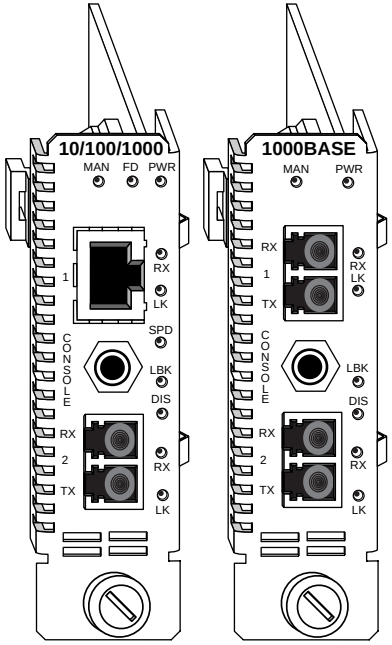
Radiance Gigabit Ethernet Services Line Card



Installation and User Guide

Models: R851-1S / R851-SS

Radiance Gigabit Ethernet Services Line Card

Line Cards:

R851-1S _____ 10/100/1000 Mbps RJ-45 to 1000BASE-X
R851-SS _____ 1000BASE-X to 1000BASE-X

Small Form-Factor Pluggable (SFP) Fiber Optic Transceivers:

O211-M5_____ SFP MM/LC (850 nm, 16 dB) 500 m
O211-10 _____ SFP SM/LC (1310 nm, 16 dB) 10 km
O211-25 _____ SFP SM/LC (1310 nm, 19 dB) 25 km
O211-40 _____ SFP SM/LC (1550 nm, 23 dB) 40 km
O211-70 _____ SFP SM/LC (1550 nm, 28 dB) 70 km
O211-1A _____ SFP SM/LC (1550 nm, 36 dB) 100 km

Bidirectional Wavelength Division Multiplexing (BWDM) SFP Fiber Optic Transceivers:

O311-10-31 _____ SFP SM/SC BWDM (1310 nm/1490 nm, 24 dB) 10 km
O311-10-49 _____ SFP SM/SC BWDM (1490 nm/1310 nm, 24 dB) 10 km

Coarse Wavelength Division Multiplexing (CWDM) SFP Fiber Optic Transceivers:

O411-80-31 _____ SFP SM/LC CWDM (1310 nm, 28 dB @ GbE) 80 km
O411-80-33 _____ SFP SM/LC CWDM (1330 nm, 28 dB @ GbE) 80 km
O411-80-35 _____ SFP SM/LC CWDM (1350 nm, 28 dB @ GbE) 80 km
O411-80-37 _____ SFP SM/LC CWDM (1370 nm, 28 dB @ GbE) 80 km
O411-80-39 _____ SFP SM/LC CWDM (1390 nm, 28 dB @ GbE) 80 km
O411-80-41 _____ SFP SM/LC CWDM (1410 nm, 28 dB @ GbE) 80 km
O411-80-43 _____ SFP SM/LC CWDM (1430 nm, 28 dB @ GbE) 80 km
O411-80-45 _____ SFP SM/LC CWDM (1450 nm, 28 dB @ GbE) 80 km
O411-80-47 _____ SFP SM/LC CWDM (1470 nm, 28 dB @ GbE) 80 km
O411-80-49 _____ SFP SM/LC CWDM (1490 nm, 28 dB @ GbE) 80 km
O411-80-51 _____ SFP SM/LC CWDM (1510 nm, 28 dB @ GbE) 80 km
O411-80-53 _____ SFP SM/LC CWDM (1530 nm, 28 dB @ GbE) 80 km
O411-80-55 _____ SFP SM/LC CWDM (1550 nm, 28 dB @ GbE) 80 km
O411-80-57 _____ SFP SM/LC CWDM (1570 nm, 28 dB @ GbE) 80 km
O411-80-59 _____ SFP SM/LC CWDM (1590 nm, 28 dB @ GbE) 80 km
O411-80-61 _____ SFP SM/LC CWDM (1610 nm, 28 dB @ GbE) 80 km

Accessory:

R800-CA_____ Console Cable

Contents

Chapter 1: Overview

The feature-rich Radiance R851 Gigabit Ethernet Services Line Card is a three-port network interface device (NID) designed for superior manageability. The R851-1S provides a 10/100/1000BASE-T user port and a small form-factor pluggable (SFP) network port with numerous wavelength and distance options. This device is ideal for environments that are gradually migrating toward GbE. For fiber networks, the R851-SS provides two SFP-based ports, one each for the user and the network interfaces. Both models include a third console port for direct management of the NID.

Both data interfaces on the GbE services line card support baby giant frames (up to 1532 bytes untagged and 1536 bytes tagged) and auto-negotiation. When auto-negotiation is enabled, the copper port on the R851-1S auto-detects MDI-II/MDI-X[1]. The copper port also supports configurable flow control (forced collisions in half duplex and PAUSE frames in full duplex).

Management software for the R851 can be downloaded in the field for future updates. Two different versions for both the operational software and the FPGA firmware may be stored on the device.

Advanced management capabilities include temperature and voltage monitoring, interface control enable/disable, a built-in optical power meter, loopback testing, Link Loss Carry Forward, Link Loss Return, and Far End Fault to assist in troubleshooting.

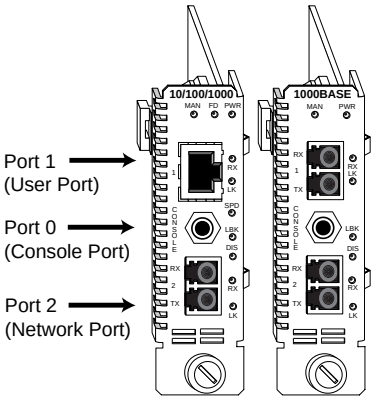
Path Fault Management

As the CPE demarcation point, the R851 services line card verifies network connectivity by responding to ping requests addressed to unicast and subnet broadcast addresses. Through SNMP, the R851 can also deliver information on the health and status of the device and its network connections. SNMP provides Internet-standard management and can be used for surveillance and fault management.

Additional features include sophisticated management access control which protects the system and network connections from denial of service attacks from the user's network. Management access control automatically discards unauthorized traffic received over the user port,

1.When forcing 10 or 100 Mbps, a crossover cable may be needed.

making the device impervious to all traffic conditions and traffic patterns. Access control is also provided by reserving the 0x000 VLAN for use with management. This management VLAN can be made unavailable to users by changing the VLAN ID, then traffic received from the user's network over this VLAN will be discarded.



Key Features

The Radiance services line card provides the following key features:

- 10/100/1000 Mbps support on the R851-1S copper port.
- Auto-negotiation on both ports.
- Built-in optical power meter that enables proactive maintenance by eliminating the need to disable the fiber link(s) for testing.
- Real-time monitoring of line card temperature and power.
- Duplex and speed control on the R851-1S copper port.
- Link Loss Return (LLR), Link Loss Carry Forward (LLCF), and Far End Fault (FEF) to aid in troubleshooting.
- Loopback mode to test for connectivity and link integrity.
- Automatic MDI-II/MDI-X conversion on the R851-1S copper port when auto-negotiation is enabled.
- Accept and process ARP messages, and respond to ARP requests and replies.

- Console port for direct device communication.
- Half- and full-duplex flow control on the R851-1S copper port.
- Small form-factor pluggable (SFP) transceivers on the fiber port(s) with support for distances up to 100 km.
- Hot swappable board and optics.
- Full signal retiming, reshaping, and reamplification (3 Rs).
- Ping support for network path connectivity testing.
- Transparency to user data traffic, including single and double VLAN-tagged Ethernet frames.
- Field-programmable for upgrading management software. Traffic filtering and forwarding to provide access control security.
- Filtering at full line rate in both directions under all frame sizes and mixed traffic conditions.
- Compatibility with industry-standard SNMP-based management applications.
- SNMPv1 support.
- TFTP support.
- DHCP client support.
- Telnet support.
- •A unique end-station MAC address.
- Support for SNMPv1 community based profiles and views for read-only, read-write, and administrative access.
- Line rate performance of up to 1,488,000 minimum-sized frames per second.
- Transparent MAC-layer forwarding and filtering. (No Spanning Tree)
- Compliance with IEEE 802.1Q-2002 VLAN bridge forwarding aspects.
- Two service class levels: management and user.
- Static ARP and IP address entries.

Chapter 2: Installation Guide

Safety Warning

Electrostatic Discharge Warning
Electrostatic discharge precautions should be taken when handling any line card. Proper grounding is recommended (i.e., wear a wrist strap).

1. Unpack the Line Card

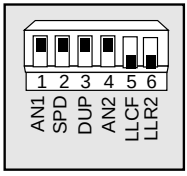
Your order has been provided with the safest possible packaging, but shipping damage does occasionally occur. Inspect your line card(s) carefully. If you discover any shipping damage, notify your carrier and follow their instructions for damage and claims. Save the original shipping carton if return or storage of the card is necessary.

2. Set the Switches

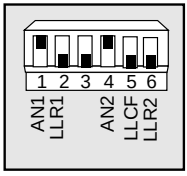
A bank of six DIP switches is located on the back of the card. These switches allow you to select from several modes of operation. Functional switches are clearly marked on the card's circuit board. Refer to the following tables for the proper setting of the DIP switches.

When setting DIP switches, the UP position is when the lever of the DIP switch is pushed away from the circuit board. The DOWN position is when the lever is pushed toward the board.

Default Switch Settings



R851-1S



R851-SS

Table 1: R851-1S DIP Switches

Switch Label	Position	Function
AN1	UP (default)	Auto-negotiation is enabled. Port 1 advertises 1000 Mbps full duplex capability to its link partner.
	DOWN	Auto-negotiation is disabled. Speed and duplex are determined by the SPD and DUP switch settings.
SPD	UP (default)	Port 1 is set to 100 Mbps when AN1 is disabled.
	DOWN	Port 1 is set to 10 Mbps when AN1 is disabled.
DUP	UP (default)	Port 1 is set to full duplex when AN1 is disabled.
	DOWN	Port 1 is set to half duplex when AN1 is disabled.
AN2	UP (default)	Auto-negotiation is enabled. Port 2 advertises 1000 Mbps full duplex capability to its link partner.
	DOWN	Auto-negotiation is disabled. Port 2 is set to 1000 Mbps full duplex.
LLCF	UP	Link Loss Carry Forward is enabled.
	DOWN (default)	Link Loss Carry Forward is disabled.
LLR2	UP	Link Loss Return is enabled on Port 2.
	DOWN (default)	Link Loss Return is disabled on Port 2.

Table 2: R851-SS DIP Switches

Switch Label	Position	Function
AN1	UP (default)	Auto-negotiation is enabled. Port 1 advertises 1000 Mbps full duplex capability to its link partner.
	DOWN	Auto-negotiation is disabled. Port 1 is set to 1000 Mbps full duplex.
LLR1	UP (default)	Link Loss Return is enabled on Port 1.
	DOWN	Link Loss Return is disabled on Port 1.
AN2	UP (default)	Auto-negotiation is enabled. Port 2 advertises 1000 Mbps full duplex capability to its link partner.
	DOWN	Auto-negotiation is disabled. Port 2 is set to 1000 Mbps full duplex.
LLCF	UP (default)	Link Loss Carry Forward is enabled.
	DOWN	Link Loss Carry Forward is disabled.
LLR2	UP	Link Loss Return is enabled on Port 2.
	DOWN (default)	Link Loss Return is disabled on Port 2.

R851-1S Switches

Auto-Negotiation (AN1)

AN1 is the auto-negotiation switch for Port 1. To operate at 1000 Mbps, AN1 must be enabled. When auto-negotiation is enabled, the port advertises 10/100/1000 Mbps half/full duplex capability to its link partner. When auto-negotiation is disabled, the speed and duplex for Port 1 are set through the SPD and DUP switches.

Speed (SPD)

The speed switch applies to Port 1 and is effective only when auto-negotiation (AN1) is disabled. Port 1 is set to 100 Mbps when the SPD switch is up, and 10 Mbps when the switch is down.

Duplex (DUP)

The duplex switch applies to Port 1 and is effective only when auto-negotiation (AN1) is disabled. Port 1 is set to full duplex when the DUP switch is up, and half duplex when the switch is down.

Auto-Negotiation (AN2)

AN2 is the auto-negotiation switch for Port 2. When auto-negotiation is enabled, Port 2 advertises 1000 Mbps full duplex capability to its link partner. The mode of operation is determined through the auto-negotiation process. If auto-negotiation is disabled, Port 2 will be set to 1000 Mbps full duplex.

Link Loss Carry Forward (LLCF)

Link Loss Carry Forward (LLCF) is provided as an aid in troubleshooting a remote connection. When LLCF is enabled, loss of the receive signal at Port 1 prevents Port 2 from transmitting idle link signals onto the cable. Conversely, if Port 2 does not detect a receive signal, Port 1 will not transmit idle link signals. When LLCF is disabled (default), the card continuously transmits idle link signals. The switch enables/disables LLCF on both ports simultaneously. Refer to the “Link Loss Carry Forward (LLCF)” on page 66 in the User Guide section for additional information.

