

# Garland Technology

## EdgeSafe™: 100G Bypass Modular Network TAP User Guide

M100G1AC, M100G1DC



See every bit, byte, and packet®

Office: 716-242-8500  
[support@garlandtechnology.com](mailto:support@garlandtechnology.com)  
[garlandtechnology.com](http://garlandtechnology.com)

Copyright © 2021 Garland Technology, LLC. All rights reserved.

No part of this document may be reproduced in any form or by any means without prior written permission of Garland Technology, LLC.

The Garland Technology trademarks, service marks ("Marks") and other Garland Technology trademarks are the property of Garland Technology, LLC. EdgeSafe Series products of marks are trademarks or registered trademarks of Garland Technology, LLC. You are not permitted to use these Marks without the prior written consent of Garland Technology.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Notice

The purchased products, services and features are stipulated by the contract made between Garland Technology and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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

## 1. Introduction

The Garland Technology's EdgeSafe Bypass TAP (hereafter referred to as the M100G1AC) is an active external bypass switch that protects network integrity from network failures and enhances network maintenance. It generates heartbeat packets, and by detecting the flow of heartbeat packets, it controls the operation mode of the network.

A Garland M100G1AC 1U Unit is a 1U host system which supports up to two 100G modules. A 100G module supports one segment.

The following figure shows a Garland M100G1AC 1U Unit with two 100G modules.



Figure 1. M100G1AC 1U Unit with two 100G modules

The M100G1AC supports 100 Gigabit Ethernet Multi-mode Fiber (100GBase-SR4 and 100GBase-SR10) and 100 Gigabit Single-mode Fiber (100GBase-LR4) network standards. Either 100G module includes two MPO/LC ports for network connection and two CFP4/CXP ports for the attached inline network system.

The following table explains the items in a Garland M100G1AC 1U Unit shipment package. Depending on your order, your shipment package comes with a 1U host system and one or two 100G modules.

<b>M100G1AC</b>	<b>Number of Modules</b>	<b>Module type</b>	<b>Power supply</b>	<b>Power cord</b>
Intelligent 100G Switch 1U Box	1: One module 2: Two modules	100G module with bypass will show BCSR4 BCLR4 BCSR10	Blank: 90-240 V AC, Redundant - hot swap - 48V DC	Blank: No power cord -EU -US -CN

The following table explains different models of the Garland M100G1AC 1U Unit.

<b>Part number (P/N)</b>	<b>Description</b>
M1001Gxx	Bypass Switch 1U Host System
M100GSR10BP	4 ports 100 Gigabit CFP4 (SR4) fiber Intelligent Bypass Switch module
M100GSR4BP	M100G1AC with one bypass segment - SR4
M100GLR4BP	M100G1AC with one bypass segment - LR4

## 2. Features and specifications

This chapter introduces the key features, bypass specifications, and default configurations of the M100G1AC.

### 2.1 Key features

The following sections explain the key features of M100G1AC.

#### 2.1.1 Supported operation modes

The M100G1AC supports four modes of operation: **Inline**, **Bypass**, **TAP** and **Linkdrop**.

- In **Inline** mode, the M100G1AC diverts the network traffic to the attached inline network system. This is the normal operation mode.
- In **Bypass** mode, the M100G1AC diverts the network traffic to another network system instead of the attached inline network system.
- In **TAP** mode, the M100G1AC mirrors incoming traffic in port Net0 to port Mon0 and incoming traffic in port Net1 to port Mon1.
- In **Linkdrop** mode, the M100G1AC disables the links on both network ports (Net0, Net1). It simulates switch/router cable disconnection.

## 3. For detailed description of operation modes, see Chapter 4. Theory of operation System management overview

A user can use a username and password to access the M100G1AC management interface via COM, SSH or Web. The initial user name is **admin** and the default password is **Garland2015**.

The M100G1AC supports multiple users' login.

The M100G1AC defines three types of user privileges to restrict user access:

- **Admin**: Full read-write access to all configurations (**Bypass Configuration/System/User/ SNMP**); privileges to add, delete, or modify local users on the M100G1AC. The initial user account **admin** is the only administrator account and no other administrator accounts are allowed to be created. This administrator account cannot be deleted, and the privileges cannot be modified.
- **Normal**: Full read-write access to **Bypass Configurations** and read-only access to other configurations (**System/User/SNMP**).
- **Readonly**: Read-only access to all configurations.

The **Admin** user can change everyone's password. The **Normal** users and Readonly users can change only their own password.

### 3.1.1 Garland Technology Double Bypass Safe architecture

The M100G1AC is designed with the Garland Technology Double Bypass Safe architecture, which is based on two bypass routing circuitries: an active bypass routing circuitry and a passive bypass routing circuitry. When the active one fails, the passive one will be activated.

### 3.1.2 Configuration methods

The M100G1AC can be configured through the following methods:

- Simple command line interface (CLI), via a serial communication console port and an Ethernet port using SSH
- Simple Web management interface
- Simple Network Management Protocol (SNMP)

### 3.1.3 Centralized management

The M100G1AC performs centralized management to all bypass segments in the system.

### 3.1.4 Power supplies

The M100G1AC comes with two redundant 90-240 V AC power supplies or two redundant -48 V DC power supplies.

### 3.1.5 Summary of key features

The following list summarizes the key features of the M100G1AC:

Self-generating heartbeat packets - No driver or management port is required to generate pulses.

- Sets to Bypass when inline system failure is detected
- Sets to Bypass when inline system link failure is detected
- Sets to Bypass when inline software application system hang is detected
- Sets to Bypass on power failure
- Sets to Inline when inline system recovery is detected
- Double Safe Bypass architecture with two routing circuitries
- Centralized management
- Two on board Watch Dog Timer (WDT) controllers
- Software programmable timeout interval
- Enable/Disable software programmable WDT
- Independent Inline/Bypass/Tap/Linkdrop operation in every module
- Supports up to two 100G Bypass segments in a 1U chassis
- Simple command line interface for configuration via serial port
- SSH management interface via network management port
- Web GUI management interface via network management port
- Supports SNMP versions 1, 2c, 3 (SHA, AES)
- Supports remote log
- Support RADIUS
- Supports TACACS+
- Supports NTP
- Supports time zone
- Supports multi configuration backup
- Supports two-port link feature
- Two redundant power supplies

- Optional: - 48V dc power supplies

## M1001Gxx

- Supports Short Range Fiber 100 Gigabit Ethernet (100GBase-SR4 50um).

## M1001Gxx

- Supports Long Reach Fiber 100 Gigabit Ethernet (100GBase-LR4).

## M1001Gxx

- Supports Short Range (100m) Fiber 100 Gigabit Ethernet with Optical module CXP (100GBase-SR10).

### 3.2 Bypass specifications

Item	Description
<b>WDT interval (software programmable)</b>	<p>Routing Transmit heartbeat packets every 3ms - 10sec (Default: 5ms) Verify packets received every 10ms - 50sec (Default: 20ms)</p> <p>Double Bypass Transmit heartbeat packets every 300ms - 60sec (Default: 7sec) Verify packets received every 1S - 253sec (Default: 20sec)</p>

### 3.2 Bypass specifications

Item	Default configuration
<b>Mode at power-up</b>	Bypass
<b>Heartbeat</b>	Activated
<b>Bypass switch is ready and inline device responds to heartbeat</b>	Change to Inline
<b>Inline device responds to heartbeat</b>	Normal
<b>Inline device does not forward heartbeat</b>	Bypass
<b>Mode at power-off</b>	Bypass
<b>Heartbeat packet</b>	Internetwork Packet Exchange

## 4. System management overview

A user can use a username and password to access the M100G1AC management interface via COM, SSH or Web. The initial user name is **admin** and the default password is **Garland2015**.

The M100G1AC supports multiple users' login.

The M100G1AC defines three types of user privileges to restrict user access:

- Admin: Full read-write access to all configurations (Bypass Configuration/System/User/ SNMP); privileges to add, delete, or modify local users on the M100G1AC. The initial user account admin is the only administrator account and no other administrator accounts are allowed to be created. This administrator account cannot be deleted, and the privileges cannot be modified.
- Normal: Full read-write access to Bypass Configurations and read-only access to other configurations (System/User/SNMP).
- Readonly: Read-only access to all configurations.

The **Admin** user can change everyone's password. The **Normal** users and **Readonly** users can change only their own password.

The M100G1AC supports RADIUS/TACACS+ remote login. RADIUS and TACACS+ cannot be enabled at the same time. To enable either, the other needs to be disabled first.

RADIUS users share the same privilege level, which can be configured through Web or CLI.

TACACS+ user or user group privilege can be configured on server side by adding a service tag (default is "silc-system", which can be configured through Web or CLI) to tacacs+ server configuration as below:

```
service = silc-system {  
  
    # 1: readonly; 5: normal; 10: admin  
  
    user-privilege = 10  
}
```

And TACACS+ user will be assigned Readonly privilege if the service tag is missing in server configuration.



## 5. Theory of operation

### 5.1 Module and Segments

The M100G1AC bypass operation is provided at the segment level.

M100G1AC system can have a maximum of two modules, and each module may have a maximum of 1 100G

bypass segment.

In each M100G1AC bypass segment there are always 4 ports, two of them are named NET ports NET0 and NET1, and the other two ports are named MON ports MON0 and MON1.

The two external ports connected to the NET ports are usually switch or router ports, and we refer to them as **Router Ports** within the document.

The two external ports connected to the MON ports are usually from an **Inline Network Appliance** (A Firewall for example), and we refer to them as **Appliance Ports** within the document.

### 5.2 Modes of operation

Each bypass segment supports the following predefined operation modes

- Inline - the M100G1AC diverts the network traffic to the attached inline network system. This is the normal operation mode.
- Bypass - the M100G1AC diverts the network traffic to another network system instead of the attached inline network system.
- In TAP mode, the M100G1AC mirrors incoming traffic in port Net0 to port Mon0 and incoming traffic in port Net1 to port Mon1.
- In Linkdrop mode, the M100G1AC disables the links on both network ports (Net0, Net1). It simulates switch/router cable disconnection.

By default, the M100G1AC operate in Inline mode. When traffic is received on the NET ports, it will be forwarded to the **Appliance Ports** via the corresponding MON ports. The network appliance will need to work like a network bridge for the two **Router ports** to communicate with each other.

Each bypass segment in inline mode will continuously transmit pre-defined heartbeat packets to the Appliance Ports via the MON ports. When receiving a heartbeat packet from one of the MON ports, the Inline Network appliance will need to forward it to the other MON ports, to bridges the heartbeat packet. As long as the M100G1AC detects the flow of heartbeat packets, it stays in **Inline** mode.

When one of the following events occurs, the **Inline Network Appliance** fails to receive or forward the heartbeat packets, and the M100G1AC will not be able to detect the flow of heartbeat packets, then the M100G1AC

switches from Inline mode to **Active Bypass, TAP, or Linkdrop** mode according to the predefined settings of the **Heartbeat Active Expire OP Mode** parameter:

- Application failure
- Monitor link is down
- Power failure (Will switch to Passive bypass or LinkDrop).
- User's request to bypass the heartbeat packets manually

When the **Inline Network Appliance** recovers and resumes heartbeat packet transmission and the M100G1AC will switch back to **Inline** mode.

### 5.2.1 Inline mode

The following diagram illustrates the working mechanism of **Inline** mode.  
The network appliance can then choose to reject packets received or inject packets into the network.

Since that network appliance may have down time, so it will affect the connection between the two external Switch/router ports. This is where heartbeat and bypass mode will help.

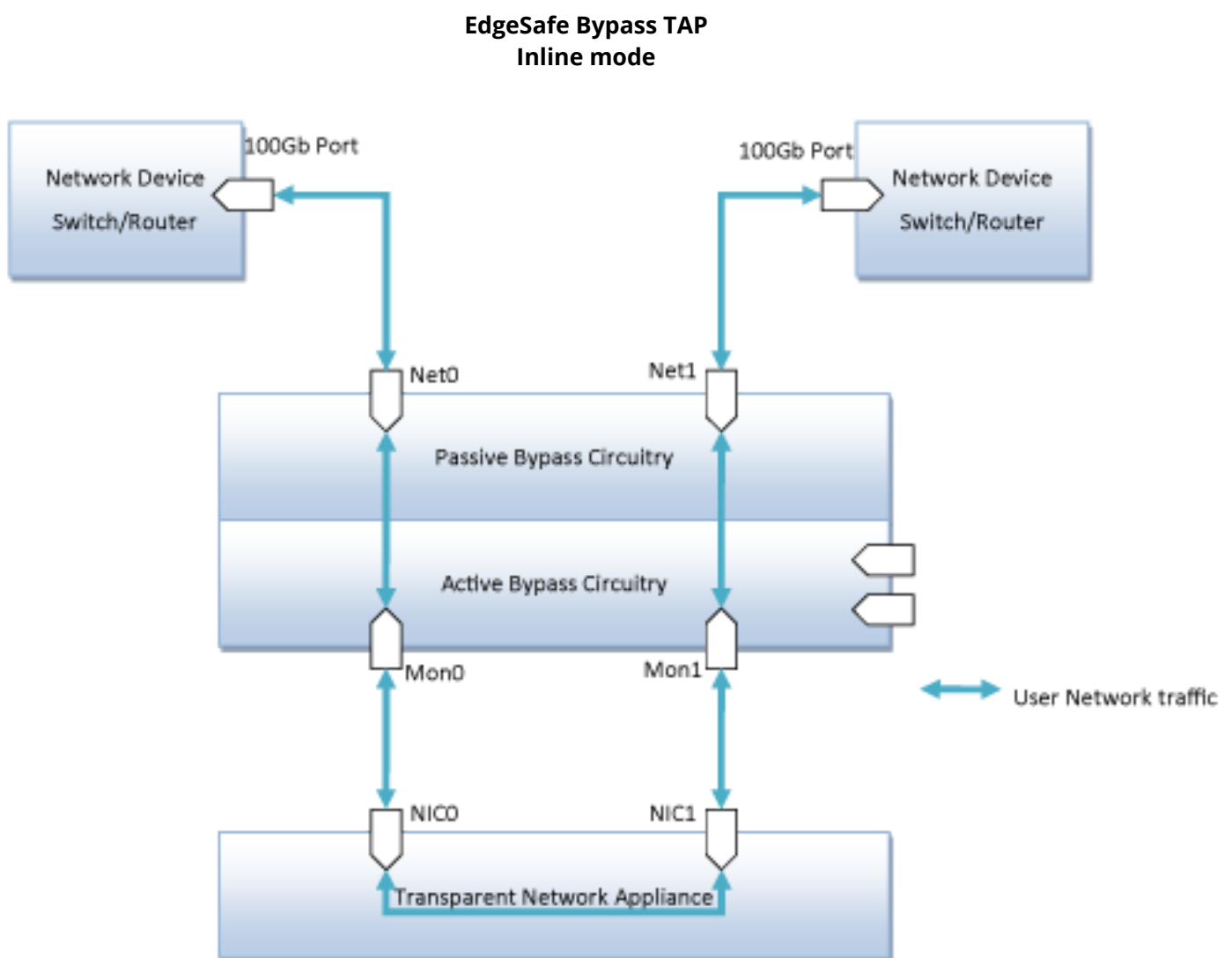
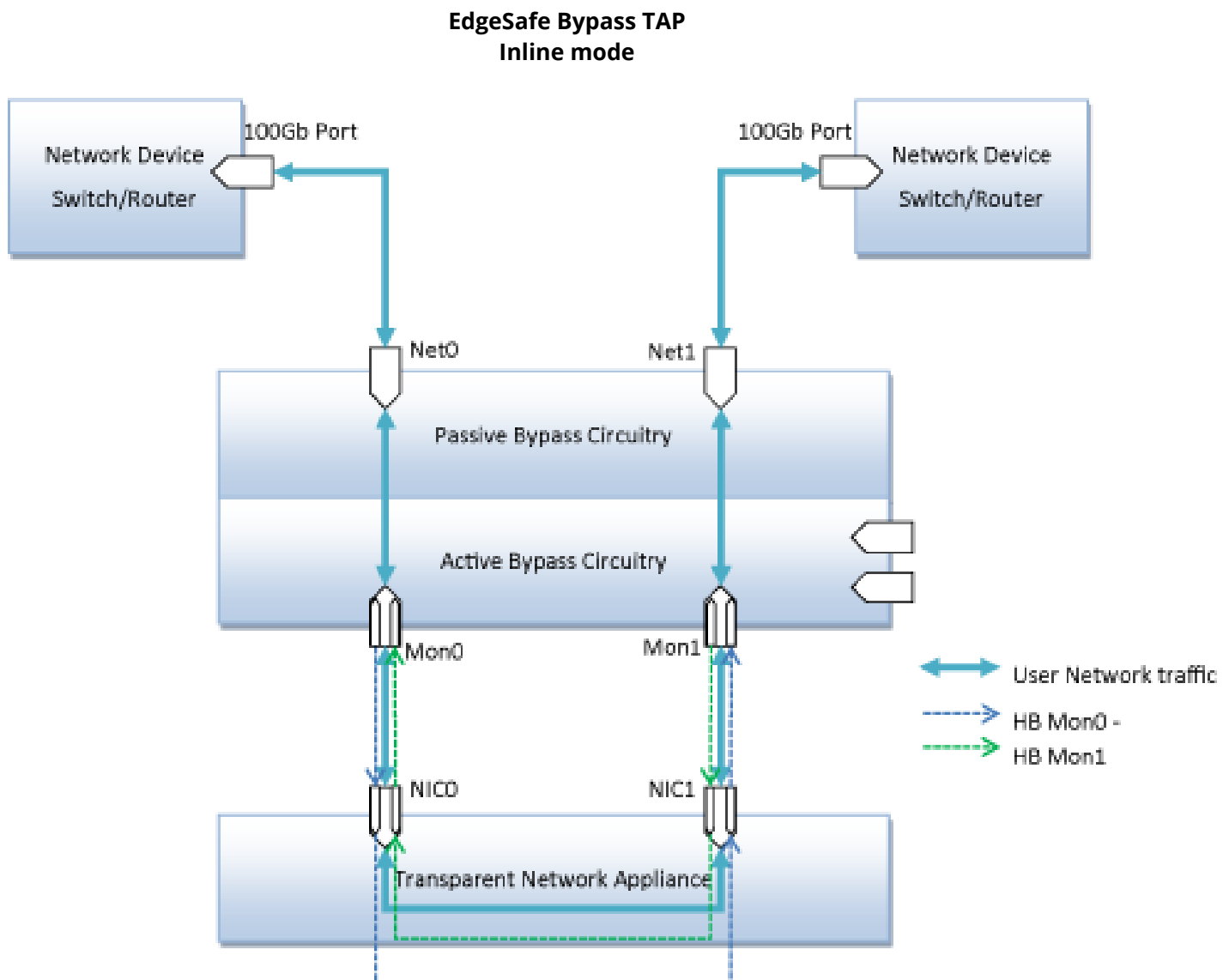


Figure 2. M100G1AC Inline mode

### 5.2.2 Inline mode with heartbeat checking

In event of an application failure (including power failure of the monitor/network device), the monitor/network device stops transmitting the heartbeat packets, and the M100G1AC will not be able to detect the flow of heartbeat packets, then the M100G1AC switches from **Inline** mode to **Active Bypass**, **TAP**, or **Linkdrop** mode according to the predefined settings of the **Heartbeat Active Expire OP Mode** parameter.

