: command succeeded. IBS10GP\$ set snmp srv ip 192.168.0.44 New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get snmp entry ======== entry index 2 == = test1 snmp user: 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. IBS10GP\$



#### **7.1.6** snmp community access – show/set\_snmp\_access

Each entry supports different levels 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.
- show\_snmp\_access

IBS10GP\$ get snmp access snmp community access: read. command succeeded. IBS10GP\$ set snmp access read write New SNMP setting will take effect after apply snmp. command succeeded. IBS10GP\$ apply snmp SNMP restart is in progress, please wait. scommand succeeded. IBS10GP\$ get snmp access snmp community access: read, write. command succeeded. IBS10GP\$ get snmp entry ======= entry index 1 = customer snmp user: 1 snmp version: 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. IBS10GP\$



#### 7.1.7 snmp password – set\_snmp\_user\_psw

The SNMP V 3 requires a password to encrypt and decrypt the SNMP information.

- set\_snmp\_user\_psw
- set\_snmp\_user\_psw [OLD] NEW set snmp user password (8 60 symbols).

IBS10GP\$ set\_snmp\_user\_psw silicom2008 silicom2015 New SNMP setting will take effect after apply\_snmp. command succeeded. IBS10GP\$

#### 7.1.8 snmp community status (show/set\_snmp\_status)

The snmp\_comunity\_status activate or deactivate the SNMP entry

- set\_snmp\_status off/on
- set snmp community status.

snmp community status: on command succeeded. IBS10GP\$ set_snmp_status off New SNMP setting will take effect after apply_snmp. command succeeded. IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	IBS10GP\$ get_snmp_status
command succeeded. IBS10GP\$ set_snmp_status off New SNMP setting will take effect after apply_snmp. command succeeded. IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	snmp community status: on
IBS10GP\$ set_snmp_status off New SNMP setting will take effect after apply_snmp. command succeeded. IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	command succeeded.
New SNMP setting will take effect after apply_snmp. command succeeded. IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	IBS10GP\$ set_snmp_status off
command succeeded. IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	New SNMP setting will take effect after apply_snmp.
IBS10GP\$ apply_snmp SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	command succeeded.
SNMP restart is in progress, please wait. command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	IBS10GP\$ apply_snmp
command succeeded. IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	SNMP restart is in progress, please wait.
IBS10GP\$ get_snmp_status snmp community status: off command succeeded. IBS10GP\$	command succeeded.
snmp community status: off command succeeded. IBS10GP\$	IBS10GP\$ get_snmp_status
command succeeded. IBS10GP\$	snmp community status: off
IBS10GP\$	command succeeded.
	IBS10GP\$



#### 7.1.9 SNMP TRAP IP port - show/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).
- show\_snmp\_trap\_port

IBS10GP\$ get\_snmp\_trap\_port snmp trap port: 166 command succeeded. IBS10GP\$ set\_snmp\_trap\_port 162 New SNMP setting will take effect after apply\_snmp. command succeeded. IBS10GP\$ apply\_snmp SNMP restart is in progress, please wait. ^[[Acommand succeeded. IBS10GP\$ get\_snmp\_trap\_port snmp trap port: 162 command succeeded. IBS10GP\$

#### 7.1.2 SNMP MSG IP port - show/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).
- show\_snmp\_msg\_port

IBS10GP\$ get\_snmp\_msg\_port snmp trap port: 164 command succeeded. IBS10GP\$ set\_snmp\_trap\_port 161 New SNMP setting will take effect after apply\_snmp. command succeeded. IBS10GP\$ apply\_snmp SNMP restart is in progress, please wait. ^[[Acommand succeeded. IBS10GP\$ get\_snmp\_trap\_port snmp trap port: 161 command succeeded. IBS10GP\$



## 7.2 SNMP Variables

#### Variable code:

### .iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).garland(15694).ibs(2).X.0

Variable name	Variablecode (X=)	Туре	Attributes	Value	Description
ibs DevName	1.2	OCTET STRING (SIZE(132))	read-only		Unit name.
ibsDevTrackingNumber	1.3	OCTET STRING (SIZE(132))	read-only		Show device tracking number.
ibs DevHwVer	1.4	OCTET STRING (SIZE(132))	read-only		Show device hardware version.
ibs DevFwVer	1.5	OCTET STRING (SIZE(132))	read-only		Show device firmware version.
ibs SnmpAgentVer	1.6	OCTET STRING (SIZE(132))	read-only		SNMP agent version
ibs Mon0Link	1.8	INTEGER	read-only	down(1), up(2)	Monitor port 0 link status.
ibs Mon1Link	1.9	INTEGER	read-only	down(1), up(2)	Monitor port 1 link status.
ibs Net0Link	1.10	INTEGER	read-only	down(1),up(2)	Network port 0 link status.
ibs Net1Link	1.11	INTEGER	read-only	down(1), up(2)	Network port 1 link status.
ibs ApplState	1.12	INTEGER	read-only	unknown(1), fail(2), alive(3)	Application state.
ibs TermStatus	1.13	INTEGER	read-only	disconnected( 1), connected(2)	Rs232 management port status.
ibsFanStatus	1.25	OCTET STRING (SIZE(30256))	read-only		Show device Fan status
ibsLogLastLine	1.14	INTEGER	read-only		Show log file last line number.
ibsLogReadLine	1.15	INTEGER	read-write		Show/set log file line number to read from.
ibsShowLog	1.16	OCTET STRING (SIZE(12048))	read-only		Show log file content (20 lines beginning from the last read line).
ibsDevUbootVer	1.17	OCTET STRING (SIZE(1128))	read-only		Show U-boot version.
ibsDevKernelVer	1.18	OCTET STRING (SIZE(1128))	read-only		Show kernel version.
ibsLogType	1.19	INTEGER	read-write	swdaemon(1), swctl(2), passive(3), snmp(4), kern(5), auth(6)	Show/set log file type.
ibsSupportInfo	1.20	OCTET STRING (SIZE(12550))	read-only		Show technical support information.
ibsStatistics	1.21	OCTET STRING (SIZE(12550))	read-only		Show device statistics counters.
ibsClearStatistics	1.22	INTEGER	read-write	clear(1)	Clear device statistics. Set only the variable, read will return zero.
ibsPowerStatus	1.23	OCTET STRING (SIZE(10.128))	read-only		Show device power status
ibs SnmpVer	2.1	INTEGER	read-write	1(1), 2c(2), 3(3)	Set the SNMP version. Take effect after setting ibsSnmpApply
ibs SnmpServerIp	2.2	IP Address	read-write		Set/Show SNMP server IP address. Take effect after setting ibs SnmpApply
ibs SnmpUser	2.3	OCTET STRING (SIZE(164))	read-write		Set SNMP user/community and WEB interface user name. Take effect after setting ibsSnmpApply