Link Loss Return (LLR2)

Link Loss Return (LLR) is only applicable to Port 2. When LLR is enabled, loss of the receive signal at the fiber port shuts down its own transmitter. When LLR is disabled (default), the fiber port continually transmits idle link signals. Refer to “Link Loss Return (LLR)” on page 64 in the User Guide section for additional information.

R851-SS Switches

Auto-Negotiation (AN1 and AN2)

Auto-negotiation is supported independently on each port. When auto-negotiation is enabled, the port advertises 1000 Mbps full duplex capability to its link partner. The mode of operation is determined through the auto-negotiation process. If auto-negotiation is disabled, the port will be set to 1000 Mbps full duplex. Use AN1 for Port 1 and AN2 for Port 2.

Link Loss Carry Forward (LLCF)

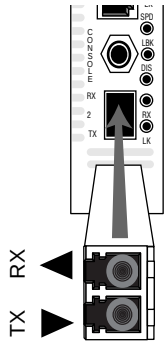
Link Loss Carry Forward (LLCF) is provided as an aid in troubleshooting a remote connection. When LLCF is enabled, loss of the receive signal at Port 1 prevents Port 2 from transmitting idle link signals onto the cable. Conversely, if Port 2 does not detect a receive signal, Port 1 will not transmit idle link signals. When LLCF is disabled (default), the card continuously transmits idle link signals. The switch enables/disables LLCF on both ports simultaneously. Refer to the “Link Loss Carry Forward (LLCF)” on page 66 in the User Guide section for additional information.

Link Loss Return (LLR1 and LLR2)

Link Loss Return (LLR) is supported independently on each port. When LLR is enabled, loss of the receive signal at that port shuts down its own transmitter. For example, if LLR is enabled on Port 2 and its receiver stops detecting link pulses, then Port 2’s transmitter will stop sending link pulses. When LLR is disabled (default), the port continually transmits idle link pulses. Refer to “Link Loss Return (LLR)” on page 64 in the User Guide section for additional information. Use LLR1 for Port 1 and LLR2 for Port 2.

3. Install the SFP Optics

The R851-1S and R851-SS require one or two small form-factor pluggable (SFP) optics. Each set of optics is shipped separately. To install the optics, align the SFP module so the receiver (▲) is positioned above the transmitter (▼). For a BWDM module, align it so the visible part of the circuit board located at the back of the module is to the right. Slide the module into the empty slot. Push the SFP firmly in place. Remove the protective covering on the connector.

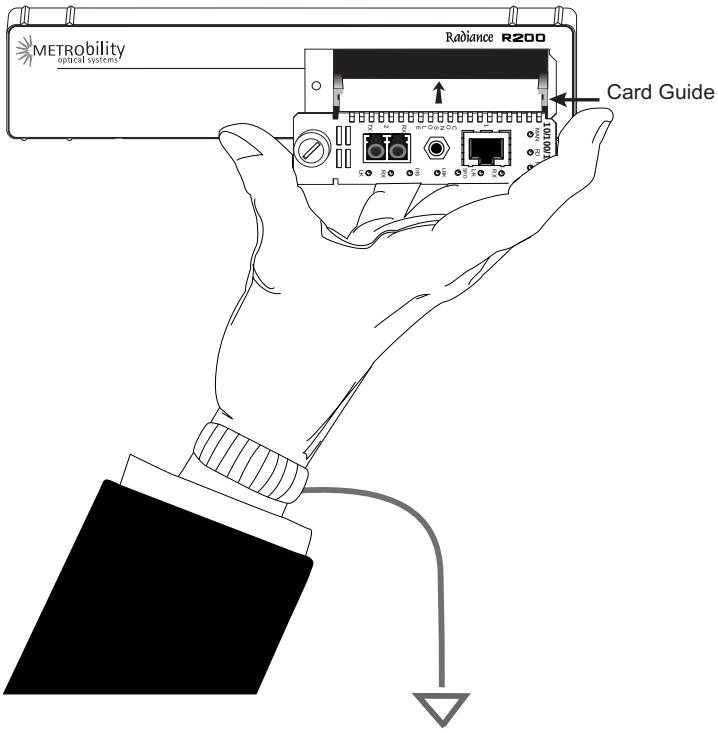


Important: *The Radiance services line card is designed and tested to operate using only Metrobility-supplied SFP transceivers. Safety, performance, and reliability are guaranteed only when Metrobility transceivers are used.* ***Installing unspecified parts may damage the product and will void the unit's warranty.***

4. Install the Line Card

The Radiance services line card offers the ease of plug-and-play installation and is hot-swappable. The card must be firmly secured to the chassis before network connections are made. Follow the simple steps outlined below to install your line card.

- Grasp the card by the front panel as shown.

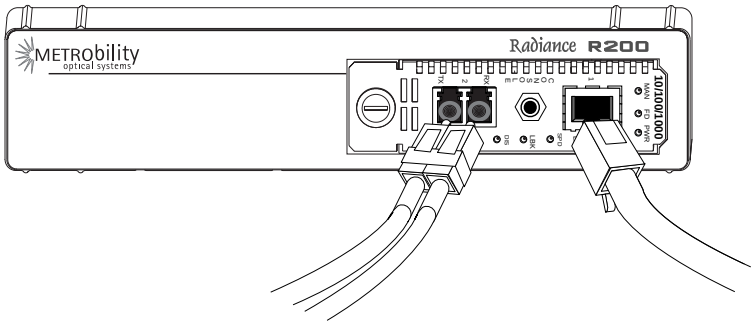


- Insert the card into a slot in the chassis. Make sure that the top and bottom edges of the board are aligned with the card guides in the chassis. Do not force the card into the chassis unnecessarily. It should slide in easily and evenly.
- Slide the card in until the top and bottom edges of the front panel are flush and even with the edges of the chassis.
- To secure the card to the chassis, turn the thumbscrew clockwise until it is snug. The card is now properly installed and ready for connection to the network.

Note: *Metrobility recommends using dual power supplies if more than twelve (12) R851-SS services line cards are installed in an R5000 chassis* **and** *the operating environmental ambient temperature is expected to exceed 40° C. This will ensure adequate cooling for a full complement of sixteen (16) R851-SS line cards in the R5000 in operating environments up to 50° C.*

5. Connect to the Network

To connect the line card to the network, remove the dust plugs from the SFP optics and insert the cables into the appropriate connectors as illustrated below. Make sure the card is secured to the chassis before making network connections.



Twisted-Pair Interface (R851-1S only)

The twisted-pair port provides a shielded RJ-45 connector that supports a maximum segment length of 100 meters.

Fiber Optic Interface

The R851-1S and R851-SS services line cards provide one or two fiber optic ports, respectively. For maximum flexibility in designing or expanding your network, these fiber ports support any combination of the following Metrobility small form-factor pluggable (SFP) transceivers. Each transceiver provides as a set of LC or SC connectors. The maximum distance and cable type supported by the SFP transceivers is as follows:

Model #	Distance	Fiber Type
O211-M5	500 m	MM
O211-10	10 km	SM
O211-25	25 km	SM
O211-40	40 km	SM
O211-70	70 km	SM

Model #	Distance	Fiber Type
O211-1A	100 km	SM
O311-10-xx	10 km	SM (BWDM)
O411-80-xx	80 km	SM (CWDM)

Important: *The distances noted are for reference purposes only. The most important factor to achieve the desired distance is the optical power budget. Metrobility specifications indicate the typical transmit power budget. The actual distance is a function of the fiber type and quality, the number and quality of splices, the type and quality of connectors, the transmission loss, and other physical characteristics.*

When making fiber optic connections, make sure that the transmit (TX) optical fiber of the services line card connects to the receive (RX) optical fiber of the connected device, and that the transmit (TX) optical fiber of the device connects to the receive (RX) optical fiber of the services line card.

BWDM Interface

The bidirectional wavelength division multiplexed (BWDM) transceiver provides one singlemode SC connector that supports a maximum segment length of 10 km. BWDM transceivers must always be used in complementary pairs. That is, the O311-10-31 must be connected to the O311-10-49. The O311-10-31 transmits data at a wavelength of 1310 nm and receives at 1490 nm. Correspondingly, the O311-10-49 transmits data at 1490 nm and receives at 1310 nm.

Use the link (LK) LEDs on the front panel of the card to verify correct segment connectivity. As you insert the cable into each port, the LK LED will be lit if the following conditions are met:

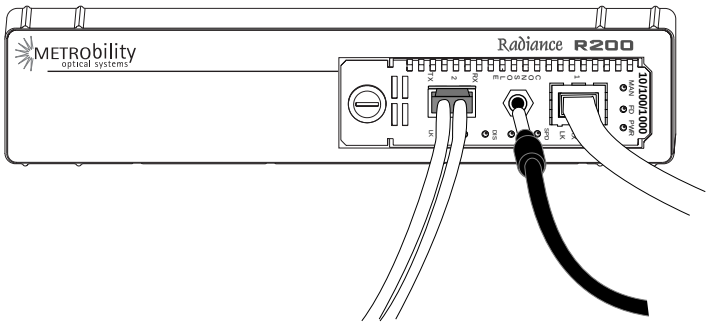
- Power is being applied to the chassis.
- There is an active device connected to the other end of the cable, and it is sending idle link signals.
- All connections are secure and the cables are undamaged.
- Both ends of the cable are set to the same auto-negotiation state. To maximize device compatibility, the R851 is shipped with auto-negotiation enabled on both ports. If necessary, disable auto-negotiation and set full duplex on the fiber port of the remote device to establish link.

For information on replacing the SFP transceiver, refer to “Changing the SFP Transceiver” on page 69 in the User Guide section.

Console Port (optional)

Follow the instructions in this section if you are using a console cable (R800-CA) to communicate with the R851.

Remove the dust plug from the console port. Using the R800-CA null-modem console cable, connect the console port on the R851 to the serial port on your PC. The cable provides a three-conductor in-line plug for insertion into the console port jack on the line card and a female DB9 connector to connect to the PC’s DB9 port.

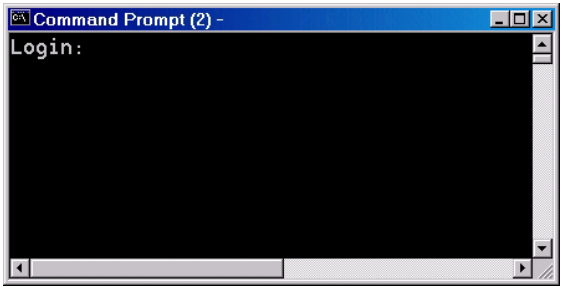


Note: *Do not remove the dust plug from the console port until you are ready to connect the console cable to the port. When you remove the console cable, please replace the port’s dust plug.*

The PC terminal session parameters are as follows:

57,600 baud / 8 bits / 1 stop bit / no parity / no flow control

Following power-up, the boot image is automatically executed. It starts by performing a system initialization, followed by diagnostic tests. After diagnostics are completed successfully, a login prompt will appear on the console screen. If necessary, press <Enter> to get the login prompt.



If the diagnostics are unsuccessful, a failure message will appear.

When device configuration is complete, disconnect the console cable and reinsert the dust plug.

Chapter 3: Management

This section contains information regarding the management and software configuration options available on the Radiance GbE services line card. Management access (SNMP and telnet) are enabled on both ports.

Default Software Settings

CLI Access . . . . . Enabled

DHCP Client . . . . . Enabled

DHCP Server Address 0.0.0.0

DHCP Max Retries Before Timeout . . . . . 3 (28 seconds)

Far End Fault . . . . . Disabled

Full-Duplex Flow Control . . . . . Disabled

Half-Duplex Flow Control . . . . . Disabled

ICMP . . . . . All Enabled

IP Address (zeroconf) 169.254.0.0

Layer 2 Control Protocols . . . . . All Forwarded

Loopback Mode . . . . . Disabled

Loopback Timeout . . . . . 30 seconds

Management Access . . . . . Enabled (Ports 0 and 2); Disabled (Port 1)

Management VLAN identifier . . . . . 0 (Disabled)

Network Mask 255.255.0.0

OAM Admin State . . . . . Disabled (Port 1); Enabled (Port 2)

OAM Mode . . . . . Passive (Port 1); Active (Port 2)

Port Management . . . . . Enabled

Port State . . . . . Enabled

SNMP Access . . . . . Enabled

SNMP Administrative Community String . . . . . admin

SNMP Read-Only Community String . . . . . public

SNMP Read-Write Community String. . . . . .private

Trap Destination Community String . . . . . public

Trap Destination IP Address 0.0.0.0

Trap Destination UDP Port 162

User VLAN . . . . . Disabled

Managed Objects

MIB-II

The Radiance GbE services line card supports the following standard Management Information Base (MIB-II) managed object groups, pertaining only to the end-station traffic. Objects from within these MIB groups are accessible by and available to SNMP-based management stations over UDP/IP.

- System (end-station only)
- Interfaces (end-station and data interface)
- IpNetToMedia (end-station only)
- IP (end-station only)
- ICMP (end-station only)
- TCP (end-station only)
- UDP (end-station only)
- SNMP (end-station only)
- AT (end-station only)

Enterprise-Specific Objects

Metrobility-specific managed objects provide control of the following objects:

- End-station IP addressing information
- SNMP access communities
- Up to 4 SNMP trap destination addresses and communities
- Download server addresses

- Download management software
- Interface control (enable/disable)
- Input/output laser levels
- Management VLAN
- Management port

The Metrobility enterprise ID number is 10527.