In **Active Bypass** or **TAP** mode, the network traffic continues to flow through the network ports and is not diverted to the monitor ports. As soon as the monitor/network device recovers and resumes transmitting the heartbeat packets, the M100G1AC resumes **Inline** mode after detecting the heartbeat packets for a period of time set by the **hb\_holdtime** parameter.



### 5.2.3 Bypass Mode (Active Bypass Mode)

The following diagram illustrates the working mechanism of **Bypass** mode or Active Bypass mode.

In this mode, traffic will bypass the M100G1AC device, which means packets received from Net0 port will be forwarded to the device connected to NET1 port, Packets received from Net1 port will be forwarded to the device connected to NET0 port. The mode is also called Active Bypass mode, as packets are actually going through the switch circuitry.

**EdgeSafe Bypass TAP  
Bypass mode**

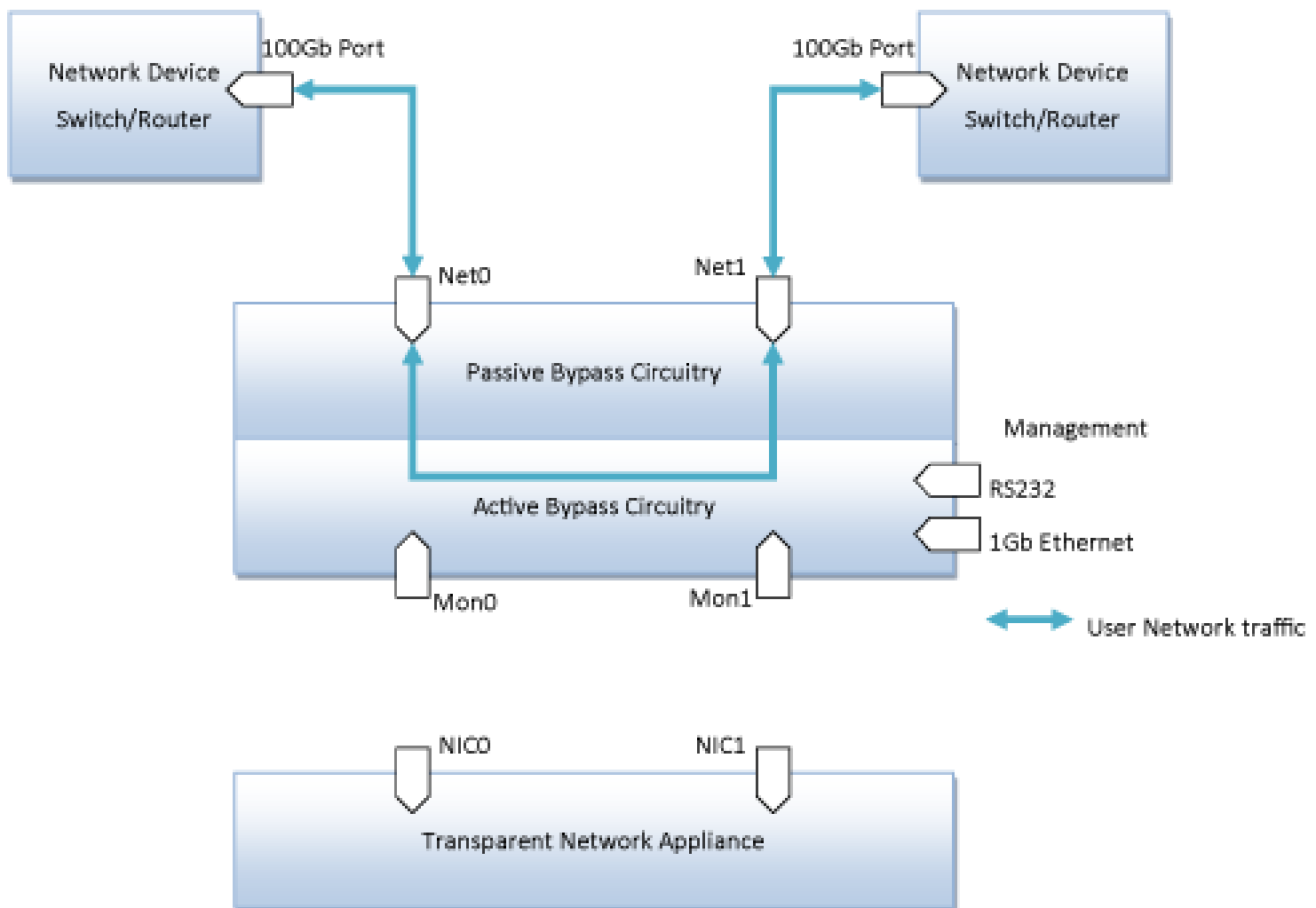


Figure 4. M100G1xx Heartbeat detection with Bypass mode

### 5.2.4 Passive Bypass and Power failure

In event of a power failure, the M100G1AC bypasses the Ethernet ports by switching to **Passive Bypass** mode.

The network traffic continues to flow through the network ports but is not diverted to the monitor ports. When power is restored, the M100G1AC resumes **Inline** mode after detecting the heartbeat packets for a period of time set by the **Heartbeat Expire Timer** parameter.

**Note:** The **Heartbeat Expire Timer** parameter can be change via management port from their initial default value.

The following diagram illustrates the working mechanism of **Passive Bypass** mode.

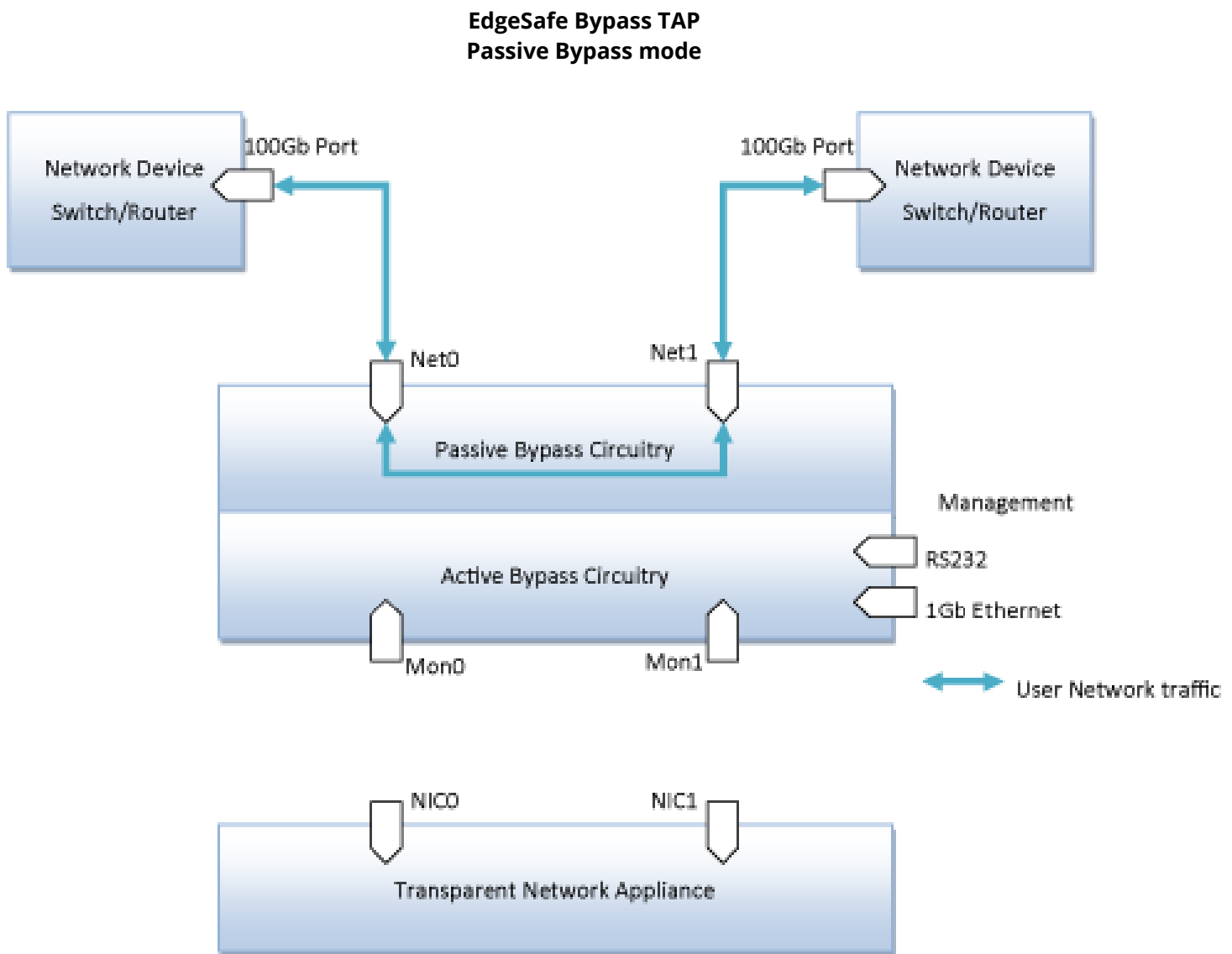


Figure 5. M100G1xx Passive Bypass mode

### 5.2.5 TAP mode

In **TAP** mode, incoming traffic in port Net0 is mirrored to port Mon0 and incoming traffic in port Net1 is mirrored to port Mon1.

The following diagram illustrates the working mechanism of **TAP** mode.

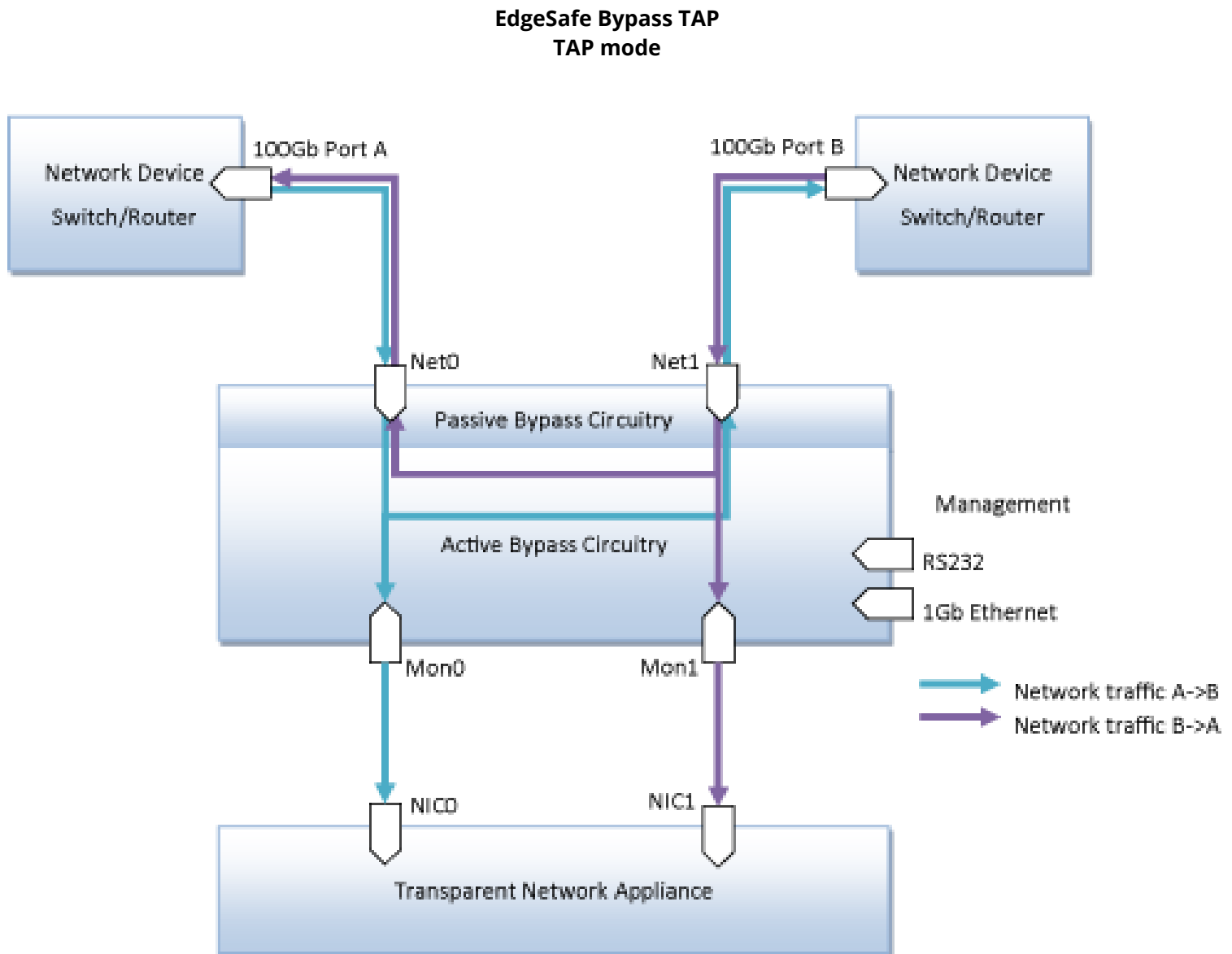


Figure 6. M100G1xx TAP mode

### 5.2.6 TAPI12 mode

When TAPI12 mode 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.

The following diagram illustrates the working mechanism of **TAPI12** mode.

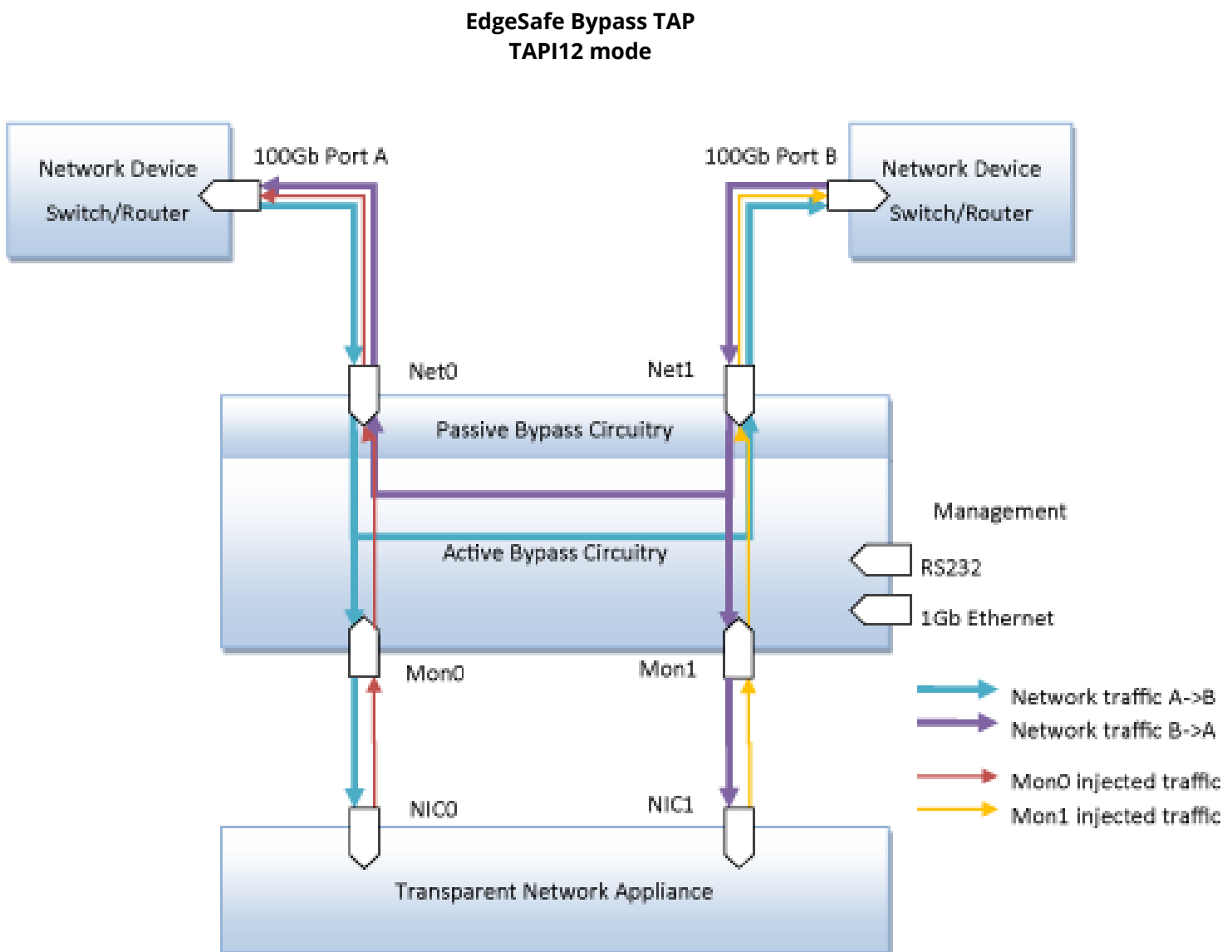


Figure 7. M100G1xx TAPI12 mode

### 5.2.7 TAPA mode

When TAPA mode is enabled, incoming traffic in port Net0 is mirrored to both monitor ports (Mon0, Mon1) and incoming traffic in port Net1 also is mirrored to both monitor ports (Mon0, Mon1).

The following diagram illustrates the working mechanism of **TAPA** mode.