Variable name	Variablecode (X=)	Туре	Attributes	Value	Description
ibs SnmpPassword	2.4	OCTET STRING (SIZE(17121))	write-only		Define the SNMP v3 and WEB interface password. Parameter consists of old and new passwords separated by semicolon. Take effect after setting ibsSnmpApply
ibs SnmpApply	2.5	INTEGER	write-only	apply (1)	Activate all the SNMP changes.
ibs SysTime	3.1	OCTET STRING (SIZE(132))	read-write		Set/Show device current time/Date.
ibs SysIp	3.3	lpAddress	read-write		Set/Show IBS IP address.
ibs SysNetmask	3.4	IpAddress	read-write		Set/Show IBS IP subnet mask.
ibs SysGateway	3.5	IpAddress	read-write		Set/Show IBS gateway IP address.
ibs SysResetLog	3.6	INTEGER	write-only	reset	Reset/Clear IBS log file.
ibs SysReboot	3.8	INTEGER	write-only	reboot (1)	Reboot the IBS.
	3.9				
ibs UnitName	3.10	(SIZE(132))	read-write		Set/Show unit name
ibs SysTftplp	3.11	IP Address	read-write		Set/Show TFTP server IP address.
ibs SysTftpRoot	3.12	OCTET STRING (SIZE(164))	read-write		Set/Show TFTP server root directory.
ibs SysUpdate	3.13	INTEGER	read-write	update(1), force(2)	Update the IBS firmware.
ibs SysUpdateStatus	3.14	OCTET STRING (SIZE(11024))	read-only		Show IBS firmware update status.
ibs SysResetErr	3.14	ÎNTEĞER "	read-write	reset(1)	Reset/Clear IBS errors.
ibsSysWhoami	3.15	INTEGER	read-write	on(1), off(2)	Unit identification. On/off system OK led blink.
ibsSysRemoteLog	3.16	INTEGER	read-write	on(1), off(2)	Show/set remote log state. NOTE: next SNMP command should be send not before 1 sec after this command
ibsSysRemoteLogServerIp	3.17	IP Address	read-write		Set/Show remote log server IP address. NOTE: next SNMP command should be send not before 1 sec after this command
ibsSysNTP	3.18	INTEGER	read-write	on(1), off(2)	Show/set NTP state.
ibsSysNTPServerIp	3.19	IpAddress	read-write		Set/Show NTP server IP address.
ibsSysDayLight	3.20	INTEGER	read-write	default(1), off(2)	Show/set daylight saving mode. The daylight saving mode will be set finally by ibsSysTimezone.
ibsSysTimezone	3.21	OCTET STRING (SIZE(164))	read-write		Show/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 ibsSysDayLight with parameter OFF first. To complete timezone setting reboot should be issued.
ibsSysWebUser	3.22	OCTET STRING (SIZE(530))	read-write		Show/set the WEB user name.
ibsSysWebPassword	3.23	OCTET STRING (SIZE(17121))	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.
ibsSysSaveConfig	3.24	OCTET STRING (SIZE(420))	read-write		Save device configuration. Set only variable, read will return zero.
ibsSysRestoreConfig	3.25	OCTET STRING (SIZE(420))	read-write		Restore device configuration. Set only variable, read will return zero. The unit will be rebooted.
ibsSysRemoveConfig	2.26	OCTET STRING SIZE(420))	read-write		Remove device configuration. Set only the variable, read will return zero.
ibsSysListConfig	2.27	OCTET STRING (SIZE(12550))	read-only		Show saved device configurations.
ibsSysShowConfigNext	3.28	OCTET STRING (SIZE(12550))	read-only		Show saved device configurations next buffer.



Variable name	Variablecode	Туре	Attributes	Value	Description
ibsSysTacacsKey	3.29	OCTET STRING (SIZE(8127))	read-write		Set the Tacacs secret key. Set only variable, read will return zero length string
ibsSysTacacsState	3.30	INTEGER	read-write	off(1), on_clear(2), on_encrypted (2)	Show/set TACACS state.
ibsSysTacacsServerIp	3.31	IpAddress	read-write		Show/set the IP address of the TACACS server.
ibsSysTelnetState	3.32	INTEGER	read-write	off(1), on(2)	Show/set Telnet state.
ibsSysSetMgmtPermitIP	3.35	OCTET STRING (SIZE(92550))	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)
ibsSysRemoveMgmtPermi tl P	3.36	OCTET STRING (SIZE(92550))	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)
ibsSysShowMgmtPermitIP	3.37	OCTET STRING (SIZE(92550))	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)
ibsSysTacacsMultiUsers	3.38	INTEGER	read-write	off(1), on(2)	Show/set TACACS multi users state.
ibsSysSetTrapAccount	3.39	OCTET STRING (SIZE(92550))	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 ibsSnmpApply.
ibsSysRemoveTrapAccount	3.40	OCTET STRING (SIZE(92550))	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 ibsSnmpApply.
ibsSysShowTrapAccount	3.41	OCTET STRING (SIZE(92550))	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)
ibsSysPowerOff	3.42	INTEGER	read-write	Poweroff(1)	Power off the IBS module.Set only command, read will return zero.
ibsSysPwOffState	3.47	INTEGER	read-write	bypass (2) Disconnect (4)	Device power off state: bypass or disconnect
ibsSysRxTxErrTrapTimeout	3.49		read-write	off(1), on(2)	Enable generating trap on rx/tx error
ibsSysRxTxErrMonAction	3.50		read-write		Allow to choose network ports state when errors detected on monitor port
ibsSysRxTxErrNetAction	3.51		read-write		Allow to choose network ports state when errors detected on network ports
ibsSysRxTxErrRateThreshold	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
ibsConf2pl	4.1	INTEGER	read-write	enable (1), disable (2)	Show/Set two-port link mode
ibsConfHbExpState	4.2	INTEGER	read-write	bypass(2), tap(3), linkdrop(4)	Show/Set heartbeat expiration mode.



Variable name	Variablecode	Туре	Attributes	Value	Description
				tapi12(5), tapa(6), tapai1(7), tapai2(8), tapai12(9)	
ibsConfHbInterval	4.3	INTEGER	read-write		Show/Set heartbeat interval.
ibsConfHbHoldTime	4.4	INTEGER	read-write		Show/Set heartbeat hold time
ibsConfHbActModeLock	4.5	INTEGER	read-write	enable (1), disable (2)	Show/Set heartbeat active mode lock state.
ibsConfHttps	4.6	INTEGER	read-write	enable (1), disable (2)	Show/Set HTTPS protocol enable status.
ibsConfSesTimeout	4.7	INTEGER	read-write		Show/Set WEB session timeout.
ibsConfEnActHbRestore	4.8	INTEGER	read-write	enable (1), disable (2)	Set/Show enable active heartbeat restore.
ibsConfHbPkt	4.11	OCTET STRING (SIZE(482048))	read-write		Show current heartbeat packet content. Set new heartbeat packet content. Packet size: 24-1024 bytes.
ibsConfHbTxDir	4.12	INTEGER	read-write	mon0(1) mon1(2) bidir(3)	Set/Show heartbeats transmit port. If ibsConfHbTxDir is set to either mon0 or mon1 the ibsConfHbFail will be reset to unidir.
ibsConfHbFail	4.13	INTEGER	read-write	unidir(1) bidir(2)	Set/Show criteria for determine heartbeat failure. If ibsConfHbTxDir set to either mon0 or mon1, the ibsConfHbFail must be set to unidir.
ibsConfDefHbPkt	4.14	INTEGER	read-write	default(1)	Restore default heartbeat packet content. Set only the variable, read will return zero.
ibsConfMgmtPortParams	4.15	INTEGER	read-write	auto(1), force_10h(2)	Set/Show ethernet management port parameters. auto - autonegotiation with counterpart ethernet port. force_10H - force 10 Mbit/s half duplex mode.
ibsConfM2n	4.16	OCTET STRING (SIZE(57))	read-write		Set/Show the monitor port link to network link feature state. Set Example: 'on;off' - enable this feature for MON0 and disable for MON1 Show Example: 'MON0: on:MON1: off'.
ibsConfWeb	4.17	INTEGER	read-write	off(1), on(2)	Set/Show WEB interface state (on/off)
ibsOpHbActMode	5.1	INTEGER	read-write	on (1), off (2)	Show/Set heartbeat active mode on/off.
ibsOpActBypass	5.2	INTEGER	read-write	off (1), on (2), tap (3), linkdrop(4), tapi12(5), tapa(6), tapai1(7), tapai2(8), tapai12(9)	Show/Set the state of the active bypass state (inline/bypass/tap/linkdrop).
ibsOpPasBypass	5.3	INTEGER	read-only	off (1), on (2)	Show the state of the passive bypass state.
ibsRecoveryDefault	6.1	ÍNTEGER	write		Restore system default parameter.
ibsTrapConfApplFail	7.2	INTEGER	read-write	enable (1), disable (2)	Enable/Disable Showting trap info on application failed/restored events status change: ibs TrapApplFail / ibsTrapApplRecover.