Remote Management Statistics

Through software, you can view Remote Monitoring (RMON) statistics for the Radiance GbE services line card.

Each port on the card supports the complete RMON Group 1 statistics outlined in RFC 2819 and RFC 3273.

RFC 2819

etherStatsOctets
etherStatsPkts
etherStatsBroadcastPkts
etherStatsMulticastPkts
etherStatsCRCAlignErrors
etherStatsUndersizePkts
etherStatsFragments
etherStatsJabbers
etherStatsCollisions
etherStatsPkts64Octets
etherStatsPkts65to127Octets
etherStatsPkts128to255Octets
etherStatsPkts256to511Octets
etherStatsPkts512to1023Octets
etherStatsPkts1024to1518Octets
etherStatsOversizePkts
etherStatsDropEvents

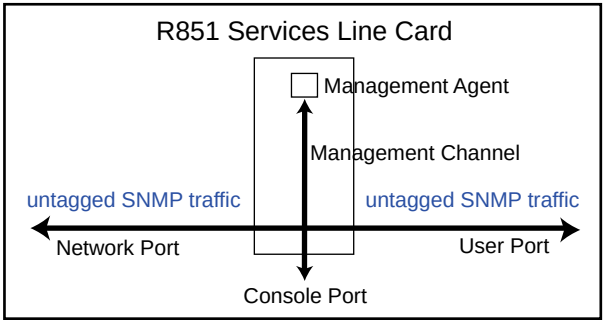
RFC 3273

etherStatsHighCapacityOverflowPkts
etherStatsHighCapacityPkts
etherStatsHighCapacityOverflowOctets
etherStatsHighCapacityOctets
etherStatsHighCapacityOverflowPkts64Octets
etherStatsHighCapacityPkts64Octets
etherStatsHighCapacityOverflowPkts65to127Octets
etherStatsHighCapacityPkts65to127Octets
etherStatsHighCapacityOverflowPkts128to255Octets
etherStatsHighCapacityPkts128to255Octets
etherStatsHighCapacityOverflowPkts256to511Octets

etherStatsHighCapacityPkts256to511Octets
etherStatsHighCapacityOverflowPkts512to1023Octets
etherStatsHighCapacityPkts512to1023Octets
etherStatsHighCapacityOverflowPkts1024to1518Octets
etherStatsHighCapacityPkts1024to1518Octets

Setting a Secure Management Channel

By default, the R851's VLAN identifier (VID) is 0, which indicates no internal management VLAN. In this state, the card forwards all untagged SNMP traffic through both ports, as illustrated below. No security is provided, which means any device connected to any port can make configuration changes to the R851.



Through software, you can create a secure management channel by assigning it a new management VID[2]. The most secure configuration is to have only one port (typically, the network port) enabled for management. This is the recommended configuration, and it allows you to restrict access to the card's management agent, thus preventing unauthorized modifications and other misuses.

The following table describes the management options available on the R851 along with the security vulnerabilities associated with each configuration.

2.Valid management VLAN IDs are in the range 1 to 4094.

Table 1: R851 Management Options and Vulnerabilities

Configuration	Configuration Description	Vulnerabilities
Management VLAN (single port)	A management VLAN ID is assigned to one of the ports. Only frames that contain this VID and are from the specified port are allowed access to the R851 management agent.	None
No Management VLAN (single port)	One port is configured for management. Any device connected to this port can manage the R851.	User could respond to ARP request and steal R851's IP address.
Management VLAN (both ports)	A management VLAN ID is specified. Any frame that contains the VID, regardless of its source, is allowed to access the R851 management agent.	Denial of service due to misuse of unicast MAC address, or broadcast on the specified management VLAN if the user port is also a member.
No Management VLAN (both ports) DEFAULT SETTING	No security. Any device connected to either port can manage the R851.	Untagged broadcast volume could overrun traffic to management port. User could respond to ARP and steal IP address.

Once a management VID has been configured, set it back to 0 to disable VLAN management.

The R851 transparently passes reserved multicast protocols such as IEEE 802.3ad, BPDU, GMRP, and GVRP. Transporting these protocols, however, can introduce additional possibilities for denial-of-service attacks including traffic volume from:

- MAC addresses 01-80-C2-00-00-00 through 01-80-C2-00-00-10
  - — BPDU
  - — 802.3 slow protocols (LACP, Marker and OAM)
- GMRP and GVRP

The following table describes the misuses that could cause denial of service when using reserved multicast protocols along with the various management configurations.

Table 2: R851 Management Vulnerabilities When Using Reserved Multicast Protocols

Configuration	Vulnerabilities
Management VLAN (single port) with reserved multicast	Denial of service through misuse of reserved multicast traffic.
No Management VLAN (single port) with reserved multicast	Denial of service through misuse of reserved multicast or untagged broadcast. Untagged broadcast volume could overrun traffic to management port. User could respond to ARP and steal R851's IP address.
Management VLAN (both ports) with reserved multicast	Denial of service through misuse of reserved multicast, unicast MAC address, or broadcast on the specified management VLAN if the user port is also a member.
No Management VLAN (both ports) with reserved multicast	Denial of service through misuse of reserved multicast, unicast MAC address, or untagged broadcast. Untagged broadcast volume could overrun traffic to management port. User could respond to ARP and steal the IP address.

Software Settings

Several functions and settings on the Radiance GbE services line card can be modified only through software commands. This section describes the card's management features including IP addressing management.

IP Addressing Management

You can configure the R851 to obtain its IP addressing information (IP address, network mask, and default gateway) through any of the following means:

- DHCP assignment
- Manual configuration
- Default value

DHCP Assignment

By default, the R851 has DHCP enabled for obtaining its IP addressing information. When DHCP is enabled, the R851 enters a discovery mode to locate a DHCP server. The card makes up to three[3] attempts to resolve its IP addressing information. If any of the attempts is successful,

3. The max number of retires is configurable. The retry count starts at 4 seconds and doubles for each additional retry (1 = 4 seconds, 2 = 12 seconds, 3 = 28 seconds, 4 = 60 seconds, 5 = 124 seconds)

the card will use the information assigned by the DHCP server. The card will also save the DHCP server's IP address along with the address lease time. Once the addressing information is acquired, the R851 preserves it in memory and renews it continuously. However, the addressing information is not preserved across power cycles. If the card is reset or loses power, it will enter the discovery mode again and attempt to obtain new IP addressing information.

When DHCP is disabled, the R851 uses its last known IP addressing information (i.e., the address that was used to issue the command to disable DHCP). After the R851 successfully acquires its addressing information, through whatever means, we recommend disabling DHCP if you want to ensure that the card always uses this information. The IP addressing information is retained across power cycles when DHCP is disabled.

Manual Configuration

Regardless of the DHCP setting, IP addressing information can be assigned manually. When manually entering the IP addressing information via SNMP, you must also apply the changes by setting mosAdminApplyIPChanges to 1 in the METROBILITY-ADMIN-MIB. The R851 will verify that the information you entered is valid and begin using the new values if there are no problems. If for any reason there is a conflict, the R851 will send a generic SNMP error.

Saving the IP information across power cycles depends on the DHCP setting:

- If DHCP is disabled, the new address will be stored and preserved. If you want to save the addressing information through resets and power cycles, make sure DHCP is disabled after the information is entered successfully.
- If DHCP is enabled, the R851 will enter the discovery mode at each power cycle and attempt to obtain new IP addressing information. The manually configured information will be maintained across a power cycle only until a DHCP server assigns it a new IP address, or until someone manually enters the IP addressing information again.

Default Value

To return the R851's IP address, network mask, and gateway back their factory defaults, follow the procedure described in Resetting the Board. Resetting the board using this method forces all software settings back to their original values.

Start-up Failure

During the initial discovery mode, if a DHCP server is not found within the timeout period[4], the R851 will generate its own IP address. Once an address is generated, the R851 enters a probing phase to verify that the address is unique. If the address is identical to one previously claimed by another device, the R851 will generate a new address repeatedly until it is successful.

Note: *Do not send ARP requests (pings) to the R851 during its initialization. All ARP requests received during the probing phase[5] are interpreted as address collisions and discarded. If a collision occurs, the R851 will immediately discard the address it is verifying and generate another one.*

If DHCP is enabled, every five minutes following a successful self-generated address assignment, the R851 will attempt to acquire its addressing information by locating a DHCP server.

If DHCP is disabled, the R851 will maintain its last known IP addressing information regardless of how the information was acquired, even if it was self-generated.

Far End Fault

Far End Fault (FEF) is only applicable to fiber ports. FEF allows a management station to receive notification of a failure in the remote R851's network port receiver. When two services line cards are connected through their network ports, FEF allows the local card to detect a failure in the remote card's fiber receiver. When FEF is enabled, the local R851 will send an SNMP alarm to its trap destination(s) if a far end fault condition is detected. No alarm will be sent if the condition occurs but FEF is disabled.

4. The timeout period depends on the number of retries. The timeout period is configurable from 4 seconds (# of retries = 1) up to 124 seconds (number of retries = 5).
5. The probing phase lasts approximately 6 seconds.

Full-Duplex Flow Control

Full-duplex flow control is only applicable to the copper port (Port 1) on the R851-1S. It is used to avoid dropping frames during periods of network congestion. If full-duplex flow control is enabled, the port will issue a PAUSE frame whenever there is no buffer space available for incoming frames. Full-duplex flow control applies only when the copper port is in full-duplex mode with auto-negotiation enabled. Additionally, during the negotiation process, the port's link partner must indicate support for PAUSE frames.

The following table describes when full-duplex flow control is enabled/disabled. In the table, "Port 1's Link Partner" is the flow control capability of the device connected to Port 1. The Link Partner's capability is obtained through auto-negotiation. 0 = disabled, 1 = enabled, and X = not applicable.

Table 3: Full-Duplex Flow Control Modes

Port 1's Link Partner	Full-Duplex Flow Control Settings	Auto-Negotiation	Full-Duplex Flow Control
X	X	0	Disabled
0	0	1	Disabled
0	1	1	Disabled
1	0	1	Disabled
1	1	1	Enabled

Half-Duplex Flow Control

Half-duplex flow control is only applicable to the copper port (Port 1) on the R851-1S. When that port is operating at half duplex, the R851 line card provides an option to activate backpressure flow control. If half-duplex flow control is enabled, the card will generate a jamming pattern to force a collision whenever it cannot allocate a buffer for the port's incoming frames.

ICMP

The R851 supports Internet Control Message Protocol (ICMP) to confirm basic network connectivity. By default, the unit is enabled to respond to all ping requests. Through software, you can reconfigure the R851 as follows:

- All ICMP messages are not processed
- All ICMP messages are processed

- Only unicast ICMP messages are processed. The card will not process ICMP messages sent to IP multicast, IP subnet broadcast, and IP limited broadcast addresses.

Note: *The ICMP setting cannot be reconfigured at runtime.*

Loopback Mode

Loopback is provided as a means of testing connectivity and link integrity. The R851 supports the following loopback modes:

- Local Loopback
- Remote Loopback
- OAM Loopback

Once loopback is enabled, the R851 can be taken out of loopback using one of the following means:

- Timeout. The timeout period is configurable from 30 seconds to 5 minutes. The default is 30 seconds.
- Software commands.
- A reset or full power cycle of the card.
- Removing the card and then reinserting it into the chassis.

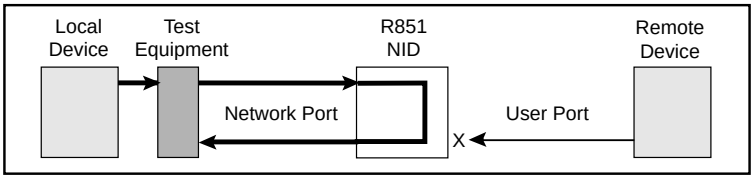
Note: *Loopback is not supported on the user port (Port 1). If you attempt to enable loopback on Port 1, you will receive an error message.*

Local Loopback

Local loopback is provided for testing link integrity on the network port (Port 2) of a standalone R851 NID. When local loopback is enabled on the network port, the port returns its incoming data back to the sender, while continuing to receive and process management frames. Management frames are not looped back—only data frames are returned. When local loopback is enabled, the LBK LED is lit and the user port is disabled.

Local loopback is typically enabled to evaluate the network segment by using standard packet-generating test equipment. During local loopback, the incoming data is transmitted through the entire circuitry of the R851 board, not just the network port. This allows the entire circuit to be tested.

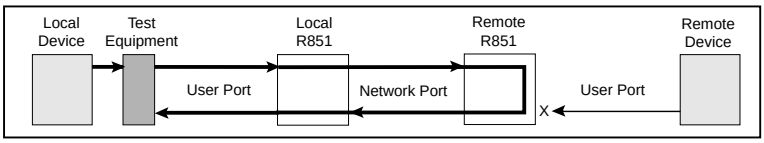
RMON statistics are incremented on both ports, even though the physical interface of the user port is neither transmitting nor receiving traffic.



Remote Loopback

Remote loopback is only applicable when two R851 cards are in a back-to-back configuration and they are being managed by the R502-M management card. Remote loopback is performed on the network port of the remote R851. When remote loopback is enabled, the remote network port returns its incoming data back to the sender, while continuing to receive and process management frames. Management frames are not looped back—only data frames are returned. During remote loopback, the LBK LED on the remote R851 is lit and its user port is disabled. The LBK LED on the local R851 remains off.