**EdgeSafe Bypass TAP  
TAPA mode**

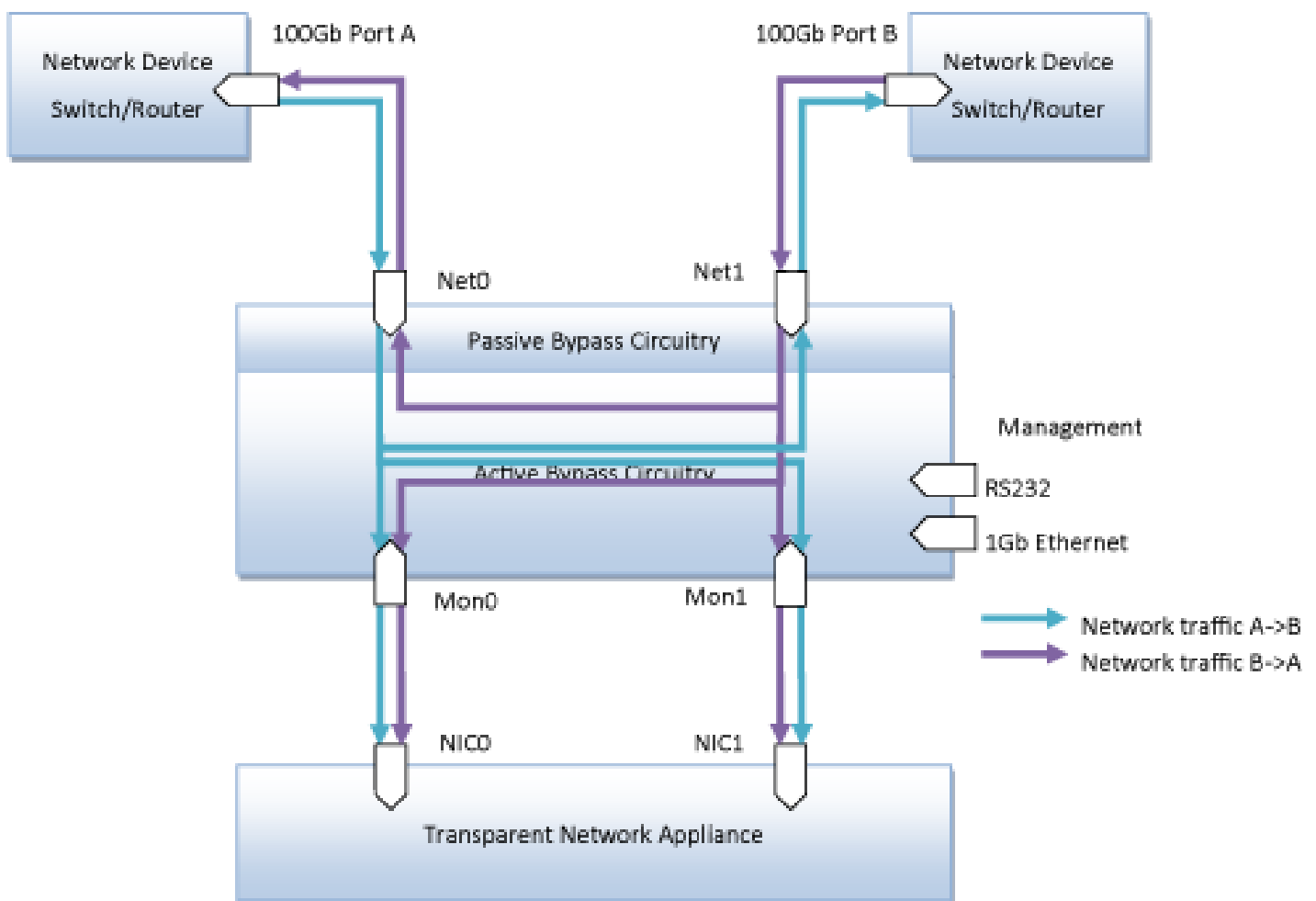


Figure 8. M100G1AC TAPA mode



### 5.2.8 TAPAI1 mode

When TAPAI1 mode is enabled, incoming traffic in port Net0 is mirrored to both monitor ports (Mon0, Mon1) and incoming traffic in port Net1 also is mirrored to both monitor ports (Mon0, Mon1). Packets can be injected from port Mon0. Injected packets from Mon0 will be sent to both network ports (Net0, Net1).

The following diagram illustrates the working mechanism of **TAPAI1** mode.

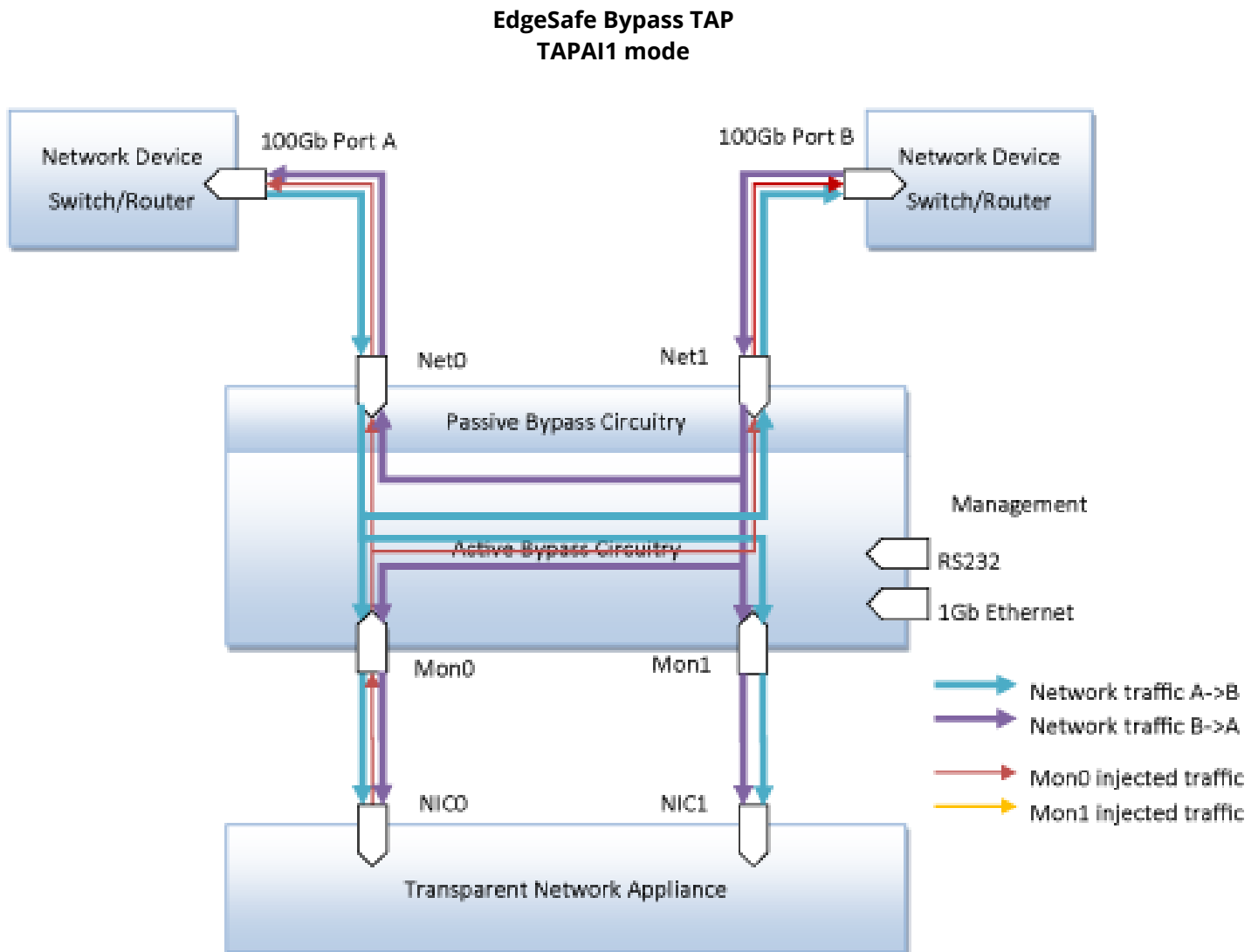


Figure 9. M100G1AC TAPAI1 mode

### 5.2.9 TAPAI2 mode

When TAPAI2 mode is enabled, incoming traffic in port Net0 is mirrored to both monitor ports (Mon0, Mon1) and incoming traffic in port Net1 also is mirrored to both monitor ports (Mon0, Mon1). Packets can be injected from port Mon1 to both network ports (Net0, Net1).

The following diagram illustrates the working mechanism of **TAPAI2** mode.

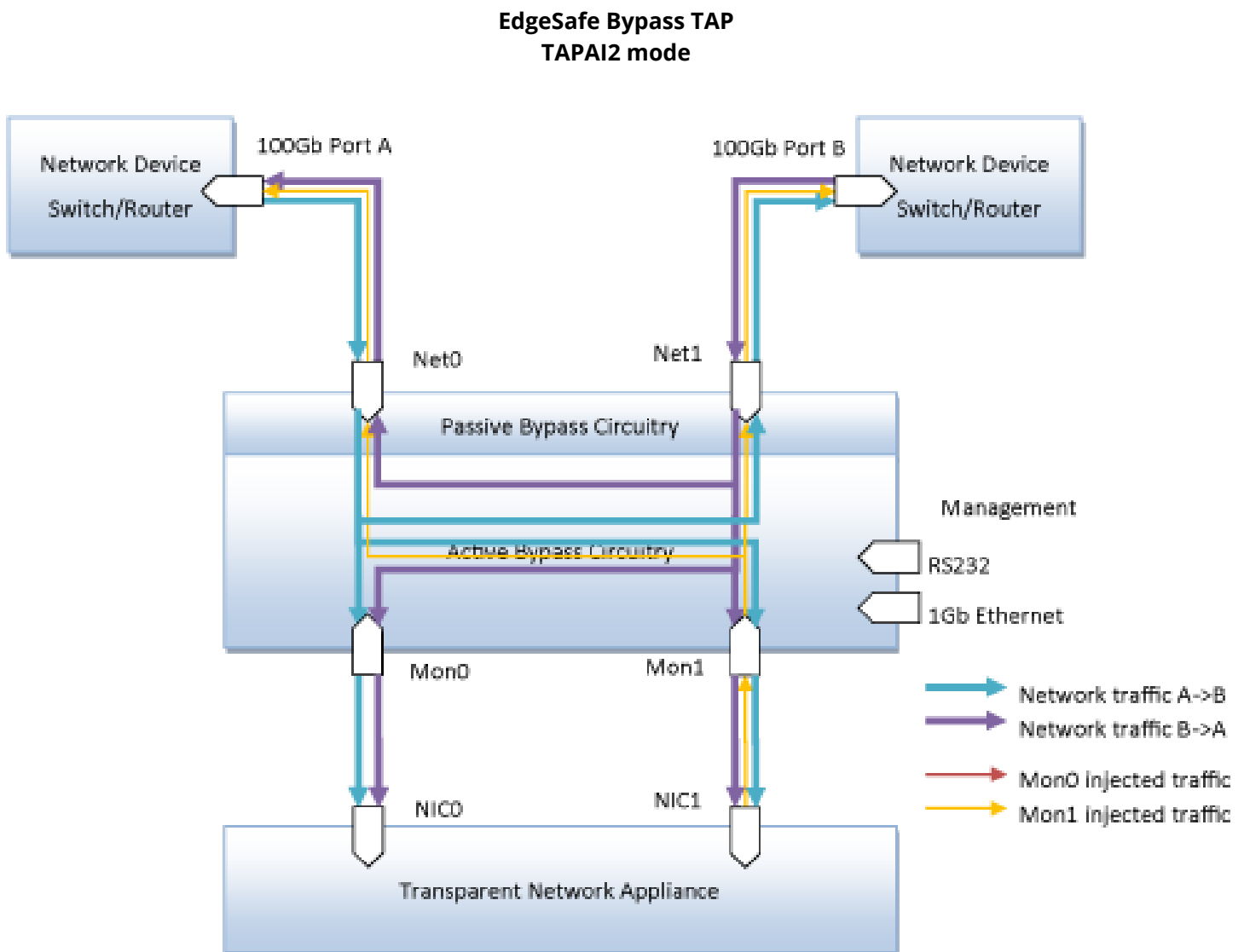


Figure 10. M100G1AC TAPAI2 mode

### 5.2.10 TAPAI12 mode

When TAPAI12 mode is enabled, incoming traffic in port Net0 is mirrored to both monitor ports (Mon0, Mon1) and incoming traffic in port Net1 also is mirrored to both monitor ports (Mon0, Mon1). Packets can be injected from each monitor port to both network ports (Net0, Net1).

The following diagram illustrates the working mechanism of **TAPAI12** mode.

**EdgeSafe Bypass TAP  
TAPAI12 mode**

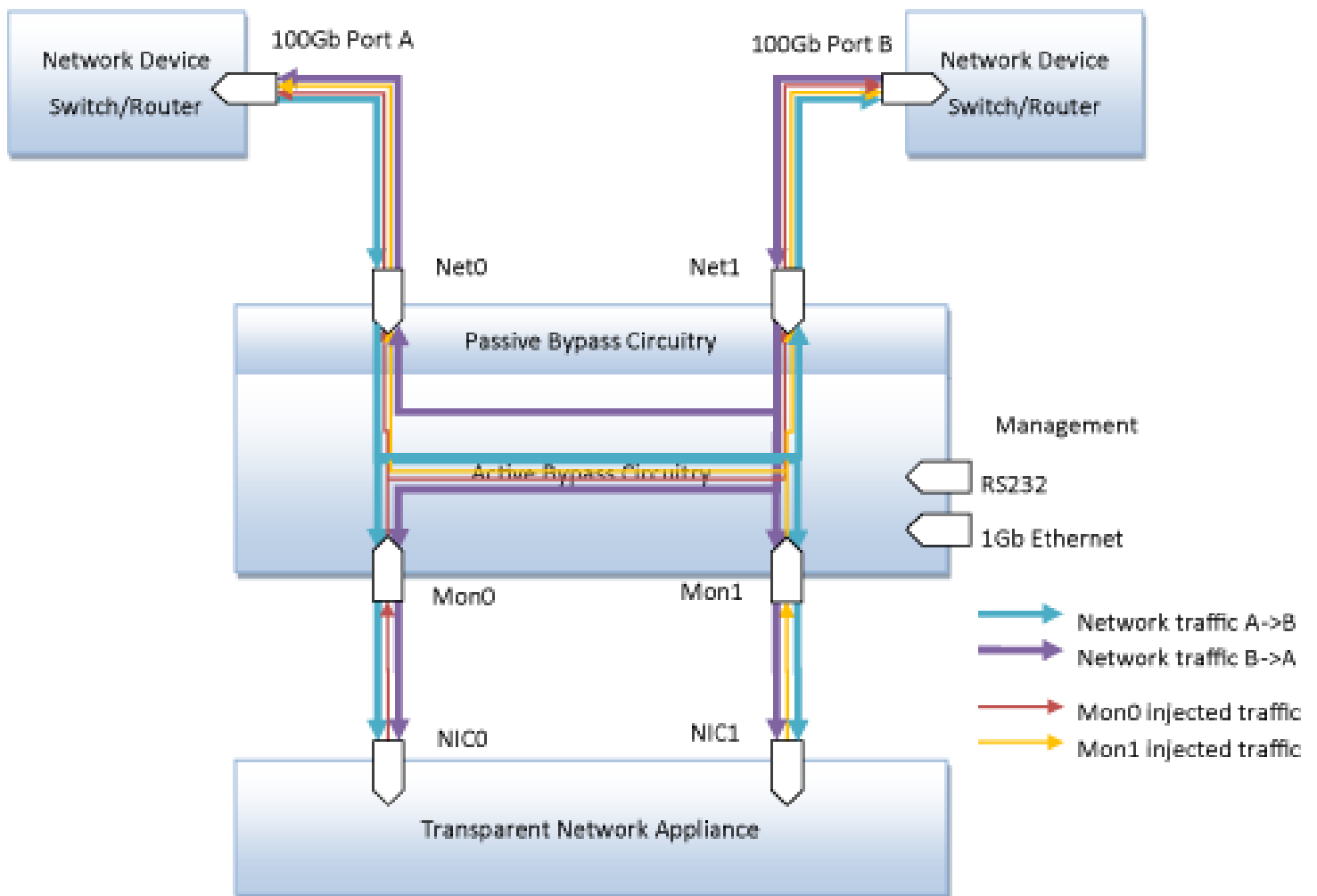


Figure 11. M100G1AC TAPAI12 mode

### 5.2.11 Linkdrop mode

In **Linkdrop** mode, the M100G1AC disables the link on both network ports (Net0, Net1). The M100G1AC simulates switch/router cable disconnection.

The following diagram illustrates the working mechanism of **Linkdrop** mode.

#### Linkdrop mode

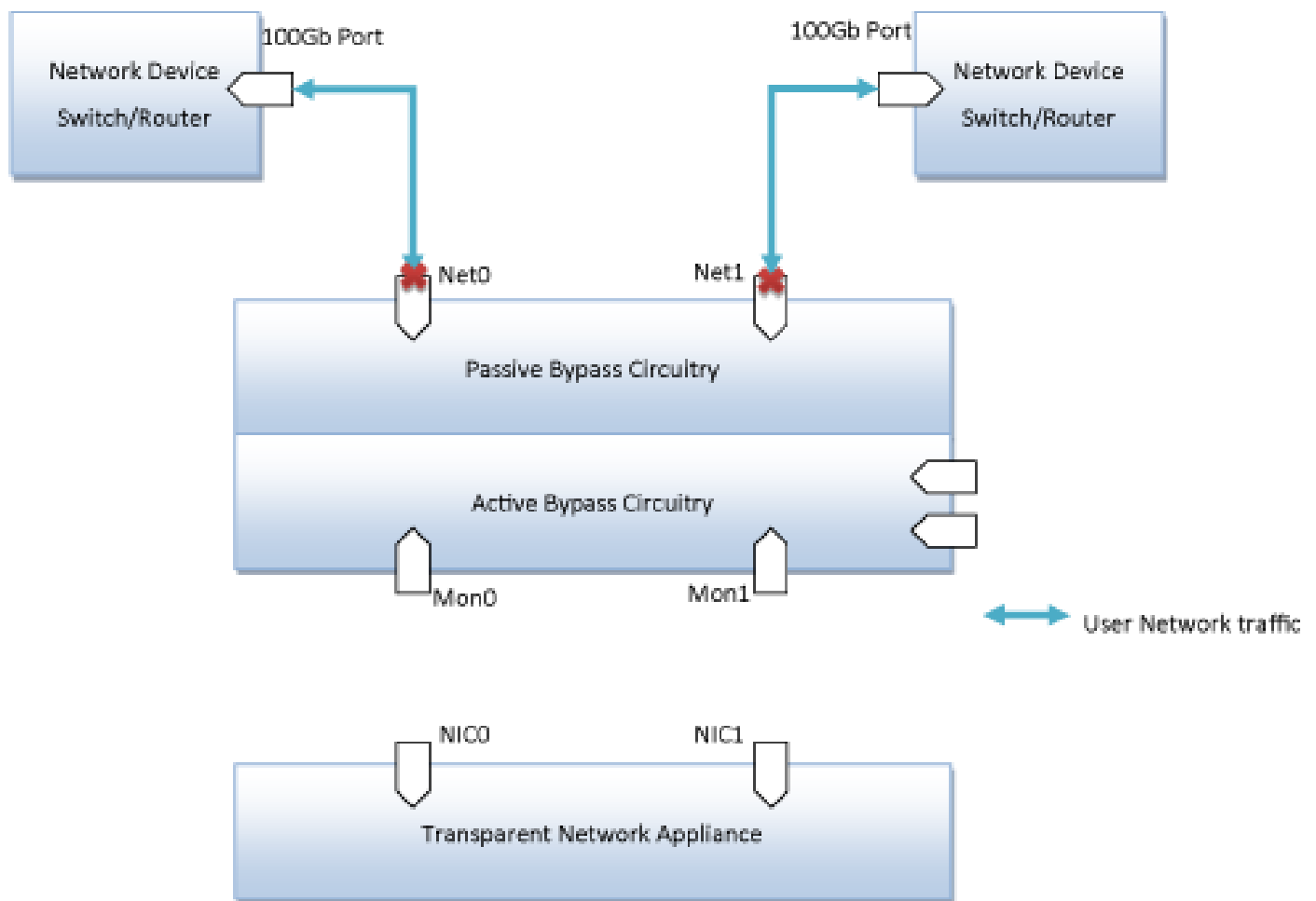


Figure 12. M100G1xx Linkdrop mode

## 5.3 Heartbeat Checking Mode

The Heartbeat Checking Mode is an Appliance aliveness detection mechanism that M1001Gxx system used to determine whether to switch from INLINE mode to BYPASS mode for the NET ports, in order to maintain traffic forwarding operation in the event of Transparent Network Appliance failures.