Variable name	Variablecode (X=)	Туре	Attributes	Value	Description
ibsTrapConfBypass	7.3	INTEGER	read-write	enable (1) disable (2)	Enable/Disable SHOWting trap info on bypass(passive and Active) status change events: ibsTrapActBypassOn / ibs TrapActInlineOn, ibs TrapPasBypassOn / ibsTrapPasBypassOff, ibs TrapTapOn, ibsTrapLinkDropOn, ibs TrapTapi12On, ibs TrapTapaOn, ibs TrapTapai1On, ibs TrapTapai2On, ibs TrapTapai12On.
ibsTrapConfMonLink	7.4	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on Monitor ports Link status change events: ibs TrapMon0LinkDown / ibsTrapMon0LinkUp, ibs TrapMon1LinkDown / ibsTrapMon1LinkUp.
ibsTrapConfNetLink	7.5	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on Network ports Link status change events: ibs TrapNet0LinkDown / ibs TrapNet0LinkUp, ibs TrapNet1LinkDown / ibsTrapNet1LinkUp.
ibsTrapConfTerm	7.6	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on Terminal connect / disconnect status change events: ibs TrapTermDisc / ibs TrapTermCon.
ibsTrapConfErr	7.7	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on error reports from the system: ibsTrapErr.
ibsTrapConfLogSize	7.8	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on Log size overflow: ibs TrapLogSize.
ibsTrapConfUpdate	7.10	INTEGER	read-write	enable (1), disable (2)	Enable/Disable SHOWting trap info on update finish event: ibsTrapUpdate, ibsTrapUpdateReboot



## 7.3 SNMP Traps

Тгар	Value	Description
ibsTrapStart	1	Reserved
ibsTrapApplFail	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.
ibsTrapApplRecover	3	Trap is sent when the Monitor application starts again to send the
		HB packets
ibsTrapPasBypassOn	4	Trap is sent when passive bypass changes to bypass mode.
ibsTrapPasBypassOff	5	Trap is sent when passive bypass changes to inline mode.
ibsTrapActBypassOn	6	Trap is sent when active bypass changes to bypass mode.
ibsTrapActInlineOn	7	Trap is sent when active bypass changes to inline mode.
ibsrapMon0LinkDown	8	Trap is sent when monitor port-0 link drops.
ibsTrapMon0LinkUp	9	Trap is sent when monitor port-0 link is restored.
ibsTrapMon1LinkDown	10	Trap is sent when monitor port-1 link drops.
ibsTrapMon1LinkUp	11	Trap is sent when monitor port-1 link is restored.
ibsTrapNet0LinkDown	12	Trap is sent when network port-0 link drops.
ibsTrapNet0LinkUp	13	Trap is sent when network port-0 link is restored.
ibsTrapNet1LinkDown	14	Trap is sent when network port-1 link drops.
ibsTrapNet1LinkUp	15	Trap is sent when network port-1 link is restored.
ibsTrapTermDisc	16	Trap is sent when local serial RS232 connection is disconnected.
ibsTrapTermCon	17	Trap is sent when local serial RS232 connection is connected.
ibsTrapErr	18	Trap is sent as indication of an error within the IBS, with some
		description of the error.
ibsTrapLogSize	19	Trap is sent when the log file size exceed its maximum allowed
		size.
ibsTrapTapOn	20	This trap is sent when switch changes mode to tap.
ibsTrapUpdate	21	Trap is sent when firmware update is finished.
ibsTrapLinkDropOn	22	This trap is sent when switch changes mode to linkdrop.
ibsTrapUpdateReboot	23	Trap is sent when firmware update is finished and device is
		rebooted.
ibsTrapTapi12On	24	Trap is sent when active bypass changes to TAPI12 mode.
ibsTrapTapaOn	25	Trap is sent when active bypass changes to TAPA mode.
ibsTrapTapai1On	26	Trap is sent when active bypass changes to TAPAI1 mode.
ibsTrapTapi2On	27	Trap is sent when active bypass changes to TAPAI2 mode.
ibsTrapTapi12On	28	Trap is sent when active bypass changes to TAPAI12 mode.
ibsTrapPower1OK	29	This trap is sent when power supply 1 restored from failure.
		(only for hardware 0.3.0.11 and up)
ibsTrapPower2OK	30	This trap is sent when power supply 2 restored from failure.
		(only for hardware 0.3.0.11 and up)
ibsTrapCpuFanOK	31	This trap is sent when CPU FAN restored from failure.
		(only for hardware 0.3.0.00 and up)
ibsTrapRxTxError	32	This trap is sent when device detect RX or TX error.
		Next trap can be send in 5 sec



Тгар	Value	Description
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	his trap is sent when network port 0 was enable by 2pl/m2n
		function
ibsTrapNet1Disable2plM2n	49	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



## 7.4 SNMP request examples (net-snmp application)

SNMP v1 Show request:

snmpSHOW -v 1 -c admin 192.168.0.100 GARLAND-IBS-MIB::ibs TrapConfTerm.0 SNMP v1 set request:

snmpset -v 1 -c admin 192.168.0.100 GARLAND-IBS-MIB::ibs TrapConfTerm.0 = on SNMP v2c Show request:

snmpSHOW -v 2c -c admin 192.168.0.100 GARLAND-IBS-MIB::ibs TrapConfTerm.0 SNMP v2c set request:

snmpset v 2c -c admin 192.168.0.100 GARLAND-IBS-MIB::ibs TrapConfTerm.0 = on SNMP v3 Show request:

snmpSHOW -v 3 -u admin -l authPriv -a SHA -A gtadmin1 -x AES -X gtadmin1 192.168.0.100 GARLAND-IBS-MIB:: ibs TrapConfTerm.0

SNMP v3 set request:

snmpset -v 3 -u admin -l authPriv -a SHA -A gtadmin1 -x AES -X gtadmin1 192.168.0.100 GARLAND-IBS-MIB:: ibs TrapConfTerm.0 = on

## 7.5 Displaying log file via SNMP

Use the following command to control the log display via SNMP

- 1. ibsLogType xxx set log file type (swdaemon, swctl, passive, snmp, kernel, auth)
- 2. ibsLogLastLine Show log file last line number.
- 3. ibsLogReadLine 0 (xxx) Read the log file from line xxx
- 4. ibsShowLog Read 20 lines form the log file

### 7.6 SNMP agent, net-snmp and copyright

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



# 8 Web Interface

## 8.1 Starting web interface

The IBS WEB interface can be accessed from any WEB browser. To connect to the IBS 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 – IBS 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 effect only after clicking the "apply" button.

## 8.2 Login



On the login screen type the user name and the password. (Default username is "admin". Default password is "gtadmin1").

Usernames should include a minimum of 5 symbols and can be up to 64 symbols.

Passwords should include a minimum of 8 symbols and can be up to 128 symbols.

The first user that will be logged in to the WEB interface will show all the rights (Control /monitor) of the Web interface application, additional users will not be able to control the device, they will be able only to monitor the IBS parameters.

When the first user logs off from the WEB interface, the next user will receive all rights and will be able to (Control /monitor) the WEB interface.