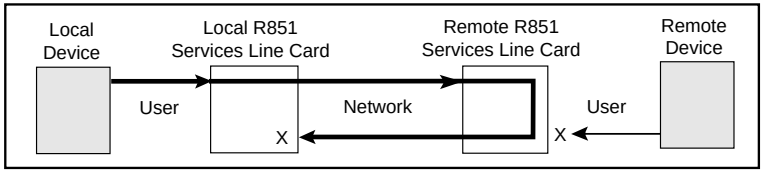
Remote loopback only can be enabled on Port 2 of the remote R851. It is typically enabled to evaluate the data flow using standard packet-generating test equipment, as shown in the illustration below. During remote loopback, the incoming data is transmitted through the entire circuitry of the remote R851 board, not just its network port. This allows the entire circuit to be tested. RMON statistics are incremented on both ports, even though the physical interface of the remote user port is neither transmitting nor receiving traffic.



OAM Loopback

OAM loopback is only applicable to when two R851 services line cards are in a back-to-back configuration with both cards connected through their network ports. By using the 802.3ah management channel, OAM loopback is initiated from the local R851 and performed on the remote R851. During OAM loopback, data on the fiber line is looped at the remote R851, returned to the local R851, and terminated there.

Because the data stream is stopped at the local R851, you do not need any external test equipment to determine the quality of the network segment. Instead, you can simply view the counters for the two services line cards to see if the data is passing properly.



To perform OAM loopback, the following conditions must be met:

- The administrative **OAM state** must be **enabled** on the network port for both the local and remote R851.
- The **OAM mode** must be **active** on the local R851's network port because it is the port that initiates loopback.
- The network port on both the local and remote R851 must be in **full-duplex** mode. (OAM is not supported on half-duplex links.)
- The **OAM loopback status** must be set to **start**.

If all the conditions are satisfied, the remote R851 will begin looping back data when the local R851 initiates OAM loopback. During OAM loopback, the remote R851 disables its user port and returns its incoming data on the network port back to the local R851. (Management frames are processed but not looped — only data frames are returned.) When the data frames arrive back at the local R851, they are terminated.

During OAM loopback, the LBK LED is lit on the remote R851. The LBK LED on the local R851 remains off.

Port Management

By default, both ports are enabled to respond to management frames such as ARP requests and SNMP commands. This feature can be disabled on either port, however, it cannot be disabled on both ports simultaneously. When management is disabled on either port, the DIS LED turns green. A port with management disabled discards all management frames, but data frames continue to be received and transmitted normally.

Port State

You can independently enable or disable the port state on either port on the services line card. Disabling the port state stops the flow of data to and from that port. Although data is neither sent nor received, the disabled port continues to accept, process, and transmit management frames. However, if LLCF is enabled and the opposite port has no link, management frames will not be transmitted.

Environmental Sensors

Through software, you can view environmental sensor information for monitoring the health of the services line card. Each sensor reading includes the current value along with the minimum and maximum values for the component. To prevent a potential problem, a trap can be set so a network manager is notified whenever any sensor threshold is crossed. For more information on traps, refer to “Traps” on page 67.

Module Sensors

There are five module sensors. Module sensors measure the main circuit board’s temperature as well as the voltage for the line card’s 1.2, 2.5, 3.3, and 5.0 volt power supplies. The 5.0 volt supply is the input power source for the services line card. The other supplies are used to power various components on the circuit board. The module temperature sensor has an accuracy of ±3° C. The voltage monitoring accuracy is ±1%.

Port Sensors

The services line card includes three SFP port sensors for each fiber port. Information is provided only when an SFP transceiver is installed in the port. One sensor provides the internal port temperature. The other two sensors provide the optical receive and transmit power levels for the fiber port. The accuracy of the RX and TX monitors is typically ±1 dBm.

Upgrading the Operating System Software

The R851 services line card can store two separate versions of the operating system software. This enables you to revert to a previous version without having to download the older version again. Downloading and installing a new revision of the software onto the R851 is performed via TFTP as configured through SNMP or through the CLI. This section describes the steps necessary to download and activate a new version of software through either SNMP or CLI.

1. Copy the new binary OS image file to a TFTP server that can be reached by the R851.
2. Using an SNMP MIB browser, set the following objects in METRO-BILITY-DOWNLOAD-MIB:
   - Set **mosDownloadServer** to the *IP address* of the TFTP server.
   - Set **mosDownloadFilename** to the *path* and *filename* of the OS file to load.
   - Set **mosDownloadLocation** to either *3* for the primary OS file location or *4* for the secondary OS file location. It is recommended that you download the software into the location that is currently not in use.
   - Set **mosDownloadInitiateLoad** to *1* to begin loading the file. The status of the download can be monitored via the **mosDownload-Status** object.
3. When the value of **mosDownloadStatus** is flashBurnComplete(4), set **mosDownloadActiveOSImage** to the location just loaded to. That is, *3* if it was loaded to the primary location, or *4* if it was the secondary location.
4. Reset the board to run the new version of the OS.

Chapter 4: CLI Commands

This section contains a complete listing of all command line interface (CLI) commands available on the R851. Each command includes a detailed description of the syntax and associated parameters.

The R851 supports the following three levels of user accounts. The default login names and passwords for each account are in parentheses.

- User (user/user)
- Administrator (admin/admin)
- Root (root/root)

The list of commands available to each user account is cumulative. That is, the Administrator account includes all User commands, and the Root account includes all commands.

Note: *For any CLI command, you can start typing the first few letters and then press the Tab key to complete the rest of the command. There must be enough letters entered to make the command unique.*

Notation Conventions

This chapter uses the conventions described in this section.

Font Conventions

Arial — Arial is the default font used for general text.

Times — This font is used for program examples, prompt responses, and other system output.

[Key] — Key names in are written in square brackets. For example, [Tab] or [Esc].

Symbol Conventions

< > — Angle brackets indicate that the enclosed information is a required field.

[ ] Square brackets indicate that the enclosed information is optional, or it is a key to press.

| A vertical bar separating two or more text items indicates that any **one** of the terms may be entered as a value.

Complete List of Commands

User Commands

change password
exit
help
logout
ping
show dhcp
show download
show fpga
show icmp
show ip
show l2controlprotocol
show l3capability
show mgmtvlan
show oamcontrol
show oamevents
show oamloopback
show oampeer
show oamstatistics
show os
show port
show portstatistics
show rmonportstatistics
show sensors
show systeminfo
show trapcontrol
show uservlan

Administrator Commands

clear l2controlprotocol
clear mgmtvlan
clear uservlan
download

loopback
reset
run config
set dhcp
set download
set fpga
set icmp
set ip
set l2controlprotocol
set l3capability
set mgmtvlan
set oamcontrol
set oamerrframe
set oamerrframesecs
set oamerrsymperiod
set oamframeperiod
set oamloopback
set os
set port
set systeminformation
set trapcontrol
set uservlan

Root Commands

clear trapdestination
clear username
set snmpcommunity
set trapdestination
set username
show snmpcommunity
show trapdestinations
show usernames

Clear Commands

clear l2controlprotocol

Description: Clear Layer 2 protocol processing action on a specified port.
Syntax: clear l2controlprotocol <stp | rstp | mstp | lacp | marker | 802.1X | bridge | garp | gvrp | gmrp> port <port number>
Parameters: 802.1X – IEEE 802.1X Port Authentication Protocol.
bridge – LAN Bridge Management Protocol.
garp – IEEE 802 Group Attribute Registration Protocol.
gmrp – IEEE 802 GARP Multicast Registration Protocol.
gvrp – IEEE 802 GARP VLAN Registration Protocol.
lacp – IEEE 802.3ad Link Aggregation Protocol.
marker – IEEE 802.3ad Marker Protocol.
mstp – IEEE 802.1 Multiple Spanning Tree Protocol.
rstp – IEEE 802.1 Rapid Spanning Tree Protocol.
stp – IEEE 802.1 Spanning Tree Protocol.
port number – the actual port number.
Example:
```
Console> clear l2controlprotocol garp port 2
Console>
```

clear mgmtvlan

Description: Clear the management VLAN ID on both ports.
Syntax: clear mgmtvlan
Example:
```
Console> clear mgmtvlan
Console>
```

clear trapdestination

Description: Clear the destination and protocol information for a trap destination host.
Syntax: clear trapdestination <IP address | all>
Parameters: IP address – IP address in dotted decimal notation.
all – all configured destination hosts.
Example:
```
Console> clear trapdestination 192.168.1.100
Console>
```

clear username

Description: Remove a user account from the device.
Syntax: clear username <username>
Parameters: username – username.
Example:
```
Console> clear username guest
Console>
```

clear uservlan

Description: Clear the specified user VLAN ID on both ports.
Syntax: clear uservlan <vlan id>
Parameters: vlan id – VLAN ID in the range 1 to 4094.
Example:
```
Console> clear uservlan 126
Console>
```

System Commands

change password

Description: Change your current user account password. The password is a case-sensitive ASCII string (32 characters max).
Syntax: change password
Parameters: None.
Example:
```
Console> change password
Enter current password: ******
Enter new password: ********
Re-enter new password: ********
Console>
```

download

Description: Download the operating system, FPGA firmware, or configuration script.
Note: The download server must first be identified using the "set download" command before this command can be executed. Refer to "set download" on page 40 for more information.
Syntax: download <os1 | os2 | fpga1 | fpga2 | config1 | config2 >
Parameters: os1 – operating system software instance 1.
os2 – operating system software instance 2.
fpga1 – FPGA embedded software instance 1.
fpga2 – FPGA embedded software instance 2.
config1 – configuration script/file instance 1.
config2 – configuration script/file instance 2.
boot – boot code. This option is not displayed.
Example:
```
Console> download config1
Console> Transferring file config1.txt
Writing image to Z80 internal FLASH

FLASH verification in progress.

Locking Z80 internal FLASH.
```

exit

Description: Log off.
Syntax: exit
Parameters: None.
Example:
```
Console> exit
```

help

Description: Show all commands that are available to the user, along with a brief description of the command, or all available commands that begin with a specified word. Optionally, press the [Tab] key to display only the commands available to your user account. No descriptions are provided when you use the [Tab] option.

Syntax: help [command]
[Tab]

Parameters: command – a one-word command

Example:
```
Console> help
change password
   Change your current password.
   :
show uservlan <vlan id | all>
   Show user VLAN IDs (1-4094) on one or more ports.
Console> help loopback
loopback <port number> <enable | disable> [timeout <30-300>]
   Activate or cancel loopback on selected port.
Console>
```

logout

Description: Log off.

Syntax: logout

Parameters: None.

Example:
```
Console> logout
```

loopback

Description: Activate loopback on the specified port.

Syntax: loopback <port number> <enable | disable> [timeout <30-300>]

Parameters: port number – the actual port number. The R851 only supports loopback on Port 2.
enable|disable – activate or cancel loopback. Enable starts a new loopback; disable cancels the current loopback.
timeout – maximum number of seconds to allow the port to remain in loopback mode. The default is 30 seconds. The range is 30 to 300 seconds.

Example:
```
Console> loopback 2 enable timeout 60
Console>
```

ping

Description: Send ICMP echo request packets to a network host.

Syntax: ping <host> [<count> [<size> [<delay>]]]

Parameters: host – IP address of the network host.
count – number of packets to send. The default is 4.
size – size of the packet in bytes. The default is 56 bytes.
delay – length of time (in milliseconds) to wait between each request. The default is 0 milliseconds.

Example: Console> ping 192.168.1.100
56 octets from 192.168.1.100: icmp_seq 0
56 octets from 192.168.1.100: icmp_seq 1
56 octets from 192.168.1.100: icmp_seq 2
56 octets from 192.168.1.100: icmp_seq 3
received 4/4 packets (0% loss)
Console>

reset

Description: Reset, or reboot, the device and optionally set operational parameters to factory defaults.
Syntax: reset [default]
Parameters: default – factory default settings.
Example: Console> reset default

run config

Description: Run the saved configuration script. (Refer to "download" on page 37 for information on downloading a script.) A script is a text file consisting of CLI commands separated by carriage returns. There is also an "echo" command that can be used to print comments to the screen while the script is running.
Syntax: run config <image number>
Parameters: image number – image number of the configuration script. Valid numbers are 1 and 2.
Example: Console> run config 1
Setting IP information.
Disabling management on Port 2.
Setting up VLAN information.
Console>

Set Commands

set dhcp

Description: Set the DHCP client's operational mode. Optionally, specify the number of address acquisition retries before reverting back to the last known valid IP address.
Syntax: set dhcp <disable | enable> [# of retries]
Parameters: disable – disables DHCP client operation
enable – enables DHCP client operation.
# of retries – integer in the range 1 to 5. The default is 3.
Example: Console> set dhcp enable 5
DHCP Enabled
Retries: 5
DHCP Server: 192.168.1.100
Console>

set download

Description: Set addressing information relative to the download server used by the download command. The file will be downloaded via TFTP.
Syntax: set download <IP address> filename <name of file>
Parameters: IP address – IP address of the download host in dotted decimal notation.
name of file – case-sensitive ASCII string (50 characters max.) denoting the name of the download file.
Example:
```
Console> set download 192.168.1.100 filename control.bin
  server: 192.168.1.100
  filename: control.bin
  protocol: tftp
  status: Previous Flash burn completed successfully
Console>
```

set fpga

Description: Select the FPGA software to be used by the device.
Syntax: set fpga <image number>
Parameters: image number – 1 or 2.
Example:
```
Console> set fpga 1
  FPGA1 image (1.1.0) will not become active until next reset.
Console>
```

set icmp

Description: Set operational, processing mode for end-station ICMP messages.
Syntax: set icmp <disable | enable | broadcastdisable>
Parameters: disable – disables processing of all ICMP messages.
enable – enables processing of all ICMP messages.
broadcastdisable – enables processing of only unicast ICMP messages, but disables processing of ICMP messages sent to IP multicast, IP subnet broadcast, and IP limited broadcast addresses.
Example:
```
Console> set icmp broadcastdisable
  status: Broadcast Disabled

Console>
```

set ip

Description: Set the device's IP address, network mask, or default gateway IP address.
Note: If you change the network portion of the IP address, the default gateway must also be updated to ensure compatibility. If the gateway cannot be reached with the new IP address, it will not be accepted.
Syntax: set ip <IP address> [mask <mask value>] [gateway <default gateway IP address>]
Parameters: IP address – end-station IP address in dotted decimal notation.

mask value – the end-station prefix, or network mask in dotted decimal notation or in /bits format.
default gateway IP address – default gateway IP address in dotted decimal notation.