To turn on Heartbeat Checking, the user will need to enable **Heartbeat Active Mode**.

### 5.3.1 Heartbeat checking Logic

When **Heartbeat Active Mode** is enabled, M1001Gxx will send heartbeat packets from Mon ports to the connected Network Appliance periodically. When the Network Appliance receives heartbeat packet from one of the Mon ports, it is supposed to forward the received heartbeat packets to the other Mon port.

#### 5.3.1 Heartbeat checking Logic

The M100G1AC will be expecting continuous Heartbeat packet forwarding by the Network appliance to its Mon ports and will use this to determine the aliveness of the Network Appliance.

If the M100G1AC does not receive heartbeat packets forwarded by the Network Appliance from the Mon ports, the M100G1AC will set the **Application State** (as shown in the **Module Status** Page) to **Failed** and switch to **Active Bypass**, **TAP** or **Linkdrop** mode according to the predefined settings of the **Heartbeat Active Expired OP Mode** parameter.

#### 5.3.1.2 Application Active Restore

**Application Active Restore** is a configuration which determines whether M100G1AC will try to recover from an Application Failure.

When **Application Active Restore** is turned on, the M100G1AC will keep sending Heartbeat packet from its Mon ports to the connected Network Appliance in order to detect the recovery of the Network Appliance.

Upon receiving the forwarded heartbeat packet again on the Mon ports, the M100G1AC will start a application recovery sequence. The M100G1AC will expect heartbeat packets to be received consecutively within a timer defined by **Heartbeat Recover Timer** before it determines that the Network Appliance has indeed recovered, and the **Application State** will be set to **OK**.

If the **Heartbeat Recover Timer** is set to 0, than the **Application State** will be set to OK upon the receiving of the first heartbeat packet forwarded by the Network Appliance.

If the Application Active Restore is turned off, then M100G1AC will stay in the Application Failed state, and the operation mode will stay in either Bypass/LinkDrop/Tap as configured in **Heartbeat Active Expired OP Mode**. And also the M100G1AC will stop sending heartbeat packets to its Mon ports. It will need user intervention to resume the normal INLINE operation.

### 5.3.2 Monitor link failure

The Mon port link failure is treated the same as a heartbeat lost event. And if Heartbeat Active Mode is turned on, the **Application State** will be set to **Failed**, and the operation mode will be set to the mode as configured in **heartbeat Active Expired OP Mode**.

## 5.4 Additional features

This section lists some additional features of M100G1AC.

#### 5.4.1 Two-port Link (2PL)

The two-port link (2PL) feature logically connects the link of the two Net ports together. When the feature is enabled, if the link of any one of network ports fails, the link of the other network port will also be dropped.

When the port that has its link failed recovers from the link failure, the link of the other port will also be turned back on again.

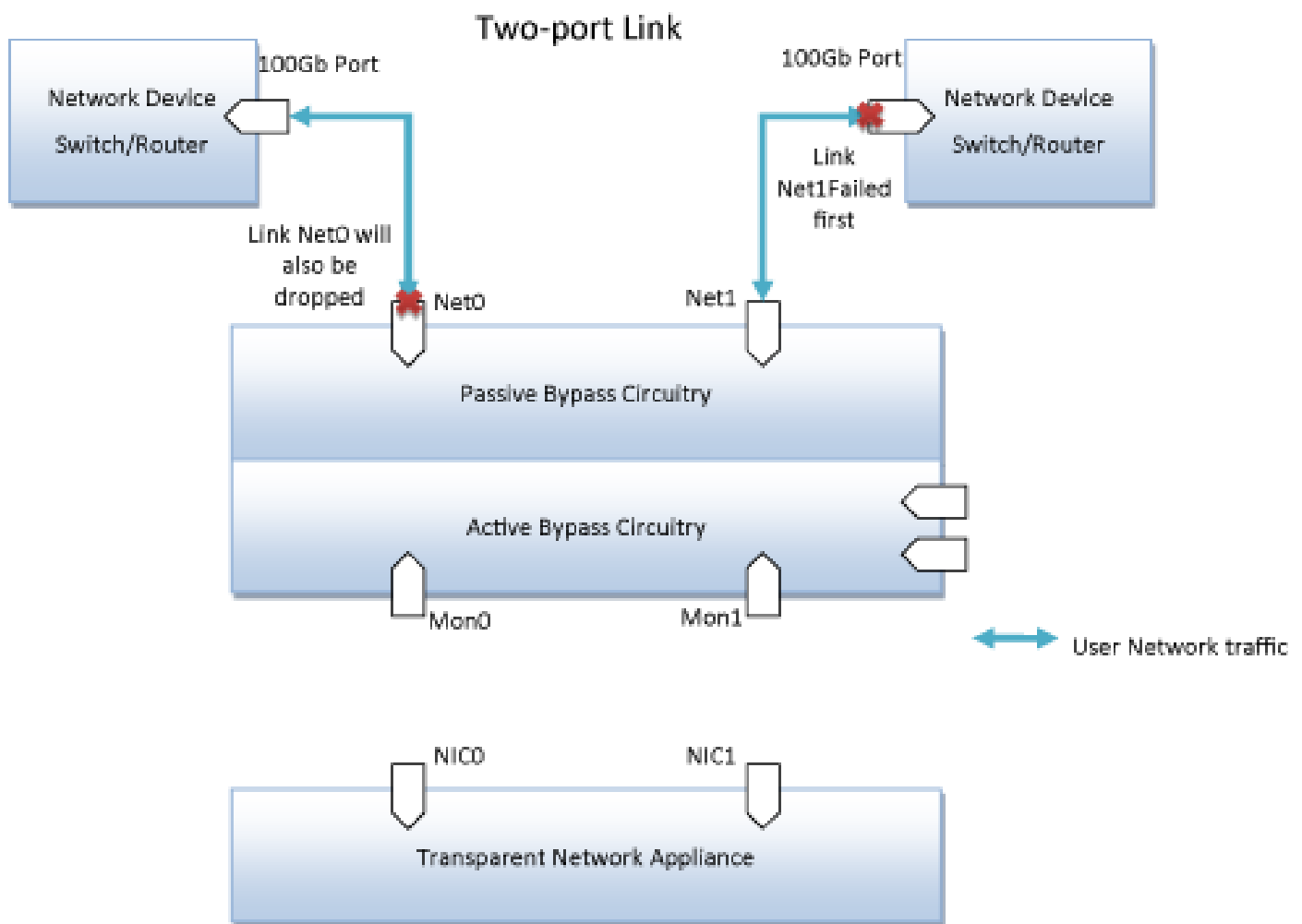


Figure 13. M1001Gxx Two-port Link(2PL) Illustration

#### 5.4.2 M2N

The M2N feature makes the link of a Net port to be in a slave state of its corresponding Mon ports. The M2N mode can be set independently on each monitor port. When enabled, if the link of the Mon port has failed, the link of the corresponding Net port will also be dropped.

This feature can be enabled with 2PL. When 2PL is enabled when M2N is also enabled on a Mon port, both NET ports will have their link dropped if the Mon port link has failed.

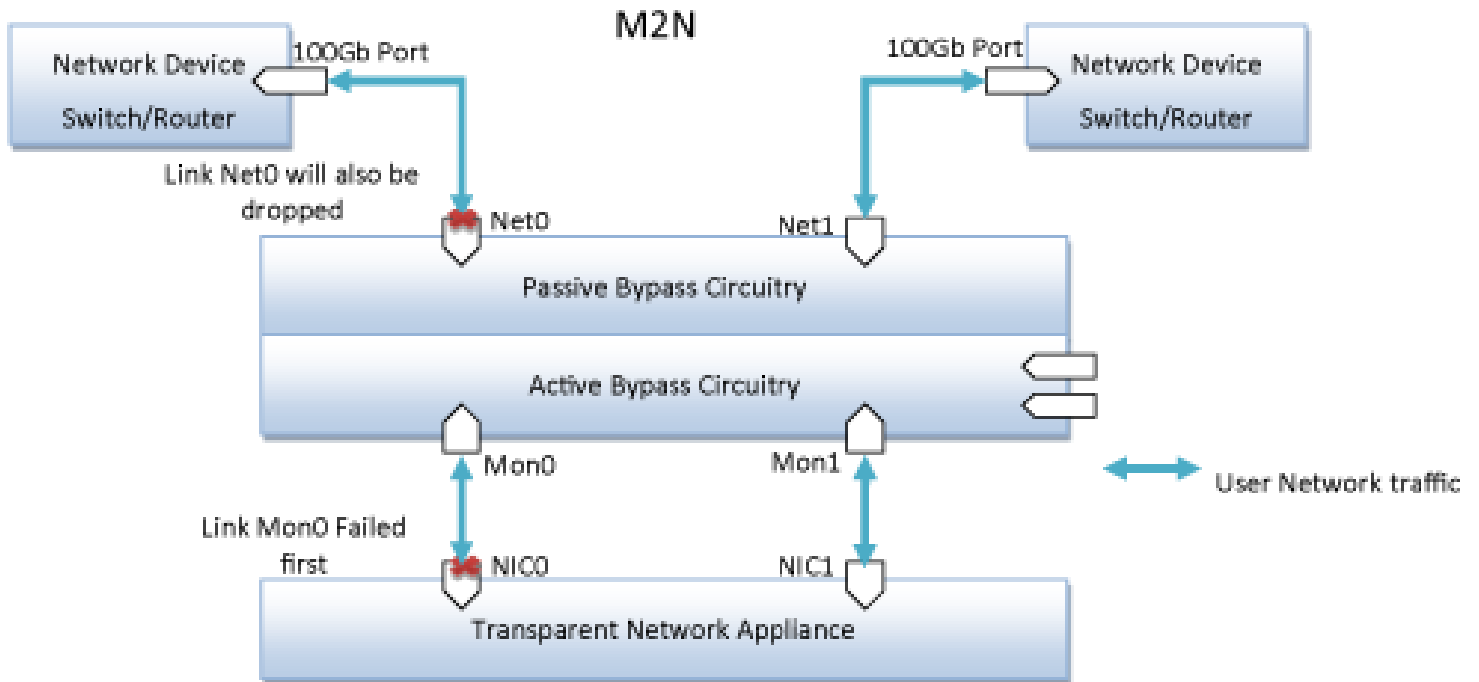


Figure 14. M1001Gxx M2N Illustration

### 5.4.3 M2M

The M2M feature is similar to the 2PL feature, but it connects the link of the two Mon ports together. When the feature is enabled, if the link of any one of Mon ports fails, the link of the other Mon port will also be dropped.

When the port that has its link failed recovers from the link failure, the link of the other port will also be turned back on again.

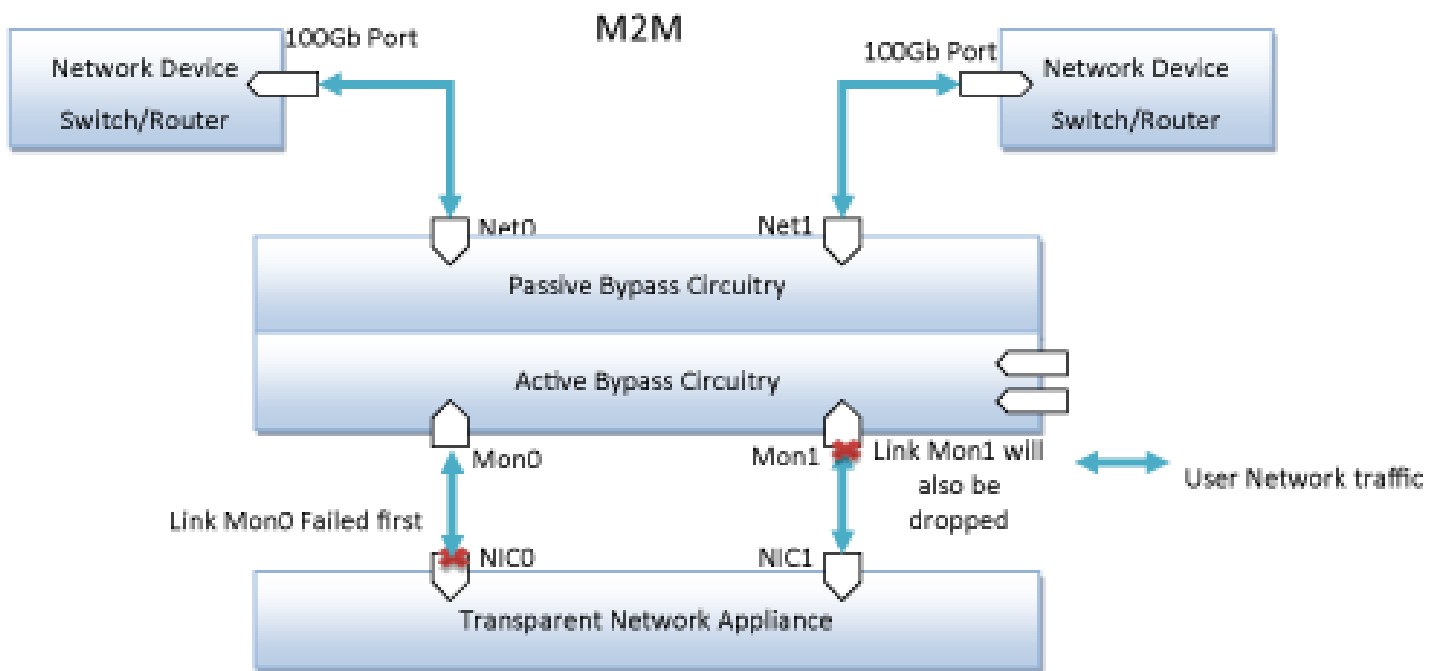


Figure 15. M1001Gxx M2M Illustration

### 5.4.4 Restoring from active expire state

The M100G1AC supports manual and auto restoration from a heartbeat expiration event.



## 6. Product Layout

This chapter introduces the front panels and rear panels of the M100G1AC 1U Unit.

### 6.1 Front panel

Depending on your order, the M100G1AC 1U Unit consists of one host system and one or two M100G1AC modules.

The following figure shows the M100G1AC 1U Unit front panel (a host system with two M100G1AC modules).



Figure 16. M100G1xx 1U Unit front panel – host system with two modules

#### 6.1.1 Host system front panel

The follow figure shows the front panel of the host system.



Figure 17. M100G1AC 1U Unit front panel – host system

The following tables explain the LEDs, switches, and connectors on the front panel of the host system.

Category	Descriptive name	Name on front panel	Description
LEDs	Power LEDs (Host system)	PS1	Green: Power is on Off: Power is off
		PS2	Green: Power is on Off: Power is off
	System status LEDs	Sys OK	Green: System is in normal operation Blinking green: Rack identification in process (whoami)
		Sys UP	Yellow: System initialization during power-up and during shutdown
		ALM	Red: System alarm
	Power LEDs (Modules)	M1	Green: Module 1 power on Red: Module 1 power off
		M2	Green: Module 2 power on Red: Module 2 power off
Switches	Power button	PWR	To turn on the system, press this button.
			To deactivate firmware when the system is on, press this button for four seconds.

Management Connectors			To turn off the system, press this button for eight seconds.
	Reset button	RST	To restart the system, press this button for more than one second.
	RJ-45 serial port	RS232	Management serial console
	RJ-45 Ethernet connector	MGNT ETH	Management Ethernet connector
	USB connector	USB	Management serial console

### 6.1.2 100G module front panel

The following figure shows the LEDs, switches, and connectors on one M100G1AC module.



Figure 18. M100G1xx SR4 module – Front panel

Category	Descriptive name	Name on front panel	Description
LEDs	Network port status LED	NET0 - Link/ACT	Green LED per port (Network / Monitor) Activity: LED will blink. Link: LED will turn on.
		NET1 - Link/ACT	
	Monitor port status LED	MON0 - Link/ACT	
		MON1 - Link/ACT	
	Inline mode LED	BP/INL	Green: System is in Inline mode
	Non-inline mode LED	BP/INL	Yellow: System is in Bypass, TAP or Linkdrop mode
	Heartbeat status LED	HB	Blinking green: Heartbeat active Off: Heartbeat inactive
Connectors			Network: Two MPO connectors Monitor: Two CFP4 connectors

### 6.1.3 100G LR4 module front panel

The following figure shows the LEDs, switches, and connectors on one M100G1xx module.



Figure 19. M100G1xx LR4 module – Front panel

Category	Descriptive name	Name on front panel	Description
LEDs	Network port status LED	NET0 - Link/ACT NET1- Link/ACT	Green LED per port (Network / Monitor) Activity: LED will blink. Link: LED will turn on.
	Monitor port status LED	MON0 - Link/ACT MON1 -Link/ACT	
	Inline mode LED	BP/INL	Green: System is in Inline mode
	Non-inline mode LED	BP/INL	Yellow: System is in Bypass, TAP or Linkdrop mode
	Heartbeat status LED	HB	Blinking green: Heartbeat active Off: Heartbeat inactive
Connectors			Network: Two MPO connectors Monitor: Two CFP4 connectors

#### 6.1.4 100G SR10 module front panel

The following figure shows the LEDs, switches, and connectors on one M100G1AC module.