## 8.3 Information Page

And AL S	ce mio:		Link info:	Error info	2
hardware version firmware version software version u-boot version kernel version tracking number	n: 1.3.0.21 n: 0.3.0.5 n: 1.1.4.37, U-Boot 1. 2.6.23-S- : 0657010000	(PPC ★ Tue 3.0, 001, 005 ≠	Monitor port 0: Up Monitor port 1: Up Network port 0: Up Network port 1: Up rs232 port: connected	First error: Last error:	ی ک
Active state: inline.	Passive s	tate: inline.	Appl state: alive.		
Power 1: ok.	Power 2	ok.	11		
Box fan 1: onorste	Bowfan S	onerate	Boy fan 3: nuerate		
Des for 4		. operate.	Downer Succession		
50% ian 4. operate	BOX IAI	v operate.	DOX IAN O. OPERAGE.		
			Statistics		
	2	ហេរ	MonQ	Mon1	Net0 🔺
RxPkts	1: 4	18757	207408	207317	2491
RxOct	ets: 1	2504141	50D118B	6338146	143494
TxOcto	ta: 1	4667789	7414B31	6971009	160484
RxPkt	Jood: 1	.92492	92 59 4	98514	1162
REUnio	astPkts: 1	.89486	91743	97287	452
RxHult	icastPkts: 1	.149	306	306	269
	adeastPkts: 4	1792	1124	1118	1277
RxBrod		26311	114832	108821	1329
RxBrod TxPkt	300d: 2	and the second second	114257	108628	493
RxBros TxPkt <sup>0</sup> TxUnio	astPkts: 2	23364	TT 15 0 1		
R×Bro: T×Pkt: T×Unic T×Unic	astPkts: 2 icastPkts: 2; icastPkts: 5	:23364 537	0	D	2 69
R×Bros T×Pkto T×Unio T×Hulo T×Bros	astPkts: 2 icastPkts: 2 icastPkts: 5 icastPkts: 2	23384 337 394	0 577	D 195	269 567
RxBrod TxPkt4 TxUnit TxBrod TxBrod RxD130	astPkts: 2 astPkts: 2 adcastPkts: 5 adcastPkts: 2 ards: 1	23364 337 394 .88638	0 577 91304	D 195 97334	269 567 0
RxBrod TxPkt4 TxUnit TxBrod RxD1st RxErro	cood: 2 castPkts: 2 cicastPkts: 5 idcastPkts: 2 cards: 1 irs: 0	23364 337 394 .88638	0 577 91304 0	0 195 97334 D	269 567 0
RxBrod TxPktd TxUnic TxBrod RxDisc RxErro TxDisc	rood: 2 castPkts: 2 cicastPkts: 5 idcastPkts: 2 cards: 1 nrs: 0 cards: 0	23364 37 394 88638 )	0 577 91304 0	0 195 97334 D D	269 567 0 0
RxBrod TxPkt0 TxUnit TxBrod RxDisc RxErro TxDisc TxErro	rood: 2 castPkts: 2 cloastPkts: 5 adcastPkts: 2 cards: 1 cards: 0 cards: 0 cards: 0	23364 337 394 88638 ) )	0 577 91304 0 0	0 195 97334 D D D	269 567 0 0 0
RxBrod TxPkt0 TxUnid TxBrod RxD13d RxErro TxD13d TxErro	rood: 2 castPkts: 2 cloastPkts: 5 adcastPkts: 2 cards: 1 cards: 0 cards: 0 cards: 0	23364 37 394 88638 ) )	0 577 91304 0 0	0 195 97334 D D D	269 567 0 0 0



### **8.3.1** Information page for device with hardware 0.3.0.11 and up

There is no information specified for this section.

Need to check if this should be here or what?

### **8.3.2** Logoff

The IBS will terminate the WEB session in case that the WEB session is passive (does not send a request to the IBS) for more than the time defined by the web\_expired\_time (default 900 sec).

If the main WEB interface window will be closed other than by pressing on the "Logoff" button, the WEB interface will be unavailable for the time defined by the web\_expired\_time (default 900 sec).

#### 8.3.3 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

#### 8.3.3.1 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

#### 8.3.3.2 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)

#### 8.3.3.3 Error info

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



#### 8.3.3.4 Status information

The Status information area contains status information:

- Active state (bypass/inline/tap/linkdrop)
- Passive state (bypass/inline)
- Application state (alive/fail/unknown)
- Power supply (1 and 2) status (only for hardware 0.3.0.11 and up)
- Box Fan status (1-6) (only for hardware 0.3.0.11 and up)

#### 8.3.3.5 Status information

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



## 8.4 Bypass Page

		Bypass configurat	ion —		-
HB active mode	HB active mode lock	HB active restore	e HB interval	HB hold time	
on 🔻	off •	an 💌	5	20	
Active bypass	HB active expire				
bypass *	bypass 🔻				
BYPASS Bypass	mode				
INLINE Applia	nce Inline mode				
TAP TAP M	lode (Directional Monitoring	g)			
LINKDROP Failed	Appliance Disables Live Li	nk			
TAPI12 TAP M	lode with Injection				
TAPA Aggreg	ate Mode (Combined Moni	toring)			
TAPAI1 Aggreg	ate Mode with Dual Injection	on from Mon0			
TAPAI1 Aggreg TAPAI2 Aggreg	ate Mode with Dual Injection ate Mode with Dual Injection	on from Mon0 on from Mon1			
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg	gate Mode with Dual Injection gate Mode with Dual Injection gate Mode with Dual Injection	on from Mon0 on from Mon1 on from Mon0 and Mo	nl		
TAPAII Aggreg TAPAI2 Aggreg TAPAI12 Aggreg	gate Mode with Dual Injection gate Mode with Dual Injection gate Mode with Dual Injection	on from Mon0 on from Mon1 on from Mon0 and Mo Selective E	nl Sypass Filters ———		
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg Filters State	gate Mode with Dual Injection gate Mode with Dual Injection gate Mode with Dual Injection Operation	on from Mon0 on from Mon1 on from Mon0 and Mo Selective B Data Up	nl Bypass Filters ———	Data	Down
TAPAII Aggreg TAPAI2 Aggreg TAPAI12 Aggreg Filters State	ate Mode with Dual Injection ate Mode with Dual Injection ate Mode with Dual Injection Operation	on from Mon0 on from Mon1 on from Mon0 and Mo Selective E Data Up 1955 (44443) 0x01	n1 Sypass Filters	Data	Down
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg Filters State IPLS V off V V	gate Mode with Dual Injection gate Mode with Dual Injection gate Mode with Dual Injection Operation view • 0x0ac	on from Mon0 on from Mon1 on from Mon0 and Mo Selective B Data Up 195 (44443) 0x00	n1 bypass Filters	Data	Down
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg Filters State	ate Mode with Dual Injection ate Mode with Dual Injection ate Mode with Dual Injection Operation view	on from Mon0 on from Mon1 on from Mon0 and Mo Selective B Data Up 19b (44443) 0x01 Advanced features	n1 bypass Filters 8235 (33333) ¥	Data	Down
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg Filters State IPLS V off V V	ate Mode with Dual Injection ate Mode with Dual Injection operation view	on from Mon0 on from Mon1 on from Mon0 and Mo Selective H Data Up 19b (44443) 0x00 Advanced features HB tx dir	nl bypass Filters 8235 (33333) V HB fail	Data M2N	Down v M2M
IAPAII Aggreg IAPAI2 Aggreg IAPAI12 Aggreg Filters State IPLS V off V V 2 port link off V	ate Mode with Dual Injection ate Mode with Dual Injection ate Mode with Dual Injection Operation view   OxOac Who am I off	on from Mon0 on from Mon1 on from Mon0 and Mo Selective H Data Up 19b (44443) 0x00 Advanced features HB tx dir mon0 v	nl Bypass Filters B235 (33333) V HB fail Undir V	Data M2N disabled •	Down v M2M off v
TAPAII Aggreg TAPAI2 Aggreg TAPAI12 Aggreg Filters State MPLS V off V V 2 port link off V	ate Mode with Dual Injection ate Mode with Dual Injection ate Mode with Dual Injection operation view   OxDac Who am I off  RX/	on from Mon0 on from Mon1 on from Mon0 and Mo Selective B Data Up 19b (44443) 0x00 Advanced features HB tx dir mon0 v TX errors processing	nl bypass Filters 8235 (33333) * HB fail undir *	Data M2N disabled •	Down M2M off •
TAPAII Aggreg TAPAI2 Aggreg TAPAI12 Aggreg Filters State IPLS V off V V 2 port link off V Trap	ate Mode with Dual Injection ate Mode with Dual Injection ate Mode with Dual Injection of the OxOace Who am I off the RX/ Timeout	on from Mon0 on from Mon1 on from Mon0 and Mo Selective B Data Up 19b (44443) 0x00 Advanced features HB tx dir mon0 v TX errors processing Mon	nl bypass Filters 8235 (33333) * HB fail unidir * Net	Data M2N disabled • Rate threshold	Down T M2M off T