Example:
```
Console> set ip 192.168.1.100 mask 255.255.255.0
Console>
```

set l2controlprotocol

Description: Set disposition for a Layer 2 control protocol on a port.

Syntax: set l2controlprotocol <stp | rstp | mstp | lacp | marker | 802.1X | bridge | garp | gvrp | gmrp> disposition <discard | forward | peer> port <port number>

Parameters:
802.1X – IEEE 802.1X Port Authentication Protocol.
bridge – LAN Bridge Management Protocol.
garp – IEEE 802 Group Attribute Registration Protocol.
gmrp – IEEE 802 GARP Multicast Registration Protocol.
gvrp – IEEE 802 GARP VLAN Registration Protocol.
lacp – IEEE 802.3ad Link Aggregation Protocol.
marker – IEEE 802.3ad Marker Protocol.
mstp – IEEE 802.1 Multiple Spanning Tree Protocol.
rstp – IEEE 802.1 Rapid Spanning Tree Protocol.
stp – IEEE 802.1 Spanning Tree Protocol, including Rapid and Multiple Spanning Tree Protocols.
discard – discard (filter) the specified Layer 2 control protocol.
forward – forward the specified Layer 2 control protocol, based on forwarding rules and policies.
peer – accept the specified Layer 2 protocol for end-station processing.
port number – the actual port number.

Example:
```
Console> set l2controlprotocol bridge disposition forward port 1
Console>
```

set l3capability

Description: Set the device's management capability to receive/transmit IP packets.

Syntax: set l3capability <disable | enable>

Parameters:
disable – disallows the reception and transmission of all IP packets to/from the management port.
enable – allows all IP packets destined for the management port to be received and allows the management port to transmit IP packets.

Example:
```
Console> set l3capability enable
  IP Capability Enabled
Console>
```

set mgmtvlan

Description: Set management VLAN ID. It will be applied to both ports.
Syntax: set mgmtvlan <vlan id>
Parameters: vlan id – VLAN ID in the range 1 to 4094.
Example:
```
Console> set mgmtvlan 1070
Console>
```

set oamcontrol

Description: Set the OAM capabilities for the specified port.
Syntax: set oamcontrol <port number> [admin <enable | disable>] [mode <active | passive>]
Parameters: port number – the actual port number.
admin – enable or disable administrative OAM mode for the specified port.
mode – specify active or passive OAM mode for the selected port. These modes differ in that active mode provides additional capabilities to initiate monitoring activities with the remote OAM port, while passive mode generally waits for the remote OAM port to initiate actions with it and responds to requests. For example, an active OAM port can put the remote port in a loopback state, while a passive OAM port cannot.
Example:
```
Console> set oamcontrol 2 admin enable mode active
Console>
```

set oamerrframe

Description: Set the window and threshold values that will determine when the Errored Frame Event will be triggered on the specified port.
Syntax: set oamerrframe <port number> [window <error frame check window>] [threshold <frame threshold>]
Parameters: port number – the actual port number.
window – The amount of time (in 100 ms increments) over which the threshold is defined.
threshold – The number of frame errors that must occur for the Errored Frame Event to be triggered. Example: if window = 100 and threshold = 5, then if 5 frame errors occur within a window of 10 seconds, an Event Notification OAMPDU will be generated with an Errored Frame Event TLV indicating that the threshold has been crossed.
Example:
```
Console> set oamerrframe 2 window 100 threshold 5
Console>
```

set oamerrframesecs

Description: Set the window and threshold values that will determine when the Errored Frame Seconds Summary Event will be triggered on the specified port.

Syntax: set oamerrframesecs <port number> [window <frame secs window>] [threshold <frame secs threshold>]

Parameters: port number – the actual port number.

window – The amount of time (in 100 ms intervals) over which the threshold is defined. The range is 100 to 9000.

threshold – The number of errored frame seconds that must occur for the Errored Frame Seconds Summary Event to be triggered. The threshold range is 1 to 900. Example: if window = 100 and threshold = 5, then if 5 frame errors occur within a window of 100 (in tenths of a second), an Event Notification OAMPDU will be generated with an Errored Frame Seconds Summary Event TLV indicating the threshold has been crossed.

Example:

```
Console> set oamerrframesecs 1 window 100 threshold 5
Console>
```

set oamerrsymperiod

Description: Set the window and threshold values that will determine when the Errored Symbol Period Event will be triggered on the specified port.

Syntax: set oamerrsymperiod <port number> [window <number of symbols>] [threshold <symbol period threshold>]

Parameters: port number – the actual port number.

window – The number of symbols over which the threshold is defined.

threshold – The number of symbol errors that must occur for the Errored Symbol Period Event to be triggered. Example: If window = 100 and threshold = 2, then if 2 symbol errors occur within 100 symbols, an Event Notification OAMPDU will be generated with an Errored Symbol Period Event TLV indicating that the threshold has been crossed.

Example:

```
Console> set oamerrsymperiod 1 window 100 threshold 2
Console>
```

set oamframeperiod

Description: Set the window and threshold values that will determine when the Errored Frame Period Event will be triggered on the specified port.

Syntax: set oamframeperiod <port number> [window <number of frames>] [threshold <frame threshold>]

Parameters: port number – the actual port number.

window – The number of frames over which the threshold is defined.
threshold – The number of frame errors that must occur for the Errored Frame Period Event to be triggered. Example: If window = 50 and threshold = 2, then if 2 frame errors occur within a window of 50 frames, an Event Notification OAMPDU will be generated with an Errored Frame Period Event TLV indicating that the threshold has been crossed.

Example: Console> set oamframeperiod 2 window 50 threshold 2
Console>

set oamloopback

Description: Start or stop remote loopback on the specified port with the remote OAM port.
Syntax: set oamloopback <port number> status <start | end>
Parameters: port number – the actual port number.
status – initiate or terminate remote loopback with the remote port. Starting remote loopback causes the specified port to send a loopback OAMPDU (with the loopback enable flags set) to the remote port. Ending remote loopback causes the specified port to send a loopback OAMPDU (with the loopback enable flags cleared) to the remote port.
Example: Console> set oamloopback 2 status end
Console>

set os

Description: Select the operating system image to be used by the device. To activate the selection, you must reset the device after changing the OS image.
Syntax: set os <image number>
Parameters: image number – 1 or 2.
Example: Console> set os 1
OS1 image (1.1.0) will not become active until next reset.
Console>

set port

Description: Set attributes for a selected port.
Syntax: set port <port number> [autonegotiate <disable | enable>] [duplex <full | half>] [flowcontrol <disable | enable>] [management <disable | enable>] [speed <10 | 100 | 1000>] [state <disable | enable>] [fef <disable | enable>] [llr <disable | enable>] [llcf <disable | enable>]
Parameters: port number – the actual port number.
autonegotiate – disable or enable auto-negotiation for the selected port.
duplex – specify full or half duplex mode for the selected port.

flowcontrol – disable or enable flow control for the selected port. PAUSE frames are used on full-duplex ports, whereas collisions are forced on half-duplex ports.
fef – disable or enable Far End Fault reporting on the selected fiber port.
llcf – disable or enable the ability to carry forward (to the other port) link loss on the selected port.
llr – disable or enable Link Loss Return status for the selected port.
management – disable or enable management access over selected port.
speed – set the speed on the selected port to 10, 100, or 1000 Mbps and disable auto-negotiation on that port.
state – disable or enable the selected port.

Example:
```
Console> set port 1 speed 100 state enable
Console>
```

set snmpcommunity

Description: Set an SNMP community and its corresponding access profile.

Syntax: set snmpcommunity <community name> profile <ro | rw | admin>

Parameters: community name – a case-sensitive ASCII string (up to 50 characters in length) denoting the receive profile on the trap destination host. If unspecified, the default value is NULL.
profile – specifies the access profile for a community user.
ro – read-only access to non-privileged objects.
rw – read-write access to non-privileged objects.
admin – full read-write access to all objects.

Example:
```
Console> set snmpcommunity public profile ro
Console>
```

set systeminformation

Description: Set system information.

Syntax: set systeminformation <administrative> [name <system name>] [location <location name>] [contact <contact name>]

Parameters: administrative – identifies state of configured information.
system name – a case-sensitive ASCII string (up to 50 characters in length) denoting the system name. Multi-word strings must be placed in quotation marks. If unspecified, the default value is NULL.
location name – a case-sensitive ASCII string (up to 50 characters in length) denoting the system location. Multi-word strings must be placed in quotation marks. If unspecified, the default value is NULL.

contact name – a case-sensitive ASCII string (up to 50 characters in length) denoting the contact name. Multi-word strings must be placed in quotation marks. If unspecified, the default value is NULL.

Example: Console> set systeminformation admin name “A B” location 45

Console>

set trapcontrol

Description: Set trap handling for a specified trap on a per destination basis.

Syntax: set trapcontrol <trap index> host <IP address> state <disable | enable>

Parameters: trap index – trap number as defined in MIB-II.

IP address – trap destination host’s IP address in dotted decimal notation.

state – enable or disable the specified trap.

Example: Console> set trapcontrol 4 host 192.168.1.100 state enable
Console>

set trapdestination

Description: Set the destination and protocol information for a trap destination host.

Syntax: set trapdestination <IP address> [port <UDP port>] [community <trap community>]

Parameters: IP address – trap destination’s IP address in dotted decimal notation.

UDP port – UDP transport port number in the range 1 to 65535. The default value is 162.

trap community – a case-sensitive ASCII string (up to 50 characters in length) denoting the receive profile on the trap destination host. The default value is public.

Example: Console> set trapdestination 192.168.1.100
Console>

set username

Description: Set the username, password, and access for user login.

Syntax: set username <user name> password <user password> access <user | admin | root>

Parameters: user name – a case-sensitive, printable ASCII string up to 32 characters in length.

user password – a case-sensitive, printable ASCII string up to 32 characters in length.

access – specifies the access level for a user login.

user – read-only access to non-privileged objects.

admin – read-write access to non-privileged objects.

root – full read-write access to all objects.

Example: Console> set username guest password guest access user
Console>

set uservlan

Description: Set the user VLAN ID on one or more ports. The user VLAN ID must be different from previously-provisioned management VLAN ID(s).

Syntax: set uservlan <user id> port <port number ... [port number n]>

Parameters: user id – VLAN ID in the range 1 to 4094.
port number – the port number to which the user VLAN is assigned.

Example:
```
Console> set uservlan 22 port 1 2
Console>
```

Show Commands

show dhcp

Description: Show the DHCP client's operational mode and operation parameters.

Syntax: show dhcp

Display Parameters: DHCP – identifies the operational mode.
disabled – DHCP client operation is disabled.
enabled – DHCP client operation is enabled.
Retries – specifies the number of address acquisition retries before reverting to using the last known valid IP address.
dhcp server – IP address of the current DHCP server.

Example:
```
Console> show dhcp
  DHCP Enabled
  Retries: 3
  DHCP Server: 192.168.1.100
Console>
```

show download

Description: Show addressing information relative to the download server used by the download command, along with the status of the current download.

Syntax: show download

Display Parameters: server – identifies the IP address of the download host.
filename – identifies the name of the download file.
protocol – identifies the download protocol. The R851 only supports TFTP (Trivial File Transfer Protocol).
status – identifies the status of the current download. The status can be any of the following descriptions:
Transfer in progress
Transfer complete
Flash burn in progress

Flash burn complete
Transfer failed
Flash burn failed

Note: The “status” parameter will only displayed if software has been downloaded since the device was last reset or booted.

Example:
```
Console> show download
  server: 192.168.1.100
  filename: config1.txt
  protocol: tftp
  status: Previous Flash burn completed successfully
Console>
```

show fpga

Description: Show the image number of the active FPGA software.

Syntax: show fpga

Example:
```
Console> show fpga
   Active FPGA image number: 1
Console>
```

show icmp

Description: Show operational, processing mode for end-station ICMP messages.