Figure 20. M100G1xx SR10 module – Front panel

The following table explains the LEDs and connectors on the front panel of an M100G1xx module.

Category	Descriptive name	Name on front panel	Description
LEDs	Network port status LED	NET0 - Link/ACT NET1- Link/ACT	Green LED per port (Network / Monitor)
	Monitor port status LED	MON0 - Link/ACT MON1 -Link/ACT	Activity: LED will blink. Link: LED will turn on.
	Inline mode LED	BP/INL	Green: System is in Inline mode
	Non-inline mode LED	BP/INL	Yellow: System is in Bypass, TAP or Linkdrop mode
	Heartbeat status LED	HB	Blinking green: Heartbeat active Off: Heartbeat inactive
Connectors			Network: Two MPO connectors Monitor: Two CFP4 connectors

## 6.2 Rear panel

The following figure shows the rear panel of the M100G1xx 1U Unit (a host system with two power modules).



Figure 21. M100G1xx 1U Unit rear panel

### Bi-colour LED

There is a bi-colour LED integrated on each power supply module. The meaning of the LEDs is as follows:

- Green: Power is on
- Blinking green: Standby (AC/DC in, only +5VSB output)
- Red: Power is off
- Blinking red: Internal fan error

## 7. Installation

This chapter provides instructions on how to install the M100G1xx.

To install the M100G1xx, do the following:

**Step 1:** Mount the M100G1AC into a rack. The M100G1xx is a ready-for-rack-mounting box.

**Step 2:** Connect to power.

For the 220V AC/110V AC M100G1xx Unit, connect two power cables to the power connectors on the rear

panel. The PWR LED on the front panel turns on.

For the -48V DC M100G1AC Unit, do the following:

1. Ensure that the DC power source is disconnected.
2. Ensure that the power switch on the M100G1AC is turned off.
3. Connect the DC input wires to the DC input terminals on the M100G1AC by doing the following:
  - a) Connect wire to ground terminal M1001Gxx (left).
  - b) Connect -48V return to "+" terminal M1001Gxx (center).
  - c) Connect -48V wire to "-" terminal (right) M100G1AC.
  - d) Turn on the DC power source. The PWR LED on the front panel turns on.

**Step 3:** Connect the RS232 DB9 management cable by doing the following:

1. Connect one end of the RS232 DB9 cable to the M1001Gxx Management RS232 port.
2. Connect the other end of the RS232 cable to your device RS232 port.
3. Use any terminal emulation software (Minicom, HyperTerminal, etc.) to connect to the CLI.
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. Turn on the M100G1AC.
6. When the login prompt is displayed, log in with the following default parameters:
  - User name: admin
  - Password: gtadmin1
7. After login, change your password, user name and date. If you plan to use the management Ethernet port, set the IP address, net mask and gateway parameters.

**Step 4:** Connect the Ethernet management port.

1. Connect Ethernet cable (CAT5) to the Management 1G Ethernet network port.
2. Use any SSH or serial console to connect to the CLI.
3. The following are the default IP and login parameters:
  - IP address: 192.168.1.254
  - Net mask: 255.255.255.0
  - Gateway: 192.168.1.1
  - Login name: admin
  - Password: gtadmin1

**Note:** No default SNMP user is set.

## 8. Command line interface (CLI)

This chapter explains command names and command functions.

To view the full command list and to quickly navigate to the descriptions of each command, use the Table of Contents of this user guide.

### 8.1 CLI Features

The CLI supports auto complete and it also supports displaying online help with "?".

Each command parameter can include any letter or number and '\_', '/', ':', ';', '!', '-' characters. But cannot contain any spaces.

### 8.2 Login

To log in to the command line interface (CLI), use serial console software and a serial cable to connect to the RS232 management port or use SSH to connect to the management IP of the M100G1AC device.

Once connected, the login prompt will be shown

Welcome to Garland Technology's EdgeSafe Bypass TAP  
M100G1AC/DC Login:

Use the following username and password as the default to access the CLI

Username: admin

Default Password: gtadmin1

Once logged in, the system prompt will be shown

M1001Gxx>

### 8.3 Command modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands.

The following sections describe the following command modes:

- Command mode: user\_exec
- Command mode: privileged\_exec
- Command mode: configure

After login, the default mode would be user\_exec, to go into privileged\_exec use the "enable" command. To go into the configure mode, use the "configure" command.

#### Notes:

- EXEC commands are not saved when the software reboots.
- Commands issued in a configuration mode can be saved to the startup configuration. When the running configuration is saved to the startup configuration, these commands will execute when the software is rebooted.

#### 8.4.1 1. Command Mode: user\_exec

##### 8.4.1.1 cli clear-history

Clear the CLI history for the current user



#### **8.4.1.2 enable**

Enter enable mode

#### **8.4.1.3 exit**

Log out of the CLI

#### **8.4.1.4 help**

View the interactive help system

#### **8.4.1.5 show cli**

Display CLI options

#### **8.4.1.6 show clock**

Display system time and date

#### **8.4.1.7 show com configured**

Display serial console configuration

#### **8.4.1.8 show device**

Display device information

#### **8.4.1.9 show health**

Display device health status

#### **8.4.1.10 show management configured**

Display system management configuration

#### **8.4.1.11 show name configured**

Display serial console configuration

#### **8.4.1.12 show session configured**

Display session configuration

#### **8.4.1.13 show users**

Display a list of user accounts

#### **8.4.1.14 show version**

Display version information for current system image

### **8.4.2 Command Mode: privileged\_exec**

#### **8.4.2.1 clear bypass all**

Clear all bypass statistics

#### **8.4.2.2 clear bypass module <select from list>**

Clear bypass statistics for a module

#### **8.4.2.3 clear bypass segment <select from list>**

Clear bypass statistics for a segment



#### **8.4.2.4 clear bypass port <select from list>**

Clear bypass statistics for a port

#### **8.4.2.5 cli clear-history**

Clear the CLI history for the current user

#### **8.4.2.6 configure**

Enter configuration mode

#### **8.4.2.7 clock set date <YYYY-MM-DD>**

Set the system date

#### **8.4.2.8 clock set time <hh:mm:ss>**

Set the system time

#### **8.4.2.9 disable**

Exit enable mode

#### **8.4.2.10 exit**

Log out of the CLI

#### **8.4.2.11 help**

View the interactive help system

#### **8.4.2.12 show bypass configured**

Display all bypass configuration

#### **8.4.2.13 show bypass configured segment <select from list>**

Display bypass configuration for a segment

#### **8.4.2.14 show bypass state**

Display all bypass runtime state

#### **8.4.2.15 show bypass state segment <select from list>**

Display bypass statistics for a segment

#### **8.4.2.16 show bypass stats**

Display all bypass statistics

#### **8.4.2.17 show bypass stats segment <select from list>**

Display bypass statistics for a segment

#### **8.4.2.18 show cli**

Display CLI options

#### **8.4.2.19 show clock**

Display system time and date

#### **8.4.2.20 show com configured**

Display serial console configuration

**8.4.2.21 show device**

Display device information

**8.4.2.22 show health**

Display device health status

**8.4.2.23 show log**

Display log or its configuration

**8.4.2.24 show log filter <filter keyword>**

Display log with filter

**8.4.2.25 show log realtime**

Display realtime log

**8.4.2.26 show log configured**

Display log configuration

**8.4.2.27 show management configured**

Display system management configuration

**8.4.2.28 show name configured**

Display device name configuration

**8.4.2.29 show ntp configured**

Display NTP configuration

**8.4.2.30 show radius configured**

Display RADIUS configuration

**8.4.2.31 show session**

Display session runtime state

**8.4.2.32 show session configured**

Display session configuration

**8.4.2.33 show snmp**

Display SNMP runtime state

**8.4.2.34 show snmp configured**

Display SNMP configuration

**8.4.2.35 show snmp engineID**

Display SNMP engine ID of the local system

**8.4.2.36 show ssh configured**

Display SSH configuration

#### 8.4.2.37 show tacacs configured

Display TACACS+ configuration

#### 8.4.2.38 show users

Display a list of user accounts

#### 8.4.2.39 show version

Display version information for current system image

#### 8.4.2.40 show web configured

Display Web configuration

#### 8.4.2.41 reload [force|noconfirm]

Reboot the system

Parameters:

**force:** Force an immediate reboot of the system even if it is busy

**noconfirm:** Reboot the system without asking whether to save changes

#### 8.4.2.42 write memory

Save running configuration to the active configuration file

### 8.4.3 Command Mode: configure

Dis

#### 8.4.3.1 bypass port-link <select from list> fec <disable|enable>

Configure FEC state for a port

Parameters:

**port-link:** The port to configure

disable: Disable FEC

enable: Enable FEC

#### Note:

Due to the passive bypass requirement, FEC option for NET0 and NET1 ports must be configured the same.

### 8.4.3.2 bypass segment <select from list> active-op-mode <bypass|inline|linkdrop|tap|tapa|tapai1|tapai2|tapai12|tapi12>

Configure active operation mode for a bypass segment

Parameters:

**segment:** The segment to configure

bypass: Bypass mode

inline: Inline mode

linkdrop: Link is disabled when the appliance fails

tap: TAP mode (directional monitoring)

tapa: Aggregate mode (combined monitoring)

tapai1: Aggregate mode with dual injection from mon0

tapai2: Aggregate mode with dual injection from mon1

tapai12: Aggregate mode with dual injection from mon0 and mon1

tapi12: TAP mode with injection

### 8.4.3.3 bypass segment <select from list> hb active-mode <disable|enable>

Enable or disable heartbeat checking for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Disable heartbeat checking

enable: Enable heartbeat checking

### 8.4.3.4 bypass segment <select from list> hb active-mode-lock <disable|enable>

Lock or unlock heartbeat checking for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Unlock heartbeat checking enable: Lock heartbeat checking

### 8.4.3.5 bypass segment <select from list> hb active-restore <disable|enable>

Enable or disable heartbeat active restore for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Disable heartbeat active restore

enable: Enable heartbeat active restore

#### 8.4.3.6 bypass segment <select from list> hb active-expired-op-mode

<bypass|linkdrop|tap|tapa|tapai1|tapai2|tapai12|tapi12>

Configure heartbeat active expired operation mode for a bypass segment (the mode to go into when heartbeat checking expires)

Parameters:

**segment:** The segment to configure

bypass: Bypass mode

linkdrop: Link is disabled when the appliance fails

tap: TAP mode (directional monitoring)

tapa: Aggregate mode (combined monitoring)

tapai1: Aggregate mode with dual injection from mon0

tapai2: Aggregate mode with dual injection from mon1

tapai12: Aggregate mode with dual injection from mon0 and mon1

tapi12: TAP mode with injection

#### 8.4.3.7 bypass segment <select from list> hb fail-detect <uni|bi>

Configure heartbeat failure detection for a bypass segment

Parameters:

**segment:** The segment to configure

uni: Detect unidirectional heartbeat failure

bi: Detect bidirectional heartbeat failure

#### 8.4.3.8 bypass segment <select from list> hb recover-time <0~50000 msec>

Configure the time to recover from a heartbeat-lost event for a bypass segment

Parameters:

**segment:** The segment to configure

#### 8.4.3.9 bypass segment <select from list> hb hold-time <10~50000 msec>

Configure the time to hold received heartbeats for a bypass segment

Parameters:

**segment:** The segment to configure

#### 8.4.3.10 bypass segment <select from list> hb interval <3~10000 msec>

Configure the heartbeat interval for a bypass segment

Parameters:

**segment:** The segment to configure

#### 8.4.3.11 bypass segment <select from list> hb tx-direction <both|mon0|mon1>

Configure heartbeat transmission port for a bypass segment

Parameters:

**segment:** The segment to configure

both: Both mon0 and mon1

mon0: mon0

mon1: mon1

#### 8.4.3.12 bypass segment <select from list> hb packet op-mode <select from list> file-url <scp source url> file-type <hex|bin>

Configure heartbeat packet operation mode from a remote SCP URL for a bypass segment

Parameters:

**segment:** The segment to configure

**op-mode:** The operation mode for which the heartbeat packet will be used

**file-url:** Set the SCP source URL , for example, xxx@x.x.x.x:/packet/file/path/file.name

hex: The file format is hex

bin: The file format is binary

#### 8.4.3.13 bypass segment <select from list> hb packet op-mode <select from list> hex-string <hex string>

Configure heartbeat packet operation mode by using hex string for a bypass segment

Parameters:

**segment:** The segment to configure

**op-mode:** The operation mode for which the heartbeat packet will be used

#### 8.4.3.14 bypass segment <select from list> hb packet op-mode <select from list> clear

Clear heartbeat packet operation mode configuration for a bypass segment

Parameters:

**segment:** The segment to configure

**op-mode:** The operation mode for which the heartbeat packet will be used

#### 8.4.3.15 bypass segment <select from list> port m2n <both|disabled|mon0|mon1>

Configure monitor to network port link fail state for a bypass segment

Parameters:

**segment:** The segment to configure

both: Both mon0 and mon1

disabled: Disabled

mon0: mon0

mon1: mon1

#### 8.4.3.16 bypass segment <select from list> port m2m <disable|enable>

Configure monitor to monitor port link fail state for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Disable m2m

enable: Enable m2m

#### 8.4.3.17 bypass segment <select from list> port power-off-bypass <disable|enable>

Configure the power off state for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Disable

enable: Enable

#### 8.4.3.18 bypass segment <select from list> port link-speed <auto|1g|10g|40g|100g>

Configure port link speed for a bypass segment

Parameters:

**segment:** The segment to configure

auto: Set automatically

1g: Set speed to 1 Gb

10g: Set speed to 10Gb

40g: Set speed to 40Gb

100g: Set speed to 100Gb

#### 8.4.3.19 bypass segment <select from list> port two-ports-link <disable|enable>

Configure two ports link state for a bypass segment

Parameters:

**segment:** The segment to configure

disable: Disable two ports link

enable: Enable two ports link

#### 8.4.3.20 bypass segment <select from list> rx-tx-errors mon-op-mode <bypass|linkdrop|none|tap>

Configure the mode to go into when errors per second on any Mon ports exceed threshold for a bypass segment.

Parameters:

**segment:** The segment to configure

bypass: Bypass mode

linkdrop: Live link is disabled because of appliance failure

none: Do nothing

tap: TAP mode (directional monitoring)

#### 8.4.3.21 bypass segment <select from list> rx-tx-errors net-op-mode <linkdrop|none>

Configure the mode to go into when errors per second on any Net ports exceed threshold for a bypass segment.

Parameters:

**segment:** The segment to configure

linkdrop: Link is disabled when the appliance fails

none: Do nothing

#### 8.4.3.22 bypass segment <select from list> rx-tx-errors rate-threshold <threshold >0>

Configure the threshold of errors per second for a bypass segment

Parameters:

**segment:** The segment to configure

#### 8.4.3.23 bypass segment <select from list> rx-tx-errors trap <disable|enable>

Enable or disable bypass trap

Parameters:

**segment:** The segment to configure

disable: Disable trap

enable: Enable trap

#### 8.4.3.24 bypass segment <select from list> rx-tx-errors timeout <>0 msec>

Configure the minimal time between traps for a bypass segment

Parameters:

**segment:** The segment to configure

#### 8.4.3.25 clear bypass stats all

Clear all bypass statistics

#### 8.4.3.26 clear bypass stats module <select from list>

Clear bypass statistics for a module

#### 8.4.3.27 clear bypass stats segment <select from list>

Clear bypass statistics for a segment

#### 8.4.3.28 clear bypass stats port <select from list>

Clear bypass statistics for a port

#### 8.4.3.29 clear bypass error rxtx all

Clear all bypass RX/TX errors

#### 8.4.3.30 clear bypass error rxtx module <select from list>



8.4.3.30 clear bypass error rxtx module <select from list>

**8.4.3.31 clear bypass error rxtx segment <select from list>**

Clear bypass RX/TX errors for a segment

**8.4.3.32 cli clear-history**

Clear the CLI history for the current user

**8.4.3.33 clock set date <YYYY-MM-DD>**

Set the system date

**8.4.3.34 clock set time <hh:mm:ss>**

Set the system time

**8.4.3.35 clock timezone <select from list> area <select from list>**

Set the system time zone

Parameters:

**timezone:** The system time zone

**8.4.3.36 com speed <9600 | 19200 | 38400 | 57600 | 115200>**

Configure serial console speed

Parameters:

9600: Set speed to 9600

19200: Set speed to 19200

38400: Set speed to 38400

57600: Set speed to 57600

115200: Set speed to 115200

**8.4.3.37 com terminal-type <terminal type, such as vt100>**

Configure serial console terminal type

**8.4.3.38 configurations save**

Save current configuration to a file (default file name is\_config\_yyyymmddHHMMSS)

**8.4.3.39 configurations save as <select from list>**

Save current configuration to the specified file

**8.4.3.40 configurations scp <URL string, such as scp://x.x.x.x/path/file>**

Upload a configuration file (default file name is\_config\_yyyymmddHHMMSS)

**8.4.3.41 configurations scp <URL string, such as scp://x.x.x.x/path/file> as <select from list>**

Save the uploaded configuration to the specified file

**8.4.3.42 configurations restore <select from list>**

Restore system configuration from the specified file

**8.4.3.44 dump create log**

Create a system log dump file as is\_log\_YYYYMMDDhhmmss

#### 8.4.3.45 dump delete

Delete a system dump file

#### 8.4.3.46 exit

Exit configuration mode

#### 8.4.3.47 halt [noconfirm]

Shut down the system

Parameters:

noconfirm: Shut down the system without asking whether to save changes

#### 8.4.3.48 help

View the interactive help system

#### 8.4.3.49 log level <debug|info|notice|warn|err|crit|alert|emerg>

Configure the system log level

Parameters:

debug: DEBUG

info: INFO

notice: NOTICE

warn: WARNING

err: ERROR

crit: CRITICAL

alert: ALERT

emerg: EMERGENCY

#### 8.4.3.50 log max-size <1-10(MB)>

Configure the maximum log file size

#### 8.4.3.51 log reset

Reset all system logs

#### 8.4.3.52 log remote <disable|enable>

Configure remote log

Parameters:

disable: Disable remote log

enable: Enable remote log

#### 8.4.3.53 log remote server <IP address>

Configure remote log server IP address

#### **8.4.3.54 management eth-if <disable|enable>**

Configure Ethernet interface

Parameters:

disable: Disable management interface

enable: Enable management interface

#### **8.4.3.55 management eth-if ip <IP address> mask <IP address>**

Configure IP address for management interface

#### **8.4.3.56 management eth-if default-gateway <IP address>**

Configure default gateway for management interface

#### **8.4.3.57 management dns ip <IP address>**

Add a DNS server

#### **8.4.3.58 management permitted <disable|enable>**

Configure management permitted IP

Parameters:

disable: Disable permitted IP check

enable: Enable permitted IP check

#### **8.4.3.59 management permitted ip <IP address> [mask <IP net mask>]**

Add a permitted IP address

Parameters:

mask: Permitted IP net mask

#### **8.4.3.60 management whoami <off|on>**

Turn on/off the whoami function, which is designed for rack identification. When the function is turned on, the Sys OK LED blinks every second.