#### 8.4.1 Bypass configuration area description

#### 8.4.1.1Heartbeat active mode select box

When heartbeat active mode is ON the IBS send heartbeat packets on its monitor ports. If the IBS does not detect the heartbeat packet received from the monitor ports the IBS 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 IBS 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.


#### 8.4.1.2 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.

#### 8.4.1.3 Heartbeat active restore select box

When the HB active mode is ON the IBS will restore to **Inline (Normal)** state when the heartbeat packets will be received from the Monitor port. When HB active mode is OFF the IBS preserves its state and no heartbeat packets are generated.

The following actions should be taken to restore the normal operation:

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

#### 8.4.1.4 Active bypass select box

When heartbeat active mode is set to OFF the IBS 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.** 

#### 8.4.1.5 HB active expire select box

When heartbeat active mode is ON the IBS send heartbeat packets on its monitor ports. If the IBS does not detect the heartbeat packet received from the monitor ports the IBS 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.

#### 8.4.1.6 Device power off state select box

The IBS supports Disconnect or Bypass mode at power off. When in Disconnect, in any event of power off the IBS will be in Disconnect mode - simulates switch / router cable disconnection on the two network ports. When in Bypass, in any event of power off the IBS will be in bypass mode. Pwoff\_status is set to Bypass mode by default Bypass. Supported only with new HW devices (IBSP hardware version 0.3.2.0 and up).

#### 8.4.1.7 Heartbeat interval textbox

The IBS generates a 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.



#### 8.4.1.8 Heartbeat hold time textbox

The IBS monitor the received packets on monitor port1, if heartbeat packets do not arrive within "hb\_holdtime" msec, the IBS 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.

#### 8.4.2 Selective bypass filter

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).

For MLPS and IP - it is possible to set the upstream (net) to Net1) or/and downstream (Net1 to Net0).

#### **8.4.3** Advanced features configuration area

#### 8.4.3.1 (2) port link

The IBS supports two ports. 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.

#### 8.4.3.2 Who am I

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

#### 8.4.3.3 Hb tx dir

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

#### 8.4.3.4 HB fail

Set /Show the HB fail criteria.

While the HB tx dir is set to bidirectional (HB packets are transmitted from both ports (mon0 andmon1) the HB fail criteria can be set to:

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

#### 8.4.3.5 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.

#### 8.4.3.6 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.

#### 8.4.4 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.

8.4.4.1 Trap

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

*8.4.4.1 Timeout* Set the timeout for sending the RX/TX traps.



#### 8.4.4.3 Mon

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

#### 8.4.4.4 Net

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

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



# 8.5 System Page

		System				
Unit name	Telnet	SSH		Configuration	1	
ibs	on 🔻	on 🔻		•		
		TACACS				
State	Server	ip Mode	. 8	Secret key	Multi users	Fall back
off	▼ 192.166.0.6	VIEW	•		off 🔻	off 🔹
		Time				
Thu Aug 20 13:50:21 20	D15 DayLigh	n T	intezone g	roup	Timeza	one
	off	Etc		•	UTC	•
		NTP				
NTP	NTP set	verip	Opera	tions		
oft •	192.168.0.6		view	•		
Et	hernet management j	port		Permitte	d Network II	? list
System IP	Netmask	Default Gate	Default Gateway Op			aitted IP
192.168.0.100	255.255.255.0	192.168.0.1		view 🔻	2	il v

#### 8.5.1 Configuration Area

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.

#### 8.5.1.1 Unit name

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

#### 8.5.1.2 Telnet

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



#### 8.5.1.3 Configuration

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

#### **8.5.2** TACACS+ configuration area

The IBS supports TACACS+ for remote access (WEB access, SNMP access, SSH access, Telnet access).

#### 8.5.2.1 TACACS+ state

The TACACS+ sate support the following modes:

- TACACS off (default: Off)
- TACACS on , clear text , SNMP on
- TACACS on , encrypted , SNMP on
- TACACS on , clear text , SNMP off\
- TACACS on , encrypted , SNMP off

#### 8.5.2.2 TACACS+ Server Ip

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

#### 8.5.2.3 TACACS+ mode

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

#### 8.5.2.4 TACACS+ secret key

Set the TACACS+ secret key (default: default\_tac\_key)

#### 8.5.2.5 TACACS multi users

Multi users control allows enable/disable TACACS+ multi users mode.

When TACACS+ multi users flag is set, the device will not check the user account, it will rely on TACACS+ server.

When TACACS+ multi users flag is reset, users can login if the IBS and TACACS+ server have this account.

#### 8.5.2.6 TACACS 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.

By setting the TACACS+ fallback to on, it enable the login fallback to the local IBS credentials.



#### 8.5.3 Time configuration area

The IBS supports TACACS+ for remote access (WEB access, SNMP access, SSH access, Telnet access).

8.5.31 Time state

Time format: mm DD HH MM YYYY

Where:

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

#### 8.5.3.2 Daylight state

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

#### 8.5.3.3 Timezone grope state

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

8.5.3.4 Timezone state

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

#### 8.5.4 NTP configuration area

The IBS clock can be synchronized from the NTP server on the network.

The IBS support Multi NTP servers

8.5.4.1 NTP

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

*8.5.4.2 NTP Server IP* Set the NTP server IP address (default IP: 192.168.0.6)

*8.5.4.3 Operation* Enable to add/view/delete NTP server

### 8.5.5 Ethernet management port area

8.5.5.1 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

#### 8.5.5.2 Netmask

The System Netmask IP address is Ethernet management port net mask address.

The new Netmask IP address will take effect only after device reboot.

Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new NETMASK IP addresses.

#### 8.5.5.3 Default gateway

The default gateway IP address is the Ethernet management port default gateway address.

The new default gateway IP address will take effect only after device reboot.

Remote control via telnet, SSH, WEB or SNMP applications should be reconfigured to use new gateway IP addresses.

#### 8.5.5.4 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 display 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/mask

For example:

192.168.2.0/24

10.0.0/8

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.



# 8.6 Account Page

			User account		
Interface web	Name customer	Old Password	New Password	Confirm new Password	WEB session timeou (sec) 900

#### 8.6.1 Interface

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

#### **8.6.2** User

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

#### 8.6.3 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

#### 8.6.4 Session timeout

The web\_exp\_time command sets the time that the WEB session can be passive (does not send requests to the IBS) before the session will be terminated by the IBS (default 900 sec).

In case that the WEB session is terminated the Login screen will appear on the WEB browser.