Syntax: show icmp

Display Parameters: status – identifies the processing state of the end-station ICMP messages.
All Disabled – ICMP message processing is disabled.
All Enabled – ICMP message processing is enabled.
Broadcast Disabled – the processing of only unicast ICMP messages is enabled. The processing of ICMP messages sent to IP multicast, IP subnet broadcast, and IP limited broadcast addresses is disabled.

Example:
```
Console> show icmp
  status: Broadcast Disabled

Console>
```

show ip

Description: Show the device’s IP address, corresponding network mask, and the default gateway IP address.

Syntax: show ip

Display Parameters: IP Address – identifies the end-station IP address.
IP Mask – identifies the end-station prefix (network mask).
Default Gateway – identifies the default route gateway IP address.

Example: Console> show ip
IP Address: 192.168.1.100
IP Mask: 255.255.255.0
Default Gateway: 192.168.1.254
Console>

show l2controlprotocol

Description: Show the disposition for Layer 2 protocols on one or more ports.

Syntax: show l2controlprotocol <stp | rstp | mstp | lacp | marker | 802.1X | bridge | garp | gvrp | gmrp | all> port <port number | all>

Parameters: 802.1X – IEEE 802.1X Port Authentication Protocol.
bridge – LAN Bridge Management Protocol.
garp – IEEE 802 Group Attribute Registration Protocol.
gmrp – IEEE 802 GARP Multicast Registration Protocol.
gvrp – IEEE 802 GARP VLAN Registration Protocol.
lacp – IEEE 802.3ad Link Aggregation Protocol.
marker – IEEE 802.3ad Marker Protocol.
mstp – IEEE 802.1 Multiple Spanning Tree Protocol.
rstp – IEEE 802.1 Rapid Spanning Tree Protocol.
stp – IEEE 802.1 Spanning Tree Protocol, including Rapid and Multiple Spanning Tree Protocols.
port number – the actual port number.
all – all three ports.

Display Parameters: Discard – specified protocol is being discarded (filtered).
Forward – specified protocol is being forwarded, based on forwarding rules and policies.
Peer – specified protocol is being accepted for end-station processing.

Example: Console> show l2controlprotocol bridge port all
Port 0:
bridge: Discard
Port 1:
bridge: Forward
Port 2:
bridge: Forward
Console>

show l3capability

Description: Show the device's management capability to receive/transmit IP packets.

Syntax: show l3capability

Example: Console> show l3capability
IP Capability Enabled
Console>

show mgmtvlan

Description: Show the management VLAN ID (1-4094) for both ports, if it has been assigned.
Syntax: show mgmtvlan
Example:
```
Console> show mgmtvlan
   Management Disabled
Console>
```

show oamcontrol

Description: Show the primary controls and status for the 802.3ah OAM capabilities for the specified port or all ports.
Syntax: show oamcontrol <port number | all>
Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: Admin State – indicates the desired administrative OAM state for the specified port.
DISABLED – OAM is in disabled.
ENABLED – OAM is in enabled.

Note: The Admin State is ignored when the port is not in full-duplex mode. OAM is not supported on half-duplex links.

Operational Status – identifies the OAM capability determined during initialization between the specified port and its peer, which is the remote port on the opposite end of the link.
DISABLED – OAM is disabled administratively on the specified port.
LINK FAULT – The port has detected a fault and is transmitting OAMPDUs with a link fault indication.
PASSIVE WAIT – The port is in passive OAM mode and is waiting to see if the remote port is capable of OAM.
ACTIVE SEND LOCAL – The port is in active OAM mode and is trying to discover whether the remote port has OAM capability but has not yet made that determination.
SEND LOCAL AND REMOTE – The port has discovered its peer, but has not yet accepted or rejected the peer's configuration.
SEND LOCAL AND REMOTE OK – The port has accepted OAM peering with the remote port.
OAM PEERING LOCALLY REJECTED – The port has rejected OAM peering with the remote port.
OAM PEERING REMOTELY REJECTED – The remote port has rejected OAM peering.
OPERATIONAL – Both the port and the remote port have accepted peering.

Mode – identifies the mode of OAM operation for the port.
PASSIVE – Port waits for the remote port to initiate OAM actions with it, but cannot initiate actions itself.
ACTIVE – The port can initiate monitoring activities with the remote port.

Max PDU Size – indicates largest OAMPDU that the port supports. The port exchanges maximum OAMPDU sizes with its peer, and both ports negotiate to use the smaller of the two maximum sizes between them.

Config Revision – indicates the configuration revision of the port as reflected in the latest OAMPDU sent by the port. The configuration revision is used to indicate configuration changes that have occurred which might require the remote port to re-evaluate whether peering is allowed.

Supported Functions– identifies OAM functions supported by the port. One or more of the following functions may be supported:
UNIDIRECTIONAL
LOOPBACK
EVENT
VARIABLE

Example:

```
Console> show oamcontrol 2
Port 2 Information:
   Admin State . . . . . : ENABLED (2)
   Operational Status  . . . . : ACTIVE SEND LOCAL (4)
   Mode. . . . . : ACTIVE (1)
   Max PDU Size . . . . . : 0
   Config Revision . . . . . : 0
   Supported Functions. . . : LOOPBACK
                              EVENT
                              VARIABLE
Console>
```

show oamevents

Description: Show the windows and thresholds for generating standard Ethernet OAM events for the specified port(s).

Syntax: show oamevents <port number | all>

Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: Error Symbol Period Window – The number of symbols (***N***) over which the threshold is defined.

Error Symbol Period Threshold – The number of symbol errors (***n***) that must occur for the Errored Symbol Period Event to be triggered. If ***n*** out of ***N*** symbols had errors, an Errored Symbol Period Event notification OAMPDU should be generated.

Error Frame Period Window – The number of frames (***N***) over which the threshold is defined.

Error Frame Period Threshold – The number of frame errors (***n***) that must occur for the Errored Frame Period Event to be triggered. If ***n*** out of ***N*** frames had errors, an Errored Frame Period Event notification OAMPDU should be generated.

Error Frame Window – The amount of time (***T***), in 100 ms increments, over which the threshold is defined.

Error Frame Threshold – The number of frame errors (***n***) that must occur for the Errored Frame Event to be triggered. If ***n*** frames in ***T*** (in tenths of a second) had errors, an Errored Frame Event notification OAMPDU should be generated.

Error Frame Seconds Summary Window – The amount of time (***T***), in 100 ms intervals, over which the threshold is defined.

Error Frame Seconds Summary Threshold – The number of errored frame seconds (***n***) that must occur for the Errored Frame Seconds Summary Event to be triggered. If ***n*** frame errors occur in ***T*** (in tenths of a second), an Errored Frame Seconds Summary Event notification OAMPDU should be generated.

Example:

```
Console> show oamevents 2
Port 2
Error Symbol Period Window: 100
Error Symbol Period Threshold: 01
Error Frame Period Window: 100
Error Frame Period Threshold: 01
Error Frame Window: 100
Error Frame Threshold: 01
Error Frame Seconds Summary Window: 100
Error Frame Seconds Summary Threshold: 01
Console>
```

show oamloopback

Description: Show the loopback state for the specified port(s).

Syntax: show oamloopback <port number | all>

Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: Loopback Status – indicates the loopback state of the specified port.
NO LOOPBACK – Normal operation with no loopback in progress.
INITIATING LOOPBACK – The local device has sent a loopback request to the remote unit and is waiting for a response.

REMOTE LOOPBACK – The remote unit has responded to the local device and indicated that it is in loopback mode.
TERMINATING LOOPBACK – The local device is in the process of ending the remote loopback.
LOCAL LOOPBACK – The remote unit has put the local device in loopback mode.
UNKNOWN – The local and remote parsers and multiplexers are in an unexpected combination.

Example:
```
Console> show oamloopback 2
Port 2 Information:
   Loopback Status . . . . . : UNKNOWN
Console>
```

show oampeer

Description: Show information about the OAM peer for the specified port(s).

Syntax: show oampeer <port number | all>

Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: MAC Address – identifies the MAC address of the remote port. The MAC address is derived from the most recently received OAMPDU.
OUI – identifies the remote port's Organizational Unique Identifier (OUI). The OUI can be used for identifying the vendor of the remote device.
Vendor Info – indicates the vendor information of the remote port as reflected in the latest Information OAMPDU received.
Mode – identifies the mode of OAM operation for the remote port.
PASSIVE – Remote port waits for the local port to initiate OAM actions.
ACTIVE – The remote port can initiate monitoring activities with the local port.
Max PDU Size – indicates largest OAMPDU that the remote port supports. The remote port exchanges maximum OAMPDU sizes with the local port, and both ports negotiate to use the smaller of the two maximum sizes between them.
Config Revision – indicates the configuration revision of the remote port as reflected in the latest OAMPDU sent by the remote port. The configuration revision is used to indicate configuration changes that have occurred which might require the local port to re-evaluate whether peering is allowed.

Supported Functions– identifies OAM functions supported by the remote port. One or more of the following functions may be supported:
UNIDIRECTIONAL
LOOPBACK
EVENT
VARIABLE

Example:
```
Console> show oampeer 2
Port 2 Peer Information:
   MAC Address . . . . . : ENABLED (2)
   OUI. . . . . : 0 0 0
   Vendor Info. . . . . : 0
   Mode. . . . . : UNKNOWN
   Max PDU Size . . . . . : 0
   Config Revision . . . . . : 0
   Supported Functions. . . : LOOPBACK
                              EVENT
                              VARIABLE
Console>
```

show oamstatistics

Description: Show show OAM statistics for the specified port (s).
Syntax: show oamstatistics <port number | all>
Parameters: port number – the actual port number.
all – specifies all ports.
Example:
```
Console> show oamstatistics 1
Port 1 Information:
PDU Received: 0                          PDU Transmitted: 98
Information Rcv'd: 0                     Information Transmitted: 98
Unique Event Notification Rcv'd: 0       Unique Event Notification Transmitted: 0
Duplicate Event Notification Rcv'd: 0    Duplicate Event Notification Transmitted: 0
Loopback Control Rcv'd: 0                Loopback Control Transmitted: 0
Variable Requests Rcv'd: 0               Variable Requests Transmitted: 0
Variable Responses Rcv'd: 0              Variable Responses Transmitted: 0
Org Specific Rcv'd: 0                    Org Specific Transmitted: 0
Unsupported Codes Rcv'd: 0               Unsupported Codes Transmitted: 0
Dropped Events: 0
Console>
```

show os

Description: Show the image number of the active operating system.
Syntax: show os
Example:
```
Console> show os
   Active OS image number: 1
Console>
```

show port

Description: Show attributes for a selected port or all ports.
Syntax: show port <port number | all> [type <administrative | operational>]
Parameters: port number – the actual port number.
all – specifies all ports.
type – specifies administrative or operational parameters.
If not specified, the operational values are shown.
administrative – specifies that configuration-related parameters are being requested.
operational – specifies that operational parameters are being requested.

Display Parameters: Port Type – identifies the Ethernet media designation for the specified port.
1000BASE_X – 1000 Mbps fiber optic.
10/100/1000BASE_T – 4 pairs Category 5 UTP.
Connector Type – identifies the connector type for the specified port.
RJ45 – RJ-45 connector.
SFP – Small Form-Factor Pluggable connector. For an SFP connector, the following parameters are also displayed:
SFP Manufacturer – manufacturer's name
SFP Wavelength – wavelength in nm
SFP Part Number – part number assigned by the manufacturer
SFP Serial Number – serial number assigned by the manufacturer
MAC Address – identifies the MAC address assigned to the specified port.
Port AN– indicates the auto-negotiation status for the specified port.
DISABLED – auto-negotiation is disabled.
ENABLED – auto-negotiation is enabled.
Port Duplex – indicates the duplex mode for the specified port.
FULL – full-duplex mode.
HALF – half-duplex mode.
Port Flow Control – indicates flow control status for the specified port. PAUSE frames are used on full-duplex ports, whereas collisions are forced on half-duplex ports.
DISABLED – flow control is disabled.
ENABLED – flow control is enabled.
Port Management – indicates management access over specified port.
DISABLED – management access is disabled.

ENABLED – management access is enabled.

Port Speed – indicates the speed of the specified port:
10 Mbps, 100 Mbps, or 1000 Mbps.

Port Admin State – indicates the administrative state of the specified port.
DISABLED – port is in disabled.
ENABLED – port is in enabled.
TESTING – port is in test mode.

Port Oper State – indicates the operational state of the specified port.
UP – a valid link is detected at the port.
DOWN – no link is detected at the port.

Port LLCF – identifies LLCF state for the specified port.
DISABLED – LLCF is disabled.
ENABLED – LLCF is enabled.

Port LLR – identifies LLR state for the specified port.
DISABLED – LLR is disabled.
ENABLED – LLR is enabled.

Port FEF – identifies FEF state for the specified port.
DISABLED – FEF is disabled.
ENABLED – FEF is enabled.

Temperature – indicates the temperature of the specified port (fiber only) in degrees Celsius and Fahrenheit.
Current – the current temperature sensor reading.
Min – the lowest temperature at which the SFP can continue to operate properly.
Max – the highest temperature at which the SFP can continue to operate properly.