Parameters:

off: Turn off the whoami function

on: Turn on the whoami function

#### **8.4.3.61 name <hostname [a-zA-Z0-9-\_.]>**

Configure device name, which will be shown in CLI prompt

#### **8.4.3.62 no configuration <select from list>**

Remove system configuration

#### **8.4.3.63 no management dns <select from list>**

Remove management DNS server

#### **8.4.3.64 no management permitted <select from list>**

Remove management permitted IP

#### **8.4.3.65 no radius <select from list>**

Remove RADIUS server

#### **8.4.3.66 no snmp community <select from list>**

Remove an SNMP community

#### **8.4.3.67 no snmp host <select from list>**

Remove an SNMP trap host

#### **8.4.3.68 no snmp user <select from list>**

Remove an SNMP trap user

#### **8.4.3.69 no tacacs <select from list>**

Remove TACACS+ server configuration

#### **8.4.3.70 no user <select from list>**

Remove a local user account

#### **8.4.3.71 ntp <disable|enable>**

Enable or disable NTP

Parameters:

disable: Disable NTP

enable: Enable NTP

#### **8.4.3.72 ntp server <Host or IP address>**

Configure NTP server

#### **8.4.3.73 radius <disable|enable>**

#### **8.4.3.74 Disable or enable RADIUS remote login. For details, refer to radius local-login <enable|disable>**

Enable or disable local users' login.

Parameters:

enable: Enable local users' login

disable: Disable local users' login

#### **8.4.3.75 radius privilege <readonly|normal|admin>**

Configure RADIUS user privilege

Parameters:

readonly: Read-only access

normal: Normal read and write access

admin: Administrator's access

#### 8.4.3.76 radius retry <Number of retry>

Configure RADIUS login retry count

#### 8.4.3.77 radius server ip <IP address> port <Port number> secret <8~128 symbols> timeout <Second number>

Add a RADIUS server

Parameters:

**ip:** RADIUS server IP

**port:** RADIUS server port

**secret:** Server secret

**timeout:** Timeout value

#### 8.4.3.78 reload [force|noconfirm]

Reboot the system

Parameters:

**force:** Force an immediate reboot of the system even if it is busy

**noconfirm:** Reboot the system without asking whether to save changes

#### 8.4.3.79 session expired-time <120~86400 seconds>

Specify the time in seconds after which an idle session is expired

Parameters:

**expired-time:** The time in seconds after which an idle session is expired

#### 8.4.3.80 show bypass configured

Display all bypass configurations

#### 8.4.3.81 show bypass configured segment <select from list>

Display bypass configuration for a segment

#### 8.4.3.82 show bypass state

Display all bypass runtime state

#### 8.4.3.83 show bypass state segment <select from list>

Display bypass statistics for a segment

#### 8.4.3.84 show bypass stats

Display all bypass statistics

#### 8.4.3.85 show bypass stats segment <select from list>

Display bypass statistics for a segment

#### 8.4.3.86 show cli

Display CLI options

#### 8.4.3.87 show clock

Display system time and date

#### **8.4.3.88 show com configured**

Display serial console configuration

#### **8.4.3.89 show configurations list**

Display the system configuration file list

#### **8.4.3.90 show configurations detail <select from list>**

Display system configuration in detail

#### **8.4.3.91 show device**

Display device information

#### **8.4.3.92 show dump**

Display system dump file list

#### **8.4.3.93 show health**

Display device health status

#### **8.4.3.94 show log [filter <filter keyword> | realtime | configured]**

Display log or its configuration

Parameters:

filter: Display log with filter

realtime: Display realtime log

configured: Display log configuration

#### **8.4.3.95 show management configured**

Display system management configuration

#### **8.4.3.96 show ntp configured**

Display NTP configuration

#### **8.4.3.97 show radius configured**

Display RADIUS configuration

#### **8.4.3.98 show session**

Display session runtime state

#### **8.4.3.99 show session configured**

Display session configuration

#### **8.4.3.100 show snmp [configured | engineID]**

Display SNMP runtime state

Parameters:

configured: Display SNMP configuration

engineID: Display SNMP engine ID of the local system

#### 8.4.3.101 show ssh configured

Display SSH configuration

#### 8.4.3.102 show tacacs configured

Display TACACS+ configuration

#### 8.4.3.103 show uptime

Display system uptime information

#### 8.4.3.104 show users

Display a list of user accounts

#### 8.4.3.105 show version

Display version information for current system image

#### 8.4.3.106 show web configured

Display Web configuration

#### 8.4.3.107 snmp <disable|enable>

Disable or enable SNMP server

Parameters:

disable: Disable SNMP server

enable: Enable SNMP server

#### 8.4.3.108 snmp apply

Apply SNMP configuration. The user needs to run this command for any of the following configuration to take effect:

**snmp community** <community name> [disable|enable|full-access|read-only]

**snmp host** <select from list> <disable|enable>

**snmp user** <disable|enable|full-access|read-only>

#### 8.4.3.109 snmp community <community name> [disable|enable|full-access|read-only]

Add or configure an SNMP v1/v2c community

**Note:** The user need to run the **snmp apply** command for the configuration to take effect.

Parameters:

disable: Disable the user

enable: Enable the user

full-access: Add full access

read-only: Add read-only access

#### 8.4.3.110 snmp host <select from list> <disable|enable>

Configure a host to send SNMP traps to

**Note:** The user need to run the **snmp apply** command for the configuration to take effect.

Parameters:

disable: Disable sending trap to this host

enable: Enable sending trap to this host

#### **8.4.3.111 snmp host <host name> v1 community <Community string>**

Add SNMP Version 1 trap host

Parameters:

**community:** SNMP community

#### **8.4.3.112 snmp host <host name> v2c community <Community string>**

Add SNMP Version 2c trap host

Parameters:

**community:** SNMP community

#### **8.4.3.113 snmp host <host name> v3 user <Name of 5~30 symbols> password <User password, at least 8 symbols> <md5|sha>**

Add SNMP Version 3 trap host

Parameters:

**user:** Set the user

**password:** Set user password

md5: Use the MD5 hash algorithm

sha: Use the SHA1 hash algorithm

#### **8.4.3.114 snmp trap disable <all|application|fan|power|sensor|switch|system|terminal>**

Disable SNMP trap type

Parameters:

all: Disable all trap types

application: Disable application trap

fan: Disable fan trap

power: Disable power trap

sensor: Disable sensor trap

switch: Disable switch trap

system: Disable system trap

terminal: Disable terminal trap

#### **8.4.3.115 snmp trap enable <all|application|fan|power|sensor|switch|system|terminal>**

Enable SNMP trap types

Parameters:

all: Enable all trap types

application: Enable application trap

fan: Enable fan trap

power: Enable power trap

sensor: Enable sensor trap

switch: Enable switch trap

system: Enable system trap

terminal: Enable terminal trap



#### 8.4.3.116 snmp user <disable|enable|full-access|read-only>

Configure an SNMP v3 access user (need to apply)

**Note:** The user need to run the **snmp apply** command for the configuration to take effect.

Parameters:

disable: Disable the user's access

enable: Enable the user's access

full-access: Add full access

read-only: Add read-only access

#### 8.4.3.117 snmp user password <User password, at least 8 symbols> <md5|sha>

Add an SNMP v3 user

Parameters:

md5: Use the MD5 hash algorithm

sha: Use the SHA1 hash algorithm

#### 8.4.3.118 ssh <disable|enable>

Configure SSH service

Parameters:

disable: Disable SSH service

enable: Enable SSH service

#### 8.4.3.119 ssh port <Port number, default is 22>

Configure SSH service port

#### 8.4.3.120 tacacs <disable|enable>

Disable or enable TACACS+ remote login. For details, refer to 3. System management overview.

Parameters:

disable: Disable TACACS+ remote login

enable: Enable TACACS+ remote login

#### 8.4.3.121 tacacs local-login <enable|disable>

Enable or disable local users' login

Parameters:

enable: Enable local users' login

disable: Disable local users' login

#### 8.4.3.122 tacacs service <Can't be slip/ppp/arap/shell/ttydaemon/ connection/system/firewall>

Set TACACS+ service tag. For details, refer to 3. System management overview.

#### 8.4.3.123 tacacs timeout <Second number>

Set TACACS+ timeout value

**8.4.3.124 tacacs server <ID number> ip <IP address> port <Port number> secret <8~128 symbols>**

Add a TACACS+ server

Parameters:

**ip:** Add a TACACS+ server IP

**port:** TACACS+ server port

**secret:** Server secret

**8.4.3.125 upgrade ftp <URL string, such as ftp://x.x.x.x/path/file> user <user name> password <password string>**

Upgrade system from an FTP URL

Parameters:

**user:** FTP user name

**password:** FTP user password

**8.4.3.126 upgrade http <URL string, such as http://x.x.x.x/path/file>**

Upgrade system from an HTTP URL

**8.4.3.127 upgrade scp <URL string, such as scp://x.x.x.x/path/file> user <user name>**

Upgrade system from an SCP URL

Parameters:

**user:** SCP user name

**8.4.3.128 user change-password new-password <Password, 6~40 symbols>**

Change local user's password

Parameters:

**new-password:** New password

**8.4.3.129 user change-password new-password <Password, 6~40 symbols> user-name <select from list>**

Change the specific local user's password

Parameters:

**new-password:** New password

**8.4.3.130 user change-password new-encrypt-password <Secret string>**

New secret

**8.4.3.131 user change-password new-encrypt-password <Secret string> user-name <select from list>**

Change the specific local user's password by using an encrypted password

**8.4.3.132 user name full-name <Such as: 'James Bush'> password <Password, 6~40 symbols> privilege <readonly|normal|admin>**

Add a local user

Parameters:

**password:** Set password

**privilege:** Set user privilege

readonly: Read-only access

normal: Normal read and write access

admin: Administrator's access

**8.4.3.133 user name full-name <Such as: 'James Bush'> encrypt-password <Encrypt string> privilege <readonly|normal|admin>**

Add a local user by using an encrypted password

Parameters:

**privilege:** Set user privilege

readonly: Read-only access

normal: Normal read and write access

admin: Administrator's access

**8.4.3.134 web session-expired-time <60~3600 seconds>**

Specify the time in seconds after which an idle Web session is expired

**8.4.3.135 web http <disable|enable>**

Configure HTTP service

Parameters:

disable: Disable HTTP service

enable: Enable HTTP service

**8.4.3.136 web http port <Port number, default 80>**

Configure HTTP listening port

**8.4.3.137 web https <disable|enable>**

Configure HTTPS service

Parameters:

disable: Disable HTTPS service

enable: Enable HTTPS service

**8.4.3.138 web https port <Port number, default 443>**

Configure HTTPS listening port

**8.4.3.139 web https ssl cert file-url <scp source url>**

Configure the HTTPS SSL certificate from a file URL, for example, xxx@x.x.x.x:/packet/file/path/file.name

**8.4.3.140 web https ssl cert encrypt <Encrypted string>**

Configure the HTTPS SSL certificate by using encrypted string

#### 8.4.3.141 web https ssl key file-url <scp source url>

Configure the HTTPS SSL key from an SCP URL, for example, xxx@x.x.x.x:/packet/file/path/file.name

#### 8.4.3.142 web https ssl key encrypt <Encrypted string>

Configure the HTTPS SSL key by using encrypted string

#### 8.4.3.143 write memory

Save running configuration to the active configuration file

## 9. Web interface

This chapter introduces the M100G1xx Web interface.

### 9.1 Starting the Web interface

The M100G1xx Web interface can be accessed from most popular Web browsers. To connect to the M100G1xx

Web interface, use the following Web addresses on your Web browser:

- If http is enabled, use "http://device\_ip\_address"; if the http port is not the default 80, use http://device\_ip\_address:http\_port
- If https is disabled, use "https://device\_ip\_address"; if the https port is not the default 443, use [https://device\\_ip\\_address:https\\_port](https://device_ip_address:https_port) where device\_ip\_address is the M100G1xx Ethernet management port IP address.

where **device\_ip\_address** is the M100G1xx Ethernet management port IP address.

#### Notes:

- If the Web interface has been inactive (not sending requests to the M100G1xx) for a period longer than the specified Web Session Timeout value (default: 900 seconds), a login screen will be displayed. The user can configure the Web Session Timeout value by navigating to **System > Service > Web > Session Timeout**.
- Context help is provided for most Web application fields.
- All the new settings in the Web interface take effect only after the user clicks the **Commit** button.

### 9.2 Login

The following screenshot shows the login screen of the M100G1xx Web interface.

On the login screen, type the username and password to access the M100G1xx Web interface. The default username is **admin**. The default password is **Garland2015**.

The first user that logs into the Web interface will get full rights (control and monitor) in the Web interface.

The following users will not be able to control the Web interface, and they will only be able to monitor the M100G1xx parameters.

When the first user logs off from the Web interface, the next user will inherit the first user's rights and will be able to control and monitor the Web interface.

After login, the main menu of the M100G1xx Web interface is displayed, which contains the following tabs:

Each tab will be explained in subsequent sections.

### 9.3 Status

The Status tab provides access to the following status information pages:

- System
- Module (Module 1 and Module 2)
- SNMP
- Session
- System Log

#### 9.3.1 System status

Navigate to **Status > System**. The system information page is displayed, showing status of the following:

- Global
- Sensors (I2C sensors, BCM sensors, Switch sensors, Module sensors)
- Fans

##### Sensor I2C

Name	Temperature	Peak
This section contains no values yet		

##### Sensor BCM

Name	Temperature	Peak
BCM1	45	47
BCM2	47	48
BCM3	47	48
BCM4	48	49
BCM5	46	47
BCM6	47	48
BCM7	48	48
BCM8	45	46

## Sensor Switch

Name	Temperature	Peak
CP01	29	29
CP02	29	29
CP03	29	29
CP04	29	29
CP07	46	46

## Sensor Module

Name	Temperature	Peak
MO11	28	29
MO21	29	29

## Fan Status

ID	Name	Fault	Warning	Status	Speed	Run Time
1	FN11	No	No	Green	16816	3241
2	FN12	No	No	Green	16891	3280
3	FN13	No	No	Unknown	14822	3271
4	FN14	No	No	Green	16816	3343

The **Global** area provides the following information:

- **Device Type**
- **Device Serial Number**
- **Hardware Version**
- **Firmware Version**
- **Software Version**
- **UBoot Version**
- **Power Supply:** Whether the power supply is up or down
- **System Time:** The current system time
- **System up time:** How long the system has been running
- **Load average:** The average system load over a period of time. It conventionally appears in the form of three numbers which represent the system load during the last one-, five-, and fifteen-minute periods.
- **Config Change Saved:** Whether the configuration is saved to non-volatile memory.
- **Who am I:** To start the rack identification process, click the **Turn on** button. The **System status LED Sys OK** blinks every second.

The **Sensor** area shows the status (current temperature and peak temperature) of different temperature sensors, including:

- I2C sensors
- BCM sensors
- Switch sensors
- Module sensors

The **Fans** area shows the following fan status:

- **ID**
- **Name**
- **Fault (Yes/No)**
- **Warning (Yes/No)**
- **Status (Unknown /Green/Yellow/Orange/Red)**
- **Speed**
- **Run Time**

### 9.3.2 Module status

Navigate to **Status > Module X** (X indicates the module number). The status page of the corresponding module is displayed.

The following explanations use Module 1 as an example.

The following screenshot shows the status page of Module 1.

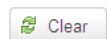
## Module 1 Information

Module Type	Bypass
Media Type	100GBase-LR4
Transceiver Type	CFP4 LR4
Segment 1 MON0 Mac	00:e0:ed:28:00:01
Segment 1 MON1 Mac	00:e0:ed:28:00:02

## Segment Status

ID	Speed	HB Checking	HB Checking Off Reason	Active State	Passive State	Application State	RxTx Error	2-Port Link State	M2N Link State	M2M Link State	Link Network 0	Link Network 1	Link Monitor 0	Link Monitor 1
1	100G	On	None	Bypass	Inline	Fail	No	OK	OK	OK	Up	Up	Up	Up

## Clear Rx/Tx Error



## Port Signal Strength

Name	Lane 0 TX(dBm)	Lane 0 RX(dBm)	Lane 1 TX(dBm)	Lane 1 RX(dBm)	Lane 2 TX(dBm)	Lane 2 RX(dBm)	Lane 3 TX(dBm)	Lane 3 RX(dBm)
Seg 1 Net 0	-0.464818	-3.741734	0.514226	-4.061604	0.430870	-3.510549	-0.752039	-3.490129
Seg 1 Net 1	-0.431116	-0.560606	0.431657	-0.352690	0.154018	-0.672219	-0.922127	-1.539104
Seg 1 Mon 0	2.082801	2.886963	2.473841	2.482920	2.102652	0.912447	2.532654	1.283026
Seg 1 Mon 1	2.121344	2.201343	2.634940	2.581820	2.151880	2.624512	1.344957	3.072820

The **Module Information** area displays the following information:

- Module Type (Bypass/Switch)
- Media Type (LR/SR)
- Transceiver Type
- Monitor 0 (Mon0) MAC address
- Monitor 1 (Mon1) MAC address



The **Segment Status** area provides the following segment information:

- ID
- Speed (**100G**)
- HB Checking (**On/Off**): Heartbeat checking
- HB Checking Off Reason (**None/ HB active off / HB restore off / MON rxtx err / Net rxtx err**)
- Active State (**Inline/Bypass/Tap/Linkdrop**)
- Passive State (**Bypass/Inline**)
- ApplicationState (**Unknown/Alive/Fail**)
- RxTx Error (**Yes/No**)
- 2-Port Link State (**OK/Fail**)
- M2N Link State (**OK/Fail**)
- M2M Link State (**OK/Fail**)
- Link Network (Net0/Net1) State (**Up/Down**)
- Link Monitor (Mon0/Mon1) State (**Up/Down**)

The **Clear Rx/Tx Error** area provides a **Clear** button for clearing Rx/Tx errors.