If the main WEB interface window will be closed in any way other than by pressing on the "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 show all the rights (Control /monitor) of the Web interface application, the next users will not be able to control the device, they will be able only to monitor the IBS parameters.

When the 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.



## 8.7 SNMP Page

			S?	MP entry c	ontrol		
	Entry		Operatio	nis			
1		•	view/edit •				
IP	Operations		Current IP				
view		•	192.168.0.6	٠			
	Status		Name			Version	Access
OF		• 60	stomer		1		read, write, trap 🔹
	Old		New S	NMP port co	ontrol	Confirm	
M 161	sg port	Trap j 162	port S	NMP trap co	ontrol		
4	Deserve	Manaton	Netlate	Transit	Emer	Unitere	
Appi Iail	Bypass	Mon link	iver link	remunal	Error	Opdate	

#### 8.7.1 SNMP Entry

The IBS supports up to 11 different SNMP entries (Entry = user name/community).

Each entry supports up to 8 different SNMP servers.

Each entry supports different levels 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.

8.7.1.1 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

8.7.1.2 SNMP version

The IBS supports SNMP versions 1, 2c and 3.

SNMP version select box destined to change the SNMP version.



#### 8.7.2 Access

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

#### **8.7.3** Name

Define the entry name = SNMP user \community name

#### **8.7.4** Status

Activate/deactivate the SNMP entry

#### 8.7.5 SNMP control port

Message (min - 1, max - 49151, default - 161)

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

#### 8.7.6 SNMP trap account

SNMP trap accounts allow you to add/remove/view additional destinations for SNMP traps.

#### 8.7.7 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.

- 1) Appl fail enable/disable following traps:
  - a) ibsTrapApplFail
  - b) ibs TrapApplRecover.
- 2) Bypass enable/disable following traps:
  - a) ibs TrapActBypassOn
  - b) ibs TrapActInlineOn
  - c) ibs TrapPasBypassOn
  - d) ibs TrapPasBypassOff
  - e) ibs TrapTapOn
  - f) ibs TrapTapi12On
  - g) ibs TrapTapaOn
  - h) ibs TrapTapai1On
  - i) ibs TrapTapai2On
  - j) ibs TrapTapai12On
- 3) Mon link enable/disable following traps:
  - a) ibs TrapMon0LinkDown
  - b) ibs TrapMon0LinkUp
  - c) ibs TrapMon1LinkDown
  - d) ibs TrapMon1LinkUp.
- 4) Net link enable/disable following traps:



- a) ibs TrapNet0LinkDown
- b) ibs TrapNet0LinkUp
- c) ibs TrapNet1LinkDown
- d) ibs TrapNet1LinkUp.
- 5) Terminal enable/disable following traps:
  - a) ibs TrapTermDisc
  - b) ibs TrapTermCon
- 6) Terminal enable/disable following traps:
  - a) ibs TrapTermDisc
  - b) ibs TrapTermCon
- 7) Error enable/disable following traps:
  - a) ibs TrapErr
  - b) ibsTrapPower1OK (only for hardware 0.3.0.11 and up)
  - c) ibsTrapPower1OK (only for hardware 0.3.0.11 and up)
  - d) ibsTrapCpuFanOK (only for hardware 0.3.0.00 and up)
- 8) Log size enable/disable following traps:
  - a) ibs TrapLogSize
- 9) Update
  - a) ibs TrapUpdate
  - b) ibs TrapUpdateReboot



## 8.8 Log file page

	Info		Bypass	Sy	stem	Account	1	Snmp	Log fi	ile _	HB packe	t Res	cue
						Lo	g file v	iew					
Tue	Feb	18	14:20:43	2014	Active	e switch	: "inl	line"					
					appres		overes		22.000	2020			- 1
Tue	Mar	4	07:36:13	2014	swdaes	mon (ver	sion 1	1.1.4.3	7) sta	rted			- 7
Tue	Max	4	07:36:20	2013	Reagin	e switch	: "Dyl						
The	Mar	4	07:36:20	2014	Mon no	ort 0: 1	ink de	-					
Tue	Mar	4	07:36:20	2014	Hon po	ort 1: 1:	ink de	own.					
Tue	Mar	4	07:36:20	2014	Net po	ort 0: 1	ink de	awa					
Tue	Mar	4	07:36:20	2014	Net po	ort 1: 1.	ink de	own.					
Tue	Mar	4	07:43:12	Z014	Mon pr	ort 1: 1	ink up	2					
Tue	Mar	4	07:43:12	2014	Mon po	ort 1: 1	ink de	awn					
Tue	Mar	4	07:43:13	2014	Active	e switch	: "in]	line"					
		SWO	laemon 1 🔹			<		<<			>>		>
						Swdaemo	a log f	ile contr	rol				
eset b	og file	2	Remote lo	g		Remote lo	gip						
.8	1		off 🔻		192	168.0.6		1					

#### 8.8.1 Remote log file control area

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

8.8.1.1 Reset log file Reset the log file – erase the content of the log

*8.8.1.2 Remote log* Set the remote log ON/OFF (default: OFF)

8.8.1.3 Remote log Server IP

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



# 8.9 HB Packet page

Heartbeat packet
Current heartbeat packet content
000: 00 e0 ed 13 24 ff 00 e0 ed 13 24 fe 81 00 00 04 010: 81 37 ff ff 00 30 00 00 00 00 40 04 ec e2 c6 13 020: 01 02 c6 13 01 01 00 00 00 00 00 00 00 00 00 00 00 030: 00 00 00 00 00 00 00 00 00 00 00 00 0
Select new heartbeat packet
Ofesse, Lond new HB Load default HB

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



# 8.10 Rescue page

	I	Device firmware update
hoose File	No file chosen 💿 Force Updat	te.
	New firmware will take effect af Reboot the device only after you	ter reboting. 1 have successfully finished all perts of update,
		System restore
Set defaul	t Reset errors Reboot Power off	
Set defaul	t Reset errors Reboot Power off	inical support information
Set defaul III Apply	Reset errors Reboot Power off	nical support information
Set defaul	Tech Technical support informatio Sun Jul 27 11:21:15 2014	nical support information
Set defaul	Technical support informatio Sun Jul 27 11:21:19 2014 full device part number: 19 device part number: 19	nical support information a \$07-1X \$07-33
Set defaui	Technical support informatio Sun Jul 27 11:21:19 2014 full device part number: 12 device product part number: 12 Unit name: 15	nical support information
Set defaul	Technical support number: IS device product part number: IS device product part number: IS fund the tracking number: IS for the tracking number: IS	anical support information m #07-1X #07-3# #1810000040
Set defaul	Technical support informatio Sum Jul 27 11:21:19 2014 full device part number: 12 device product part number: 13 Unit name: 16 Unit name: 16 device hardware version: 17 device hardware version: 17	Inical support information
Set defaul	Tech Technical support informatio Sun Jul 27 11:21:13 2014 full device part number: IB device product part number: IB Unit name: Ib product tracking number: Ib device hardware varion: K/ device hardware varion: K/	anical support information an 1802-18 1802-18 18180100046 1 3.0.21 (DDC ver. 2.2)



#### **8.10.1** Device firmware update area

The Update command updates the IBS firmware's:

- root file system
- kernel image
- dtb
- u-boot

Follow the instructions on the firmware update user guide to perform the firmware update:

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

#### 8.10.2 System restore area

8.10.2.1 Set default parameters

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

#### 8.10.2.2 Reset errors

Reset the IBS errors.

The IBS displays on the LCD the first error only, after resetting the error the IBS will display the next error if it exists.

8.10.2.3 Reboot

Checking Reboot checkbox force the IBS to reboot

#### 8.10.2.4 Power off

Checking the Power Off check box force power off to the IBS module.

IBS reboot in process, please wait 41 sec...