Transmit Power – indicates the transmit power of the specified port (fiber only) in dBm.
Current – the current transmitter sensor reading.
Min – the lowest power at which the SFP can continue to operate properly.
Max – the highest power at which the SFP can continue to operate properly.

Receive Power – indicates the receive power of the specified port (fiber only) in dBm.
Current – the current receiver sensor reading.
Min – the lowest power at which the SFP can continue to operate properly.
Max – the highest power at which the SFP can continue to operate properly.

Example:

```
Console> show port 2
Port 2 Information:
  Port Type . . . . . : 1000BASE_X
  Connector Type . . . . . : SFP
    SFP Manufacturer . . . : Infineon AG
    SFP Wavelength  . . . . : 850 nm
```

```
    SFP Part Number  . . . : V23848-M305-C56
    SFP Serial Number . . : 30010074
  MAC Address . . . . . . . . : 40:40:9f:18:17:e5
  Port AN . . . . . . . . . . . . : ENABLED
  Port Duplex . . . . . . . . . . : FULL
  Port Flow Control . . . . . : DISABLED
  Port Management . . . . . : ENABLED
  Port Speed . . . . . . . . . . . : 1000 Mbps
  Port Admin State . . . . . . : ENABLED
  Port Oper State . . . . . . . : DOWN
  Port LLCF . . . . . . . . . . . : DISABLED
  Port LLR . . . . . . . . . . . . : DISABLED
  Port FEF . . . . . . . . . . . . : DISABLED
Temperature (Celsius)     : Current: 43   Min: -45   Max: 105   (IN RANGE)
Temperature (Fahrenheit) : Current: 99   Min: -49   Max: 221   (IN RANGE)
Transmit Power (dBm)     : Current: -6   Min: -9    Max: 0     (IN RANGE)
Receive Power (dBm)      : Current: -35  Min: -20   Max: 0     **OUT OF
RANGE**
Console>
```

show portstatistics

Description: Show MIB-II interface statistics for one port or all three ports.

Syntax: show portstatistics <port number | all>

Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: Octets Received – number of octets received.
Unicast Packets Rcv'd – number of unicast packets received.
Broadcast Packets Rcv'd – number of broadcast packets received.
Multicast Packets Rcv'd – number of multicast packets received.
Rcv'd Packets Dropped – number of received packets that were discarded during reception.
Error Packets Rcv'd – number of packets received with errors.
Octets Transmitted – number of octets transmitted.
Unicast Packets Transmitted – number of unicast packets transmitted.
Broadcast Packets Transmitted – number of broadcast packets transmitted.
Multicast Packets Transmitted – number of multicast packets transmitted.
Transmitted Packets Dropped – number of received packets that were discarded during transmission.
Error Packets Transmitted – number of packets dropped due to transmission errors.

Example: Console> show portstatistics 1

```
Port: 1
Octets Received: 294583          Octets Transmitted: 59309
Unicast Packets Rcv'd: 855       Unicast Packets Transmitted: 661
Broadcast Packets Rcv'd: 2109    Broadcast Packets Transmitted: 2
Multicast Packets Rcv'd: 166     Multicast Packets Transmitted: 0
Rcv'd Packets Dropped: 0         Transmitted Packets Dropped: 0
Error Packets Rcv'd: 0           Error Packets Transmitted: 0
Console>
```

show rmonportstatistics

Description: Show the RMON Group 1 statistics for the selected port(s).
Syntax: show rmonportstatistics <port number | all>
Parameters: port number – the actual port number.
all – specifies all ports.

Display Parameters: Octets Received – number of octets received.
Packets Rcv'd – number of packets received.
Broadcast Packets Rcv'd – number of broadcast packets received.
Multicast Packets Rcv'd – number of multicast packets received.
CRC Alignment Errors – number of CRC alignment errors due to received traffic.
Fragments Rcv'd – number of fragments received.
Undersize Packets Rcv'd – number of under-sized packets received.
Oversize Packets Rcv'd – number of over-sized packets received.
Jabbers Rcv'd – number of jabbers identified from received traffic.
Collisions – number of collisions encountered during transmission.
Size 64 Packets – number of packets (64 octets in length) received.
Size 65 - 127 Packets – number of packets (65 to 127 octets in length) received.
Size 128 - 255 Packets – number of packets (128 to 255 octets in length) received.
Size 256 - 511 Packets – number of packets (256 to 511 octets in length) received.
Size 512 - 1023 Packets – number of packets (512 to 1023 octets in length) received.
Size 1024 - 1518 Packets – number of packets (1024 to 1518 octets in length) received.
Dropped Events – number of events where traffic was dropped either during reception or transmission.

Example: Console> show rmonportstatistics 2

```
Port: 2
Octets Received: 37706                  Packets Rcv'd: 35625
Broadcast Packets Rcv'd: 87             Multicast Packets Rcv'd: 255
CRC Alignment Errors: 0                 Fragments Rcv'd: 14
Undersize Packets Rcv'd: 0              Oversize Packets Rcv'd: 0
Jabbers Rcv'd: 0                        Collisions: 0
Size 64 Packets: 0                      Size 65 - 127 Packets: 0
Size 128 - 255 Packets: 0               Size 256 - 511 Packets: 0
Size 512 - 1023 Packets: 0              Size 1024 - 1518 Packets: 0
Dropped Events: 0
```

show sensors

Description: Show all sensor readings for the main circuit board (module) and each fiber port, and indicate whether the reading is within range for proper operation. Also indicate the highest and lowest values at which the component can operate properly (warning thresholds).

Syntax: show sensors

Display Parameters:

Temperature – indicates the current, minimum, and maximum temperature reading (in degrees Celsius and Fahrenheit) of the device or port.

1.5 Volt – indicates the current, minimum, and maximum voltage reading (in millivolts) of the device's 1.5-volt supply.

2.5 Volt – indicates the current, minimum, and maximum voltage reading (in millivolts) of the device's 2.5-volt supply.

3.3 Volt – indicates the current, minimum, and maximum voltage reading (in millivolts) of the device's 3.3-volt supply.

5.0 Volt – indicates the current, minimum, and maximum voltage reading (in millivolts) of the device's 5.0-volt supply.

Transmit Power – indicates the current, minimum, and maximum reading (in dBm) of the SFP transmitter.

Receive Power – indicates the current, minimum, and maximum reading (in dBm) of the SFP receiver.

Example: Console> show sensors

```
Module Information:
Temperature (Celsius)   : Current: 48   Min: 20    Max: 70   (IN RANGE)
Temperature (Fahrenheit): Current: 118  Min: 68    Max: 157  (IN RANGE)
1.5 Volt (Millivolts)   : Current: 1540 Min: 1440  Max: 1560 (IN RANGE)
2.5 Volt (Millivolts)   : Current: 2475 Min: 2375  Max: 2612 (IN RANGE)
3.3 Volt (Millivolts)   : Current: 3250 Min: 3135  Max: 3448 (IN RANGE)
5.0 Volt (Millivolts)   : Current: 4925 Min: 4750  Max: 5250 (IN RANGE)
Port 2 Information:
Temperature (Celsius)   : Current: 43   Min: -45   Max: 105  (IN RANGE)
```

```
Temperature (Fahrenheit): Current: 109  Min: -49  Max: 221  (IN RANGE)
Transmit Power (dBm)  : Current: -6   Min: -9   Max: 0    (IN RANGE)
Receive Power (dBm)   : Current: -35  Min: -20  Max: 0    **OUT OF
RANGE**
Console>
```

show snmpcommunity

Description: Show SNMP community string for the specified access profile.
Syntax: show snmpcommunity <ro | rw | admin | all>
Parameters: ro – read-only access to non-privileged objects.
rw – read-write access to non-privileged objects.
admin – full read-write access to all objects.
all – all of the above.
Example:

```
Console> show snmpcommunity ro
   Read-Only: public
Console> show snmpcommunity all
   Read-Only: public
   Read-Write: private
   Admin: admin
Console>
```

show systeminfo

Description: Show MIB-II system group information.
Syntax: show systeminfo
Display Parameters: System Name – identifies the MIB-II sysName object.
System Location – identifies the MIB-II sysLocation object.
System Contact – identifies the MIB-II sysContact object.
Hardware Revision – the hardware version of the line card.
OS1 Revision – the version of the operating system stored in the first flash image.
OS2 Revision – the version of the operating system stored in the second flash image.
FPGA1 Revision – the version of the FPGA firmware stored in the first flash image.
FPGA2 Revision – the version of the FPGA firmware stored in the second flash image.
Serial Number – the line card's serial number.
Example:

```
Console> show systeminfo
   System Name: Metro_R851_NID
   System Location: Merrimack, NH
   System Contact: EV Jones
   Hardware Revision: A
   OS1 Revision: 1.1.0
   OS2 Revision: 1.1.0 (Currently running)
   FPGA1 Revision: 1.1.0
   FPGA2 Revision: 1.1.0 (Currently running)
   Serial Number: Q102030404
Console>
```

show trapcontrol

Description: Show trap handling for the configured traps on a per destination basis.
Syntax: Show trapcontrol <trap index | all>
Parameters: trap index – trap number.
all – identifies all configured traps.
Display Parameters: Host – identifies the trap destination IP address.
state – identifies the operational state (disabled or enabled) for the specified trap.
Example:

```
Console> show trapcontrol 5
Hosts:   192.168.1.100   192.168.1.101   192.168.1.102   192.168.3.103
-------------------------------------------------------------------------
Index 5: Enabled         Enabled         Disabled        Enabled
Console>
```

show trapdestinations

Description: Show information for any configured trap destinations.
Syntax: show trapdestinations
Display Parameters: IP Address – IP address of the trap destination.
UDP Port – identifies the User Datagram Protocol port.
Community – identifies the trap community.
Example:

```
Console> show trapdestinations
IP Address          UDP Port      Community
------------------  ------------  ---------------
192.168.1.100       162           public
192.168.1.101       162           public
192.168.1.102       162           public
192.168.1.103       162           public
Console>
```

show usernames

Description: Show all configured login usernames and their corresponding access levels.
Syntax: show usernames
Example:

```
Console> show usernames
Username            Access level
------------        ---------------
root                root
admin               admin
user                user
Console>
```

show uservlan

Description: Show user VLAN IDs on one or more ports.
Syntax: show uservlan <vlan id | all>
Parameters: vlan id – a value in the range 1 to 4094.
all – show all VLAN IDs.
Display Parameters: Tagged Ports – identifies the port on which the user VLAN is assigned.
Example:

```
Console> show uservlan 2020
VLAN ID: 2020
   Tagged Ports: 1
Console>
```

Chapter 5: User Guide

This chapter contains information about the operating features of the Radiance GbE services line card.

LED Indicators

The Radiance services line card provides several LEDs on the front panel for the visible verification of unit status and proper functionality. These LEDs can help with troubleshooting and overall network diagnosis and management. There are separate receive (RX) and link (LK) indicators for each port. The following table describes the meaning of each LED when lit.

LED Label	LED Name	Color (Status)	Indication
MAN	Managed	Green (steady)	Unit is receiving management activity.
FD	Full Duplex	Green (steady)	Copper port is operating at full duplex.
		OFF	Copper port is operating at half duplex.
PWR	Power	Green (steady)	Unit is powered ON.
RX	Receive	Green (blinking)	Port is receiving data.
LK	Link	Green (steady)	Port has a valid link.
SPD	Speed	Green (blinks at 1 sec intervals)	Copper port is running at 10 Mbps/
		Green (blinks at 0.5 sec intervals)	Copper port is running at 100 Mbps/
		Green (steady)	Copper port is running at 1000 Mbps/
LBK	Loopback	Green (steady)	Unit is in loopback mode.
		Green (blinking)	The unit has successfully reset itself to its default settings. The DIS LED will also be blinking. Only applicable when resetting the board by using the jumper.
DIS	Disable	Green (steady)	One of the ports is disabled for management.
		Green (blinking)	The unit has successfully reset itself to its default settings. The LBK LED will also be blinking. Only applicable when resetting the board by using the jumper.

Default Hardware Switch Settings

All hardware switches can be overridden through software commands. The card's default settings are listed below.

Auto-Negotiation . . . . . Enabled (UP)

Duplex[6] . . . . . Full (UP)

Link Loss Carry Forward. . . . . .Disabled (DOWN)

Link Loss Return. . . . . .Disabled (DOWN)

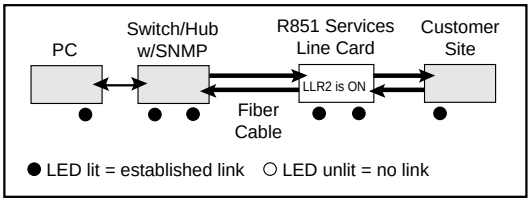
Speed[7] . . . . . 100 Mbps (UP)

Link Loss Return (LLR)

The fiber optic port(s) of the R851 services line card have been designed with LLR to assist in troubleshooting. On the R851-SS, LLR is configured independently for each port.

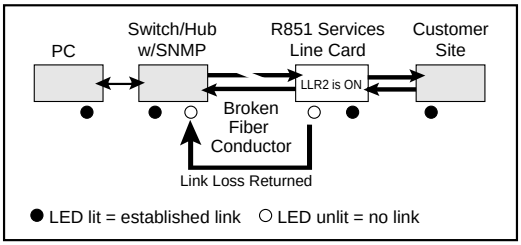
When LLR is enabled, the fiber port's transmitter shuts down if its receiver fails to detect a valid receive link. The transmitter will remain off except to periodically transmit heartbeat pulses. Every second, the transmitter will attempt to establish link for 100 ms.