The **Port Signal Strength** area shows the signal strength of network ports and monitor ports. Information for each individual lane in the SR4/LR4 link is provided, which is helpful in ensuring a stable SR4/LR4 link.

### 9.3.3 SNMP Status

Navigate to Status > SNMP. The SNMP status page is displayed, as shown:

#### SNMP Status

##### SNMP

Enabled Yes

Engine ID 0x80001f88802774d3f056a9c96e

The **SNMP** area provides the following information:

- **Enabled:** Whether SNMP is enabled (**Yes**) or not (**No**)
- **EngineID:** SNMP engine ID

### 9.3.4 Session Status

Navigate to **Status > Session**. The session status page is displayed, as shown:

#### Session

ID	User	Login Type	Login Time	Login IP	Login Port
2486	root	SSH	2016-01-28 07:55:51	192.168.49.176	60682
2522	root	SSH	2016-01-28 08:47:27	192.168.49.113	40123
2526	is_admin	WEB	2016-01-28 08:48:59		

The **Session** area shows details of the current active sessions, including:

- **User name**
- **Login Type**
- **Login Time**
- **Login IP**
- **Login Port**

### 9.3.5 System Log

Navigate to **Status > System Log**. The system log is displayed, as shown:

#### System Log

1 2 ... 286 287 288 Page: 1

```

2016-01-28T09:46:43.438284+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state PRE_FAIL , event HB_RECV , new state OK
2016-01-28T09:46:43.561444+00:00 is100_1 is_switchd:[user.err] Time SWITCH_PKT_ERR process took too long 214247us
2016-01-28T09:46:43.570478+00:00 is100_1 is_mgmtmd:[user.info] [is_mgmtmd_system_action]p_conn:0xb507f008, User:is_admin, get privilege from req: 3
2016-01-28T09:46:44.378313+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state OK , event HB_LOST , new state PRE_FAIL
2016-01-28T09:46:44.379252+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state PRE_FAIL , event HB_RECV , new state OK
2016-01-28T09:46:44.430401+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state OK , event HB_LOST , new state PRE_FAIL
2016-01-28T09:46:44.431316+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state PRE_FAIL , event HB_RECV , new state OK
2016-01-28T09:46:44.456572+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state OK , event HB_LOST , new state PRE_FAIL
2016-01-28T09:46:44.457540+00:00 is100_1 is_switchd:[user.info] Segment 1.1 Port MON0 HB state PRE_FAIL , event HB_RECV , new state OK
2016-01-28T09:46:44.554540+00:00 is100_1 is_switchd:[user.err] Time SWITCH_PKT_ERR process took too long 212699us

```

Tips for reviewing the system log:

- The log is displayed in backward scheduling order. The latest events are displayed on the first page while the earliest events on the last page.
- Users can select or type a page number to review the log on a particular page.
- Users can use the **Search** button to filter the log.
- To clear all the logs, click **Reset Log**.

## 9.4 Statistics

The **Statistics** tab provides statistics of the following:

- Modules (Module 1, Module 2)
- Realtime Traffic

### 9.4.1 Module statistics

Navigate to **Statistics > Module X** (X indicates the module number) to view the statistics of the corresponding module.

The following explanations use Module 1 as an example.

The following screenshot shows the statistics of Module 1.

## Module 1 Statistics

Segment 1


Realtime

Accumulative

Item	Net 0	Net 1	Monitor 0	Monitor 1
RxPkts	2593725	2591429	3089605	3089441
RxOctets	295684650	295422906	319332370	319313724
RxPktGood	2593725	2591429	3089605	3089441
RxUnicastPkts	2593725	2591429	3089605	3089441
RxMulticastPkts	0	0	0	0
RxBroadcastPkts	0	0	0	0
RxErrors	0	0	0	0
RxDiscards	36	0	657693	657660
TxOctets	294375360	294641436	321146240	321170620
TxPktGood	2582240	2584574	3110960	3111180
TxUnicastPkts	2582240	2584574	3110960	3111180
TxMulticastPkts	0	0	0	0
TxBroadcastPkts	0	0	0	0
TxErrors	0	0	0	0
TxDiscards	0	0	0	0
HeartbeatRxPkt	0	0	657837	657836
HeartbeatTxPkt	0	0	670266	670266

### Clear Statistics

Port

 Clear

Suspend auto refresh

#### Tips for reviewing the module statistics:

- The Module Statistics area lists the packet statistics of all segments and ports in the module.
- Two tabs are provided in the upper-right corner:
  - Accumulative: Click this tab to view accumulated statistics since last statistics clear operation or system bootup.
  - Realtime: Click this tab to view real-time statistics, which is updated every second.
- To clear the statistics of certain or all segments/port, use the **Clear** button in the **Clear Statistics** area.

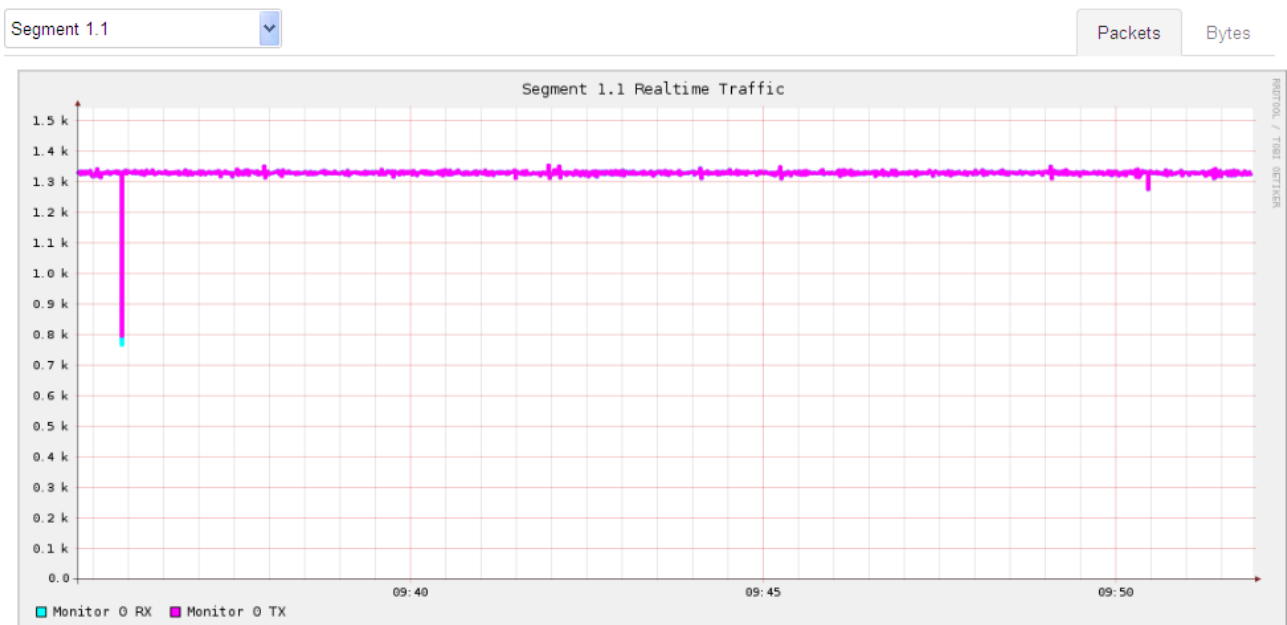
- By default, the module statistics on this page is auto-refreshed. To suspend the auto-refresh function, click the **Suspend auto refresh** button.

### 9.4.2 Realtime Traffic Statistics

Navigate to **Statistics > Realtime Traffic** to view the real-time traffic statistics over the past 1200 seconds.

The following screenshot shows the real-time traffic of segment 1.1 over the past 1200 seconds.

#### Realtime Traffic



Select the ports to display in graphic:

- |           |  |                                     |
|-----------|--|-------------------------------------|
| Net 0     | ( RX <span style="color: red;">■</span> TX <span style="color: green;">■</span> )        | <input type="checkbox"/>            |
| Net 1     | ( RX <span style="color: blue;">■</span> TX <span style="color: yellow;">■</span> )      | <input type="checkbox"/>            |
| Monitor 0 | ( RX <span style="color: cyan;">■</span> TX <span style="color: magenta;">■</span> )     | <input checked="" type="checkbox"/> |
| Monitor 1 | ( RX <span style="color: purple;">■</span> TX <span style="color: darkgreen;">■</span> ) | <input type="checkbox"/>            |

Tips for viewing the realtime traffic statistics:

- To view the realtime traffic statistics of a specific segment, select the segment from the drop-down list box.
- Two tabs are provided in the upper-right corner: Packets and Bytes. Select either to view the realtime traffic statistics of packets or bytes.
- To view the realtime statistics of a specific network port or monitor port, select the checkbox for the corresponding network port or monitor port.

## 9.5 Bypass Configuration

The **Bypass Configuration** tab provides access to the following pages:

- Module configurations
  - Heartbeat settings
  - Advanced features
  - RX/TX error processing
- Heartbeat (HB) packet configurations

### 9.5.1 Module Configuration

Navigate to **Bypass Configuration > Module X** (X indicates the module number). The corresponding **Module Configuration** page is displayed. Users can configure the various module settings.

The following explanations take Module 1 as an example.

The following screenshot shows the configuration menus for Module 1.

### Module 1 Configuration

#### Segment 1



The users can configure the following modules settings:

- **Heartbeat Settings**
- **Advanced Features**
- **RX/TX error Processing**

#### 9.5.1.1 Heartbeat setting

The following screenshot shows the **Heartbeat Setting** menu for module configuration.

## Module 1 Configuration

### Segment 1

Heartbeat Setting

Advanced Features

RX/TX Error Processing

Heartbeat Active Mode ☒

Heartbeat Active Restore ☒

Heartbeat Interval  ⓘ 3-10000ms

Heartbeat Expire Timer  ⓘ 10-50000ms

Heartbeat Recover Timer  ⓘ 0-50000ms

Active OP Mode

Heartbeat Active Expired OP Mode

Heartbeat TX Direction

Heartbeat Failure Detection


User Defined MAC ☐

Affective MAC MON0: 00:e0:ed:28:00:01, MON1: 00:e0:ed:28:00:02

Inline Heartbeat Packet

Bypass Heartbeat Packet

TAP Heartbeat Packet

 Upload Packet File

Commit

Reset

On the **Heartbeat Setting** menu, the user can configure the following:  
Config

## Heartbeat Active Mode

When the **Heartbeat Active Mode** option is enabled, the M100G1AC sends heartbeat packets to its monitor ports. If the M100G1AC does not detect the flow of heartbeat packets on the monitor ports, the M100G1AC will switch to **Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop** mode according to the predefined settings of the **Heartbeat Active Expired OP Mode** parameter.

When the **Heartbeat Active Mode option** is disabled, the M100G1AC stops sending heartbeat packets and the user can manually set **Active Bypass** to one of the following modes: **Inline, Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop**, via the management port.

## Heartbeat Active Restore

When the **Heartbeat Active Mode** option is enabled, the M100G1AC will restore to Inline mode when heartbeat packets are received from the monitor ports.

When the **Heartbeat Active Mode** option is disabled, the M100G1AC maintains its state and no heartbeat packets are generated.

To restore normal operation, do the following:

1. Restore external environment to normal work.
2. Set the **Active OP Mode** option to **Inline**.
3. Select the **Heartbeat Active Mode** option to enable the mode.

## Heartbeat Interval

The M100G1AC generates heartbeat packets to monitor port 0 (Mon0) every **Heartbeat Interval** msec (Default: 3; Minimum: 3; Maximum: 10000). The heartbeat interval should be at least three times less than the value of the **Heartbeat Expire Timer** parameter.

## Heartbeat Expire Timer

The M100G1AC monitors the received packets on monitor port1 (Mon1). If heartbeat packets do not arrive within the time specified in the **Heartbeat Expire Timer** parameter, the M100G1AC will set the **Active OP Mode** option to **Bypass, Tap, or Linkdrop** mode, depending on the predefined settings of the **Heartbeat Active Expired OP Mode** parameter.

To secure reliable detection of application failure, the **Heartbeat Expire Timer** value should be at least three times longer than the **Heartbeat Interval** parameter value (Default: 20; Minimum: 10; Maximum: 50000).

The Heartbeat Expire Timer value is maintained after a reset or power-off event.

## Heartbeat Recover Timer

Use this option to specify the time to recover from a heartbeat-lost event for a bypass segment. When it is set to 0, the segment will recover from a heartbeat-lost event immediately upon receiving of



a heartbeat packet.

### Active OP Mode

When the **Heartbeat Active Mode** option is disabled, the M100G1AC stops sending heartbeat packets, and the user can manually set Active Bypass to one of the following modes: **Inline, Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop mode**, through the **Active OP Mode** option.

### HB Active Expired OP Mode

When the **Heartbeat Active Mode** option is enabled, the M100G1AC sends heartbeat packets on its monitor ports. If the M100G1AC does not receive heartbeat packets from the monitor ports, the M100G1AC switches to **Active Bypass, TAP, TAPI12, TAPA, TAPAI1, TAPAI2, TAPAI12** or **Linkdrop** mode according to the predefined settings of the **Heartbeat Active Expired OP Mode** parameter.

### Heartbeat TX Direction

The heartbeats can be transmitted in any of the following directions:

- From port Mon0
- From port Mon1
- From both ports (Mon0 and Mon1, bidirectional)

### Heartbeat Fail Detect

When the Heartbeat TX Direction option is set to Both (bidirectional, heartbeat packets are transmitted from both port mon0 and port mon1), the Heartbeat Fail Detect criteria can be set to:

- **Bidirectional:** The M100G1AC will change its state if neither monitor ports receive the heartbeat packets. The M100G1AC will restore to its default state if at least one of the monitor ports receives the heartbeat packets.
- **Unidirectional:** The M100G1AC will change its state if either of the monitor ports does not receive heartbeat packets. The M100G1AC will restore to its default state when both monitor ports receive the heartbeat packets.

### Inline Heartbeat Packet

Config

### Bypass Heartbeat Packet

Config

### TAP Heartbeat Packet

The above three heartbeat packet configuration fields enable users to edit or load heartbeat packet content. The packet file can be a binary file or a hex text file (.txt) for a normal IP packet (length  $\geq 64$ ). The hex text file can be a continuous hex string like "11223344aabbccdd....." or contain Space/Tab/LF/CR to separate the bytes like "11 22 33 44 aa bb cc dd....."

- To edit the heartbeat packet content, type strings directly in the fields.
- To load new heartbeat packet content, use the Upload Packet File button. After the packet file is uploaded, the packet content will be displayed in the corresponding field.

### 9.5.1.2 Advanced Features

The following screenshot shows the Advanced Features menu for module configuration.

## Module 1 Configuration

### Segment 1

Heartbeat Setting   **Advanced Features**   RX/TX Error Processing

---

Two Port Link ☐

M2N 

Disabled ▼

M2M ☐

Device Power Off Mode 

Bypass ▼

Link Speed 

100G ▼

Net 0 FEC ☐ Net0 FEC and Net1 FEC must be configured the same

Net 1 FEC ☐

Monitor 0 FEC ☐

Monitor 1 FEC ☐

Commit   Reset

On the **Advanced Features** menu, the user can configure the following:

#### Two Port Link

Enable or disable the 2PL feature. See 5.4.1 Two-port Link for reference.

#### M2N

Enable or disable the M2N feature. See 5.4.2 M2N for reference.

#### M2M

Enable or disable the M2M feature. See Figure 15 M2M for reference.

#### Device Power Off Mode

The M100G1AC supports Disconnect or Bypass (default) mode at system power-off.

- When **Disconnect** is selected, in any event of power-off, the M100G1AC will go into **Disconnect** mode -
  - simulating switch/router cable disconnection on the two network ports.
- When **Bypass** is selected, in any event of power-off, the M100G1AC will go into **Bypass** mode. This is the default mode.

## Link Speed: Speed of the port (100G)

### Net 0 FEC:

Turn on FEC for NET0, only valid for SR4/LR4 modules

### Net 1 FEC:

Turn on FEC for NET1, only valid for SR4/LR4 modules

### Note:

Due to passive bypass requirement, FEC option for NET0 and NET1 ports must be configured the same.

### Monitor 0 FEC: need input

Turn on FEC for MON0, only valid for SR4/LR4 modules

### Monitor 1 FEC: need input

Turn on FEC for MON1, only valid for SR4/LR4 modules  
For FEC operation, see

## 9.5.1.3 RX/TX Error Processing

The following screenshot shows the **RX/TX Error Processing** menu for module configuration.

### Module 1 Configuration

#### Segment 1

Heartbeat Setting
Advanced Features
RX/TX Error Processing

RX/TX Error Trap ☒

RX/TX Error Timeout  sec

RX/TX Error Monitor OP Mode

RX/TX Error Network OP Mode

RX/TX Error Rate Thresh

Commit Reset

The M100G1AC can place itself into **Bypass** or **Linkdrop** mode when it detects RX/TX errors on the monitor or network ports.

On the **RX/TX Error Processing** menu, the user can configure the following:

- **RX/TX Error Trap:** Enable/Disable trap.
- **RX/TX Error Timeout:** Minimal time in seconds between traps (>0)
- **RX/TX Error Monitor OP Mode:** Change bypass mode when the number of errors per second on monitor ports exceed the threshold value. Three modes are available: **Disabled/Bypass/Linkdrop**.
- **RX/TX Error Net OP Mode:** Change bypass mode when the number of errors per second on network ports exceed the threshold value. Two modes are available: **Disabled/Linkdrop**.
- **RX/TX Error Rate Threshold:** >0 (Default: 10)

### 9.5.2 Heartbeat Packet File

Navigate to **Bypass Configuration > Heartbeat Packet File**. The following heartbeat packet configuration page is displayed.

## Heartbeat Packet File

Choose the target heartbeat packet and upload file

Module	Module 1	▼
Segment	Segment 1	▼
Operation Mode	Inline	▼

Upload a .txt with hex string or a binary file to change the heartbeat packet.

Heartbeat Packet File:  No file selected.

This page enables users to change or to load new heartbeat packet content. The packet file can be a binary file or a hex text file (.txt) for a normal IP packet (length >= 64). The hex text file can be a continuous hex string like "11223344aabbccdd....." or contain Space/Tab/LF/CR to separate the bytes like "11 22 33 44 aa bb cc dd....."