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

#### 8.10.2.5 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.



#### 8.10.3 Technical support area

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



# 9 Management push button interface

The IBS includes 2 management push buttons (PB0 and PB1). Use PB0 and PB1 buttons to query and control the IBS unit.

PB0 button:

Hold PB0 for more than 3sec to enter or exit from the main menu.

Short press on the PB0 button moves to next menu.

PB1 button:

Hold PB1 button for more than 3sec resets the IBS errors.

Short press on the PB1 button selects the item or displays the next data item.

#### 9.1 Main Menu

The INFO MNF menu includes the following queries:

- INFO
- INFOMNF
- OP
- EXIT

Use a short press on the PB0 button in order to move to the next submenu. Use a short press on the PB1 button to enter to the submenu

### 9.2 INFO menu

The INFO MNF menu includes the following queries:

- HW\_VER Display the hardware version
- FW\_VER Display the firmware version
- SW\_VER Display the software version
- UB\_VER Display u-boot version
- KERN\_VER Display kernel version
- UNIT Display the unit name
- IP\_ADDR Display the management port IP address.
- EXIT Exit to the main menu

Use a short press on the PB0 button in order to move to the next query.

Use a short press on the PB1 button to select the query and to display the next data item on the query.



## 9.3 INFO MNF menu

The INFO MNF menu includes the following queries:

- PRODUCT Display the product name
- TK\_NUM Display product tracking number
- MAC MGMT Display the management port MAC address
- EXIT Exit to the main menu

Use a short press on the PB0 button in order to move to the next query. Use a short press on the PB1 button to select the query and to display the next data item on the query.

## 9.2 OP menu

The INFO MNF menu includes the following queries:

- SHUTDOWN Shutdown the IBS module (the module will reload by removal and insertion of the module)
- REBOOT Reset the IBS module
- DEFAULT Set factory default parameters
- EXIT Exit to the main menu

Use a short press on the PB0 button in order to move to the next query.

Use a short press on the PB1 button to select the query and to display the next data item on the query.



# 10 Appendixes

### 10.1 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
- Two on Board WatchDog Timer (WDT) Controllers
- Software programmable time out interval
- 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
- Independent Bypass / Normal / Tap /Linkdrop operation in every module
- Supports up to four modules in a chassis
- Supports 6 different TAP mode of operation
- Simple CLI configuration management via serial port
- HTTP/HTTPS management interface via network management port
- Telnet management interface via network management port
- SSH management interface via network management port
- Supports SNMP version 1, 2c, 3 (SHA, AES)
- Support for SNMP multi trap destinations
- Supports remote log
- Supports TACACS+
- Support for TACACS+ multi users.
- Supports NTP
- Supports time zone
- Supports remote save/restore backup configuration
- Two redundant power supplies
- Support power supply monitoring
- Optional -48V DC power supplies

IBS10G-SR - Supports Short Range Fiber 10 Gigabit Ethernet (Base-SR).

IBS10G-LR - Supports Long Range Fiber 10 Gigabit Ethernet (Base-LR).

IBSG-SX - Supports Short Range Fiber Gigabit Ethernet (1000Base-SX).

IBSG-LX - Supports Long Range Fiber Gigabit Ethernet (1000Base-LX).

IBSG-ZX - Supports Long Range Fiber Gigabit Ethernet (1000Base-ZX).



# 10.2 Bypass specifications

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

## 10.3 Product default specifications

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 /Tap / Linkdrop
Mode at Power Off:	Bypass
Heartbeat Packet:	Internetwork Packet Exchange

## 10.4 Technical specifications

#### 10.4.1 IBSH

10.4.1.1 IBS1U/IBS1UP: Bypass Switch 1U Host System Technical Specifications

Dockings:	Front holders
Voltage Input:	100-120/200-240VAC, 5/2.5A, 50/60Hz
Power Consumption:	100W maximum - for 4 switches
Size:	444mm x 339.3mm x 44 mm ( 17.48" x 13.358" x 1.732")
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 hour

10.4.1.2 IBS1U/IBS1UP: Bypass Switch 1U Host System LEDs / Connector Specifications

LEDs:	(2) Power LED – Green, Power is on, LED per power supply
Connectors:	

#### **10.4.2** *IBS10G-SR / IBS10G-SR*

#### 10.4.2.1 IBS1U/IBS1UP: Fiber Gigabit Ethernet Technical Specifications - (Base-SR) Adapters

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, Base-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
Output Transmit Power:	Typical: -2.6 dBm Minimum: -3 dBm
Optical Receive Sensitivity:	Typical: -14.6 dBm Maximum: -11.1 dBm
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
Power Consumption:	25W max.
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

10.4.2.2 LED and Connector Specifications

LEDs:	Network / Monitor ports: Link LED – (Green) On Link partner is detected. Activity LED – (Yellow) Blinks on activity.
	Power - Green power is on Normal – Green, Switch in Normal mode. SysOK – Yellow when Sys is OK, WDT – Blink Yellow when WDT is activated Light Yellow WDT time out Off: WDT is disabled Bypass - Red when bypass, off on Normal Alarm – Red on system alarm
Connectors:	Network: 2 LC Duplex Monitor: 2 SFP+ Management: RJ-11 serial port, RJ-45 1G copper Ethernet



#### **10.4.3** *IBS10G-LR / IBS10GP-LR*

10.4.3.1 Fiber Gigabit Ethernet Technical Specifications - (Base-LR) Adapters

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, Base-LR (1310nM)
Data Transfer Rate:	20Gbit/s in full duplex mode per port
Network ports Cables and Operating	Single mode fiber:
distance:	5000m maximum at 9 um **
Insertion Loss (Passive: Normal	Typical: 1.2 dB
Mode)	Maximum: 1.6dB
Insertion Loss ( Passive: Bypass	Typical: 1.2 dB
Mode)	Maximum: 1.6dB
Voltage:	12V
Power Consumption:	25W max.
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

10.4.3.2 LED and Connector Specifications

LEDs:	Network / Monitor ports: Link LED – (Green) On Link partner is detected. Activity LED – (Yellow) Blinks on activity.
	Power - Green power is on
	Normal – Green, Switch in Normal mode.
	SysOK – Yellow when Sys is OK,
	WDT – Blink Yellow when WDT is activated Light
	Off: WDT is disabled
	Bypass - Red when bypass, off on Normal
	Alarm – Red on system alarm
Connectors:	Network: 2 LC Duplex Monitor: 2 SFP+
	Management: RJ-11 serial port, RJ-45 1G copper
	Ethernet



## 1.1 IBSG –SX / IBSGP-SX

#### 1.1.1 Fiber Gigabit Ethernet Technical Specifications - (1000Base-SX) Adapters:

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, 1000Base-SX (850nM)
Data Transfer Rate:	2Gbit/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	Typical: 0.8 dB
Mode)	Maximum: 1.9 dB
Insertion Loss ( Passive: Bypass	Typical: 0.8 dB
Mode)	Maximum: 1.9 dB
Voltage:	12V +/-5%
Size:	173.3mm x 164.9mm x 20 mm ( 6.822" x 6.73" x 0.787") 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
MTBF*:	> 150,000 hours

1.1.2 LED and Connector Specifications

LEDs:	Network / Monitor ports:
	Link LED – (Green) On Link partner is detected.
	Activity LED – (Yellow) Blinks on activity.
	Power - Green power is on
	Normal – Green, Switch in Normal mode.
	SysOK – Yellow when Sys is OK,
	WDT – Blink Yellow when WDT is activated Light
	Yellow WDT time out
	Off: WDT is disabled
	Bypass - Red when bypass, off on Normal
	Alarm – Red on system alarm
Connectors:	Network: 2 LC Duplex
	Monitor: 2 SFP
	Management
	RJ-11 serial port
	RJ-45 Ethernet // optional for future use



## 1.2 IBSG-LX / IBSGP-LX

#### 1.2.1 Fiber Gigabit Ethernet Technical Specifications - (1000Base-LX) Adapters:

IEEE Standard / Network topology:	Fiber Gigabit Ethernet, 1000Base-LX (1310nM)
Data Transfer Rate:	2Gbit/s in full duplex mode per port
Network ports Cables and	Single mode fiber:
Operating distance:	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%
Size:	173.3mm x 164.9mm x 20 mm ( 6.822" x 6.73" x 0.787")
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

1.2.2 LED and Connector Specifications

LEDs:	Network / Monitor ports:	
	Link LED – (Green) On Link partner is Detected.	
	Power - Green power is on	
	Normal – Green, Switch in Normal mode.	
	SysOK – Yellow when Sys is OK, WDT – Blink Yellow when WDT is activated Light Yellow WDT time out Off: WDT is disabled	
	Bypass - Red when bypass, off on Normal Alarm –	
	Red on system alarm	
Connectors:	Network: 2 LC Duplex Monitor: 2 SFP Management: RJ-11 serial port RJ-45 Ethernet // optional for future use	



# 10.5 Appendix D: Order Information:

IBS IBSP	System Format	Media	Media Type	Power Supply and power Cord	-R
IBS: Intelligent Bypass Switch	1U: 1U 1UP: 1U unit (with power supply trap capabilities)	1G: 1Gb 1GP: 10Gb (with power supply trap capabilities) 10G: 10Gb 10GP: 10Gb (with power supply trap capabilities)	SR: 10G Short Range SX: 1G Short Range LR: 10G Long Reach LX: 1G Long Reach ER: 10G Extended Reach EX: 1G Extended Reach T- Copper 1000BASE-T	Power Cord -US -EU -CN -48V	ROHS
			100BASE-T 10BASE-T		



P/N	Description	Note
IBS10GP-SR	10 Gigabit (SR) fiber Intelligent Bypass Switch	Multimode fiber:62.5um, module only
IBS10GP-SR	10 Gigabit (SR) fiber Intelligent Bypass Switch	Multimode fiber:62.5um, module only (with power supply trap capabilities)
IBS10GP-SR5	10 Gigabit (SR) fiber Intelligent Bypass Switch	Multimode fiber:50um , module only
IBSGP-SX	Gigabit Fiber (SX) Intelligent Bypass Switch	Multimode, fiber:62.5um , module only
IBSGP-T	Gigabit Copper Intelligent Bypass Switch	1000BASE-T , 100BASE- T , 10BASE-T , module only (with power supply trap capabilities)
IBS10GP-LR	10 Gigabit (LR) fiber Intelligent Bypass Switch	Singlemode, fiber:62.5um , module only
IBS10GP-ER	10 Gigabit (ER) fiber Intelligent Bypass Switch	ER on the Network and Monitor ports.
IBS10GP-ERSR	10 Gigabit (ER) fiber Intelligent Bypass Switch	ER on the Network ports, SR on the Monitor ports
IBS1UP-US	Intelligent Bypass Switch 1U host system	1U host system,(90-240 VAC Auto-Select), US cable
IBS1UP-EU	Intelligent Bypass Switch 1U host system	1U host system,(90-240 VAC Auto-Select), EU cable
IBS1UP-EU	Intelligent Bypass Switch 1U host system	1U host system,(90-240 VAC Auto-Select), EU cable . (with power supply trap capabilities)
IBS1UP-CN	Intelligent Bypass Switch 1U host system	1U host system,(90-240 VAC Auto-Select), CN cable
IBS1UP-48	Intelligent Bypass Switch 1U host system	1U host system,(-75 36) VDC
IBS10G1UP-1SR-EU	1U w/ 10 Gigabit Fiber (SR) Intelligent Bypass Switch	Multimode fiber:62.5um , 1U host, EU cable
IBSG1UP-1SX-EU	1U w/ Gigabit Fiber (SX) Intelligent Bypass Switch	Multimode fiber:62.5um,, 1U host, EU cable
IBSG1UP-1SX-EU	1U w/ Gigabit Fiber (SX) Intelligent Bypass Switch	Multimode fiber:62.5um , 1U host, EU cable, (with power supply trap capabilities)
IBS10G1UP-1SR5-EU	1U w/ 10 Gigabit Fiber (SR) Intelligent Bypass Switch	Multimode fiber:50um , 1U host, EU cable
IBS10G1UP-1LR-US	1U w/ 10 Gigabit Fiber (LR)) Intelligent Bypass Switch	Single mode, 1U host, US cable
IBS10G1UP-1LR-US	1U w/ 10 Gigabit Fiber (LR)) Intelligent Bypass Switch	Single mode, 1U host, US cable. (with power supply trap capabilities)
IBS10G1UP-1LR-CN	1U w/ 10 Gigabit Fiber (LR)) Intelligent Bypass Switch	Single mode, 1U host, CN cable



IBS10G1UP-1LR-48	1U w/ 10 Gigabit Fiber (LR)) Intelligent Bypass Switch	Single mode, 1U host, -48V redundant power supply
IBS10G1UP-1ER-EU	1U w/ 10 Gigabit Fiber (ER)) Intelligent Bypass Switch	10G – ER on the Network and Monitor ports, 1U host, EU cable
IBS10G1UP-1ERSR-US	1U w/ 10 Gigabit Fiber (ER)) Intelligent Bypass Switch	10G – ER on the Network ports, SR on the Monitor ports , 1U host, US cable
IBS10G1UP-2SR-EU	1U w/ Two 10 Gigabit (SR) Intelligent Bypass Switch	2 x Multimode fiber:62.5um , 1U host, EU cable
IBS10G1UP-2SR-48	1U w/ Two 10 Gigabit (SR) Intelligent Bypass Switch	2 x Multimode fiber:62.5um , 1U host, -48V redundant power supply
IBS10G1UP-2SR5-EU	1U w/ Two 10 Gigabit (SR) Intelligent Bypass Switch	2 x Multimode fiber:50um , 1U host, EU cable
IBS10G1UP-1LR-1SR	1U w/ Two 10 Gigabit Intelligent Bypass Switch. One (LR) and one (SR)	1 x Single mode, 1x Multimode, 1U host, EU cable



#### 10.6 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 the 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.

10.6.1 Safety considerations for the IBS rack mounting:

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

B. Verify that a sufficient clear space is provided around the IBS unit to allow sufficient 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 IBS 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.

Version 3.5 Page 139 of 146
10.7 TFTP server installation and configuration.
10.7.1 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)

10.7.2 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 the 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



This document is for informational purposes only. The information in this document, believed by Garland Technology to be accurate as of the date of publication, is subject to change without notice. Garland Technology assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains. ©2020 Garland Technology LLC. All Rights Reserved

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.

Networks Associates Technology, Inc copyright notice (BSD) -----Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved. Cambridge Broadband Ltd. copyright notice (BSD) -----Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved. Sun Microsystems, Inc. copyright notice (BSD) -----Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved. Sparta, Inc copyright notice (BSD) -----Copyright (c) 2003-2006, Sparta, Inc All rights reserved. Cisco/BUPTNIC copyright notice (BSD) -----Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. All rights reserved. Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003 Copyright 2000,2001 by Roman Volkov

> For questions, please contact Garland Technology Support at: 8AM-9PM (CST) Monday - Friday (Except for observed US Holidays) Tel: 716.242.8500 Online: www.garlandtechnology.com/support

> > Garland Technology: Modular Bypass System Firmware Rev Level: 0.3.3.2

> > > Office: 716-242-8500 garlandtechnology.com/support garlandtechnology.com