To upload a packet file, do the following:

1. Select the module to configure.
2. Select the segment to configure.
3. Select the operation mode: **Inline**, **Bypass**, or **TAP**.
4. Click **Browse** to navigate to the heartbeat packet file that you want to upload.
5. Click **Upload File**. After the packet file is uploaded, you can view the result by navigating to **Bypass**
6. **Configuration > Module > Heartbeat Setting**. The new packet content will be displayed in the
7. corresponding heartbeat packet field at the bottom of the page, for example:

### Inline Heartbeat Packet

[illegible]

## Bypass Heartbeat Packet

## TAP Heartbeat Packet

## 9.6 System

The System tab provides access to the following system information pages:

- General
- Service
- Management interface
- Configurations
- System Dump
- Upgrade
- Reboot/Halt

### 9.6.1 General configuration

Navigate to **System > General** to view or configure general system settings. The following screenshot shows the **General Configuration** page.

## General Configuration


### System

Device Name


### Date/Time

Timezone


New Date  YYYY-MM-DD

 Set Date

New Time  HH:MM:SS

 Set Time

NTP Enabled ☐

NTP Server  IP or hostname, 1-31 bytes

### Log

Log Level

Max Log File Size  1-10(MB)

Remote Log Enabled ☐

Remote Log Server IP

Commit

Reset

The **System** area displays the device name. The default name is **100**.

In the **DateTime** area, the user can configure the following:

- **Timezone:** The default time zone is UTC.
- **New Date:** Set the system date.
- **New Time:** Set the system time.
- **NTP Enabled:** Select whether to synchronize system clock using the NTP protocol.
- **NTP Server:** Set the NTP server using the server IP or hostname.

In the **Log** area, the user can configure the following:

- **Log Level:** A total of eight levels are available, including **DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT,** and **EMERGENCY**.
- **Max Log File Size:** Configure the maximum log file size.
- **Remote Log Enabled:** Select whether to enable the remote log function. When enabled, the M100G1AC will send log messages to the specified remote log server. This function is disabled by default.
- **Remote Log Server IP:** Specify the remote server that is to receive the log messages.

#### 9.6.2 Service settings

Navigate to **System > Service** to view or configure service settings. The following screenshot shows the **Service Configuration** page.

## Service Configuration

Note: Change web/http/https configurations will cause the web access to be temporarily unavailable, please refresh the page.

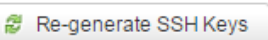
### COM

Speed

Terminal Type

### SSH

Port



### Web

Session Timeout   60-3600 sec

### HTTP

Enabled ☒

Port

### HTTPS

Enabled ☒

Port

SSL Certificate File  No file chosen

SSL Private Key File  No file chosen

The user can configure the following service settings:

- **COM:** Configure the serial COM settings, set the speed and terminal type.
- **SSH:** Configure the listening port. To regenerate SSH keys, click the **Re-generate SSH Keys** button.
- **Web:** Configure the **Web Session Timeout** value in seconds.
- **HTTP:** Enable or disable the http protocol and configure the listening port.
- **HTTPS:** Enable or disable the https protocol and configure the listening port. Upload files to update the SSL certificate and private key of the https service.



**Note:** Changing settings on this page may cause the current connection to be interrupted, and the user should visit the new address accordingly.

### 9.6.3 Management interface configuration

Navigate to **System > Management Interface** to view or configure management settings.

The following screenshot shows the **Management Interface Configuration** page.

## Management Interface Configuration

### Interface

Enabled ☒

MAC address 00:e0:ed:15:50:a2

IP Address

Mask

Gateway

CLI Session Timeout

Permitted IP ☐

### Permitted IP List

IP	Mask
This section contains no values yet	
<input type="text"/>	<input type="text"/>

Note1: IPv4 Address

### DNS Server

IP
192.168.49.4 <input type="button" value="Delete"/>
<input type="text"/>

Note1: IPv4 Address

The user can configure the following management settings.

In the **Interface** area, the user can perform the following:

- Select Enabled to activate management network access. The user can configure the device management IP address, mask and gateway. Disabling the interface will cause Web and SSH access unavailable.
- Configure the CLI Session Timeout value in seconds.
- Select or clear the Permitted IP option. When the option is selected, IP addresses not on the Permitted IP List will be denied access to M100G1AC via SSH or Web.

The **Permitted IP List** lists all permitted IP addresses and masks.

In the **DNS Server** area, the user can add DNS server IP addresses to make DNS service work.

#### 9.6.4 Configurations

Navigate to **System > Configurations** to save your configuration, restore a previous configuration, or to reset to default configuration.

The following screenshot shows the **Configurations** page.

### Configurations

Here you can save and restore your configuration and reset the device to default settings.

Configuration List	current_config	20151225 07:41:04	<input type="radio"/>
	last_config	20151225 02:47:55	<input type="radio"/>
	is_config_20151221142408	20151221 06:24:08	<input type="radio"/>
	is_config_20151127065816	20151127 06:58:19	<input type="radio"/>

Save current configuration as

Upload a configuration file as   No file selected.

Reset to default configuration

The **Configuration List** area lists all previous configuration files. You can select the radio button for the corresponding configuration file and perform any of the following:

**View:** Click this button to view the configuration file.

**Restore:** Click this button to restore the configuration defined in the file.

**Delete:** Click this button to delete the configuration file.

**Download:** Click this button to download the configuration file.

In the **Save current configuration** area, you can save the current configurations using the **Save** button.

In the **Upload a configuration file** area, you can navigate to a configuration file and upload it.

In the **Reset to default configuration** area, you can reset to the default configuration using the **Reset** button.

**Note:** Although configuration downloaded is a text based file containing CLI commands, it can't be tampered with if the user wishes to upload it later back to the M100G1AC device. However sometimes the user may like to copy a current configuration and change some specific configuration like IP address.

### 9.6.5 System Dump

Navigate to **System > System Dump** to delete, create or download system dump files, including coredump files and log files.

The following screenshot shows the **System Dump** page and the available options.

#### System Dump

Here you can create and download system dump files, including coredump files and log files.

##### System Dump File List

<input type="checkbox"/>	Filename	Size(Bytes)	Created Date
<input type="checkbox"/>	<a href="#">is_log_20151225075423.tar.gz</a>	394503	20151225 07:54:24
<input type="checkbox"/>	<a href="#">is_log_20151225074038.tar.gz</a>	393889	20151225 07:40:39
<input type="checkbox"/>	<a href="#">is_log_20151225100111.tar.gz</a>	373847	20151225 02:01:12
<input type="checkbox"/>	<a href="#">is_log_20151225095609.tar.gz</a>	372752	20151225 01:56:10
<input type="checkbox"/>	<a href="#">is_log_20151224185640.tar.gz</a>	371164	20151224 10:56:42
<input type="checkbox"/>	<a href="#">is_log_20151224173946.tar.gz</a>	369532	20151224 09:39:47

☐ Delete

Create system log dump file

To create a system log dump file, click **Create**.

To delete a system log dump file, click **Delete**.

To download a system log dump file, click the file link.

## 9.6.6 Upgrade

Navigate to **System > Upgrade** to view the current firmware version or to upgrade the firmware.

To upgrade the firmware, upload a newer version of firmware image by doing the following:

1. Click **Browse** to navigate to the intended firmware image file.
2. Click **Upload image**. If the image is correct, a confirmation window will be displayed, asking whether to proceed or not.

**Note:** If the user closes the confirmation window without making a decision, the window will be displayed again when the user clicks **System > Upgrade**.

Click **Proceed**. A progress bar is displayed, as shown.

## System

### Flash Image

Upgrade Progress:

Done: 100%



The flash has been upgraded and please reboot the system to make it work.

 Reboot

The upgrade process takes around four minutes, during which the user can stay on the progress page to watch the progress, or can go to other pages and return later to view the result.

4. When upgrade is finished, click **Reboot** to restart the system for the new image to take effect.

### 9.6.7 Reboot/Halt

To reboot or halt the system, navigate to **System > Reboot/Halt**. The following page is displayed.

## Reboot / Halt

Reboot or halt the operating system of the device.

Warning: There are unsaved changes that will be lost while powering off!

 Reboot

 Halt

Click **Reboot** to restart the system. A reboot takes around one minute.

Click **Halt** to turn off the system.

## 9.7 User

The **User** tab provides access to the following user configuration options:

**LOCAL**

**RADIUS**

**TACACS+**

**Change Password**

### 9.7.1 LOCAL

Navigate to **User > LOCAL** to access the local user configuration page, as shown:

**Local**

User

Username	Full Name	Privilege	
is_admin	IS system administrator	Admin	Delete
<input type="text"/>	Add	Note1: 1-31 bytes, [a-z][0-9][_]	

Commit
 Reset

Three types of privileges are provided for a local user: **Admin**, **Normal** or **Readonly**.

**Admin:** Full read-write access to all configuration tabs (**Bypass Configuration/System/User/ SNMP**); privileges to add, delete, or modify local users on the M100G1AC. The initial user account admin is the only administrator account and no other administrator accounts are allowed to be created. This admin account cannot be deleted, and the privileges cannot be modified.

**Normal:** Full read-write access to the **Bypass Configurations** tab and read-only access to other configuration tabs (**System/User/SNMP**).

**Readonly:** Read-only access to all configurations.

### 9.7.2 RADIUS

The M100G1AC supports RADIUS/TACACS+ remote login. RADIUS and TACACS+ cannot be enabled at the same time. To enable either, the other needs to be disabled first.

RADIUS users share the same privilege level, which can be configured through Web or CLI. Navigate to **User > RADIUS** to access the RADIUS configuration page, as shown:

#### RADIUS

##### Global

Enable ☐

User Privilege

Retry

Local Login ☒ [Allow local users login](#)

##### Server

ID	Host	Port	Secret	Timeout(sec)
This section contains no values yet				
<input type="text"/>	<input type="button" value="Add"/> <small>Note1: Number only</small>			

In the **Global** area, the user can configure the following:

**Enable:** Enable RADIUS remote login.

**User Privilege:** Set the user privilege.

**Retry:** Specify how many times to re-send a packet when there is no response from the server.

**Local Login:** Enable local users' login.

In the **Server** area, the user can configure RADIUS server settings, including **IP**, **Port**, **Secret** (encrypt/decrypt packets sent/received from the server) and **Timeout** (value in seconds).

For more information, refer to 4. System management overview.

### 9.7.3 TACACS+

The M100G1AC supports RADIUS/TACACS+ remote login. RADIUS and TACACS+ cannot be enabled at the same time. To enable either, the other needs to be disabled first.

TACACS+ user or user group privilege can be configured on server side by adding a service tag (default is "silc-system", which can be configured through web or cli) to tacacs+ server configuration as below:

```
service = silc-system {
    # 1: readonly; 5: normal; 10: admin
    user-privilege = 10
}
```

And TACACS+ user will be assigned Readonly privilege if the service tag is missing in server configuration.

Navigate to **User > TACACS+** to access the TACACS+ configuration page, as shown:

#### TACACS+

##### Global

Enable ☐

Service Tag  ⓘ Can't be slip/ppp/arap/shell/tty-daemon/connection/system/firewall

Timeout

Local Login ☒ ⓘ Allow local users login

##### Server

ID	Host	Port	Secret
This section contains no values yet			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

ⓘ Note1: Number only



In the **Global** area, the user can configure the following settings:

**Enable:** Enable TACACS+ remote login.

**Service Tag:** Configure the service tag.

**Timeout:** Specify the connection timeout value in seconds.

**Local Login:** Enable local users' login.

In the **Server** area, the user can configure TACACS+ server settings, including **IP**, **Port**, **Secret** (encrypt/decrypt packets sent/received from the server) and **Timeout** (value in seconds).

For more information, refer to 3. System management overview.

#### 9.7.4 Change Password

Navigate to **User > Change Password** to access the password configuration page, as shown:

##### Change local user password

Please enter the new password and confirmation.

User

-- choose a local user --

▼

New Password

6-40 bytes, at least contain 3 of the following: [a-z][A-Z][0-9][Nonalphanumeric]

Confirmation

Save

Reset

The **Admin** user (ID: admin) can change the password for all users.

A **Normal** user or a **Readonly** user can only change his own password.

No previous password is required to set a new password.

The password should be six to 40 bytes, and should contain at least three types of characters from the following character groups:

- [a-z]
- [A-Z]
- [0-9]
- [Non-alpha-numeric]

## 9.8 SNMP


The **SNMP** tab provides access to the following configuration pages:

- **Trap Filter**
- **Agent**

### 9.8.1 Trap Filter

Navigate to **SNMP > Trap Filter** to access the **Trap Filter Configuration** page, as shown:

#### Trap Filter Configuration

- All ☐  Select to enable all types
- System ☐
- Application ☐
- Terminal ☐
- Power ☐
- Sensor ☐
- Fan ☐
- Switch ☐

[Commit](#) [Reset](#)

The SNMP trap control is designed to enable or disable SNMP trap groups, including **Application Fail**, **Bypass**, **Monitor Link**, **Network Link**, **Terminal**, **Error**, and **Update**. All these SNMP traps are disabled by default. To enable a trap group, select the check box next to the group name.

## 9.8.2 Agent

Navigate to **SNMP > Agent** to access the **Agent Configuration** page.

### Agent Configuration

#### State

Enabled ☒

#### Communities

Community Name	Enabled	Full Access
This section contains no values yet		
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Add](#) Note1: 1-31 bytes, [a-z][0-9][\_]

#### Users

User Name	Enabled	Authentication Protocol	Full Access	Password
This section contains no values yet				
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="password"/>

[Add](#) Note1: 1-31 bytes, [a-z][0-9][\_]

#### Trap Hosts

Host Name	Enabled	Version	Community	Auth	Password
This section contains no values yet					
<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="password"/>

[Add](#) Note1: IPV4 Address

[Commit](#) [Reset](#)

In the **State** area, select **Enabled** to enable global SNMP agent configuration.

In the **Communities** area and **Users** area, a **Full Access** option is provided. Select it to grant communities or users write access.

In the **Trap Hosts** area, the user can define the IP address of the SNMP server to which the M100G1AC will send the SNMP traps.

### 9.8.3 Mib File

Navigate to SNMP > Mib File to access the Mib File Download page.

Choose a file and click “Download” to download it.

### 9.9 Logout

To log out from the M100G1AC Web interface, click the Logout tab.

### 9.10 Save

To save your configurations, click the **Save** tab. The **Save Configuration** page allows the user to save current configurations to the non-volatile memory so that the configuration will not be lost after the system reboots.

#### Save Configuration

There are some unsaved changes in current configuration, and they will be lost after system reboots.  
Please click the save button to save current configuration to disk.



## Appendix A Specifications

### M100G1AC 1U host system specifications

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

### M1001Gxx (50um)

### M1001Gxx: Fiber 40Gigabit Ethernet specifications - (100GBase-SR4) Adapters

<b>IEEE standard / Network topology</b>	Fiber Gigabit Ethernet, 100GBase-SR4 (850nm)
<b>Data transfer rate</b>	100G per port
<b>Cables and operating distance</b>	Multimode fiber:50um *50m maximum on OM3 MMF *75m maximum on OM4 MMF  Theoretical distance – Defined as half a distance
<b>Size</b>	102.2mm x161.9 mm x 40.5 mm (4.02" x 6.37" x 2")

	Width x Depth x Height
<b>Operating humidity</b>	0%–90%, non-condensing
<b>Operating temperature</b>	0°C – 40°C (32°F - 104°F)
<b>Storage temperature</b>	-20C–65C (-4F–149F)
<b>EMC certifications</b>	Class B / FCC / CE / VCCI
<b>Safety</b>	UL
<b>MTBF*</b>	> 150,000 hours

### M1001Gxx : LED and connector specifications

<b>LEDs</b>	<p>Green LED per port (Network/Monitor) Activity: LED will blink. Link: LED will turn on.</p> <p>Two LEDs: Green: Inline Mode Yellow (Orange): Non-inline mode - Bypass, TAP, Disconnect</p> <p>HB status LED: Blinking Green – Heartbeat is active Off – Heartbeat is not active</p>
<b>Connectors</b>	<p>Network: 2 MPO Monitor: 2 CFP4+</p>

### M1001Gxx

#### M1001Gxx: Fiber 100Gigabit Ethernet specifications - (100GBase-LR4) Adapters

<b>IEEE standard / Network topology</b>	Fiber Gigabit Ethernet, 100GBase-LR4 (1310nm)
<b>Data transfer Rate</b>	100Gbit/s per port
<b>Cables and operating distance</b>	<p>Single mode fiber: 5000m maximum at 9 um ** **Theoretical distance – Defined as half a distance</p>
<b>Insertion loss (Passive: Normal mode)</b>	<p>Typical: 1.2 dB Maximum: 1.6dB</p>
<b>Insertion loss ( Passive: Bypass mode)</b>	<p>Typical: 1.2 dB Maximum: 1.6dB</p>

<b>Voltage</b>	12V +/-5%, 5VSB+/-5%, 5V +/-5%
<b>Size</b>	102.2mm x161.9 mm x 40.5 mm (4.02" x 6.37" x 2") Width x Depth x Height
<b>Operating humidity</b>	0%–90%, non-condensing
<b>Operating temperature</b>	0°C – 40°C (32°F - 104°F)
<b>Storage temperature</b>	-20°C–65°C (-4°F–149°F)
<b>EMC certifications</b>	Class B FCC / CE / VCCI /
<b>Safety</b>	UL
<b>MTBF*</b>	> 150,000 hours

## Appendix B Safety precautions

### Battery



#### 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.
- Be sure to replace the battery with the same type. There is a risk of explosion if the battery is replaced by an incorrect type.
- To avoid the possibility of electric shock, all power cords must be disconnected from the switch before starting replacing the battery.

### Fiber optic ports



#### 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.

## Rack mounting

### Observe the following guidelines when mounting M100G1AC to the rack:

- A.** Verify that the maximum operating ambient temperature inside a rack assembly does not exceed 50C (122F).
- B.** Verify that a sufficient clear space is provided around the M100G1AC unit to allow sufficient amount of air flow for safe operation of the product. Keep 25 mm (0.98 inch) 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 the product 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 M100G1AC 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.

## Appendix B Safety precautions

### NET-SNMP Copyright.

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

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

Copyright 1989, 1991, 1992 by Carnegie Mellon University  
Derivative Work - 1996, 1998-

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

All Rights Reserved

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

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

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

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

Garland Technology | 716.242.8500 | [garlandtechnology.com/support](http://garlandtechnology.com/support)  
Copyright © 2021 Garland Technology, LLC. All rights reserved.

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

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

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

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

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

----- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.



All rights reserved.

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

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

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

\* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

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

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

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.  
Use is subject to license terms below.

This distribution may include materials developed by third parties.

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

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

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

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

\* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote

products derived from this software without specific prior written permission.

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

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

Copyright (c) 2003-2006, Sparta, Inc

All rights reserved.

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

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

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

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

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

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](http://www.garlandtechnology.com/support)