The diagram below shows a typical network configuration with good link status using a services line card for remote connectivity. LLR is enabled on Port 2.



If one of the fiber cables is bad (as shown in the diagram box below), the R851 will return a no link condition to its link partner. This helps the network administrator in determining the source of the loss.

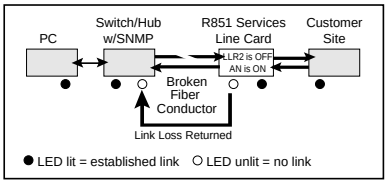
6.Applicable only to the R851-1S.
7.Applicable only to the R851-1S.

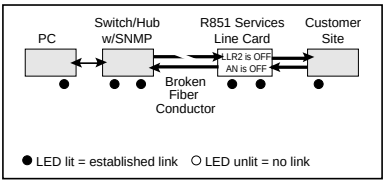


If LLR is disabled and the port's receiver loses link, the port's transmitter behavior will depend on the auto-negotiation setting. If auto-negotiation is enabled, the transmitter will shut down. If auto-negotiation is disabled, the transmitter will continue to stay up. The following table describes the transmitter's response when the port stops detecting link, based on the LLR and auto-negotiation settings.

Table 1: Transmitter Behavior When Port Loses Link

LLR	Auto-Negotiation	Fiber Transmitter
Disabled	Enabled	Off
Disabled	Disabled	On

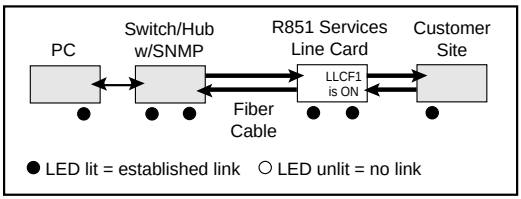




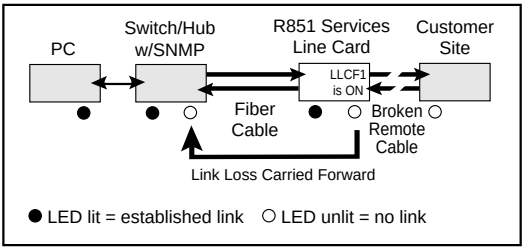
Link Loss Carry Forward (LLCF)

The R851 incorporates LLCF as an aid in troubleshooting a remote connection. When LLCF is enabled using the DIP switch, it is applied to both ports simultaneously. Through software, LLCF can be disabled or enabled independently on each port.

The diagram below shows a typical network configuration with good link status using a services line card for remote connectivity. LLCF is enabled on Port 1.



If the remote cable breaks or fails, the R851 carries that link loss forward to the switch/hub which generates a trap to the management station. The administrator can then determine the source of the problem.



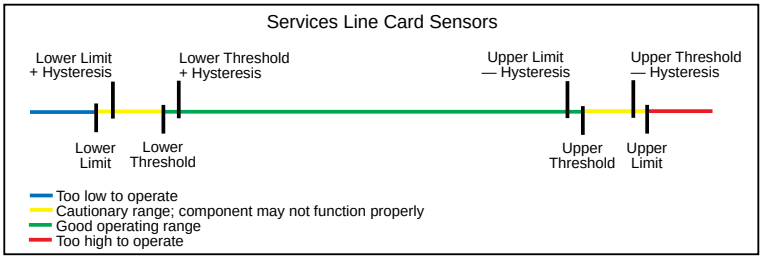
Traps

By default, all traps for the R851 are enabled. Through software, each trap can be disabled/enabled individually for each trap destination. The R851 supports up to four trap destinations. The following table describes the events that trigger SNMP trap messages to be sent to each trap destination that is configured to receive them.

Table 2: Traps Table

Trap Index	Trap Trigger
1	Sensor[a] drops and reaches its lower limit.
2	Sensor returns from lower limit plus hysteresis[b] value.
3	Sensor rises and reaches its upper limit.
4	Sensor returns from upper limit minus hysteresis value.
5	Sensor drops and reaches its lower threshold.
6	Sensor returns from the lower threshold plus hysteresis value.
7	Sensor rises and reaches its upper threshold.
8	Sensor returns from the upper threshold plus hysteresis value.
9	SFP transceiver is inserted into a port.
10	SFP transceiver is removed from a port.
11	Link Loss Carry Forward occurs.
12	Link Loss Carry Forward is reset.
13	Link Loss Return occurs.
14	Link Loss Return is reset.
15	Port receives Far End Fault notification.
16	Port receives notification that Far End Fault has been reset.

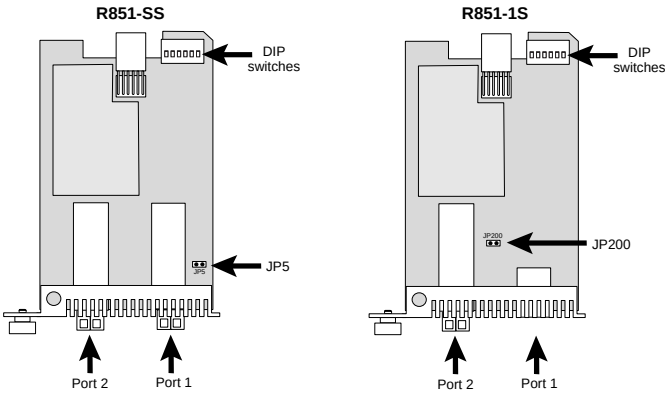
a.The R851 includes sensors that measure the circuit board temperature, SFP transceiver temperature, SFP transmit and receive laser levels, and circuit board power supply voltages.
b.The hysteresis value is an additional value added or subtracted from the limits or thresholds when traversing back and forth over the limit or threshold. This is intended to reduce the number of false warnings and to avoid the flooding of the warning messages.



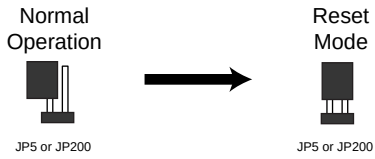
Resetting the Board

This section describes the steps required to reset the services line card back to its factory default settings.

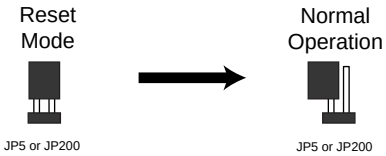
1. Locate the 2-pin jumper on the main circuit board. The jumper is labeled JP5 on the R851-SS and JP200 on the R851-1S.



2. A connector is attached to one of the pins on the jumper. Remove the connector and place it so both pins are covered, as shown below.



3. Install the card into the chassis. The board will automatically reset itself back to its original default settings. When the process is complete, the DIS and LBK LEDs on the front panel will blink.
4. Remove the card from the chassis.
5. Remove the connector from the two pins and place it onto one pin. The R851 is now ready for normal use.



Changing the SFP Transceiver

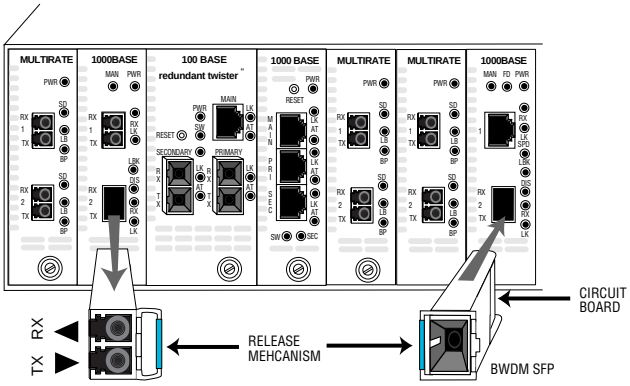
Depending on the model, the services line card supports one or two replaceable small form-factor pluggable (SFP) transceivers. This section explains how to remove and install these parts.

Important: *Use only Metrobility-supplied SFP transceivers with this product.* Installing any other part may damage the unit and will void the product's warranty.

1. Disconnect the fiber optic network cables, if they are installed, from both the transmitter (TX) and receiver (RX) on the SFP transceiver.

   WARNING: Avoid looking into the laser or cable.

2. To remove the SFP transceiver from services line card, simply pull the release mechanism (i.e., plastic tab, bail latch, etc.) and slide the module out of the slot, as shown below.



3. Align the new SFP module so the receiver (▲) is positioned above the transmitter (▼). For a BWDM SFP, align it so the visible part of the circuit board located at the back of the module is to the right.

4. Slide the new SFP module into the slot, pushing it firmly in place.

5. Remove the protective covering on the connector.

6. Reconnect the network cables. Verify proper segment connectivity via the green LK LED, which should be lit.

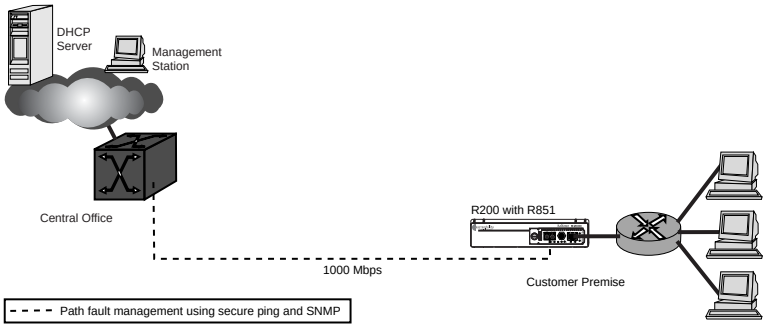
Topology Solutions

Standards-Based Multi-Service Delivery

The R851 services line card supports the delivery of point-to-point E-Line and multi-point E-LAN services as defined by the Metro Ethernet Forum. Traffic belonging to each service is classified by, and tunneled over, predetermined VLANs for segregation and transport across carrier networks. Controlled at the service line card, VLANs identify and segregate the specific ISP-access or corporate-access E-Line service, and determine corresponding prioritization and traffic management parameters for the associated traffic. Management traffic, either tagged or untagged, is given higher priority than user data traffic.

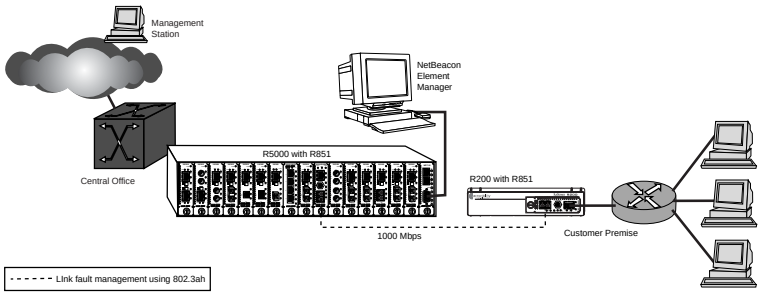
Basic Remote Management as a NID

The Radiance GbE services line card can be used with any of Metro-bility's Premise Service Platforms including the Radiance R1000, R400, and R200. Together, the platform and card create a network interface device (NID) that serves as a demarcation point at the customer site. The NID is designed specifically to maintain maximum isolation between the public and private networks. Carrier class management access control protects against denial of service on the management channel. DHCP is enabled on the R851 for obtaining its management (end-station) IP address, network mask, and default gateway. The R851 responds to SNMP requests by delivering information on its health, status, and network connections. Remote management from the Central Office is provided through SNMP using the NID's unique IP address.



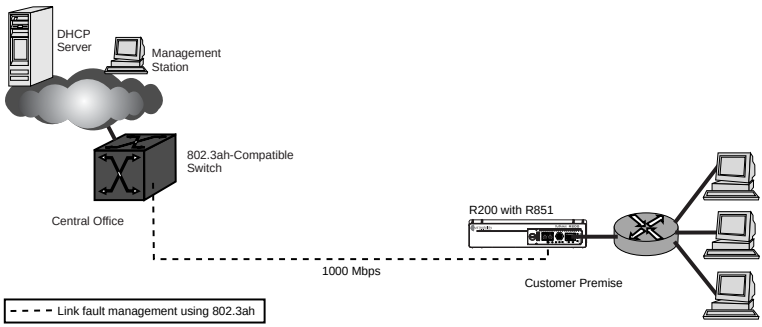
802.3ah-Based Enhanced Remote Management

A Radiance R5000 Central Service Platform in a central office or point of presence connects to a switch or router at the service provider's network. The R5000 includes a management card that collects information from the services line card, which is monitored and managed through Metrobility's NetBeacon Element Manager. In addition to standards-based link OAM, this bookended configuration enables extensions to 802.3ah OAM including the provisioning of IP end-station parameters, quality of line, quality of equipment, optical power, and historical graphs.



Future 802.3ah-Based Remote Management

The embedded software in the services line card is field upgradable. As new software is developed to support evolving standards, new features, and compatibility with IEEE 802.3ah OAM-enabled Layer 2/3 switches, it can easily be downloaded onto the device. Two versions of the operational software and FPGA firmware can be stored on the services line card.



Upgrading from Older OS Versions (1.00.09 or lower)

If your operating system version is 1.00.09 or lower, follow the procedure outlined in this section to upgrade your software.

Note: *Once the OS is upgraded, you will not be able to revert back to a version less than 1.1.0.*

OS version 1.1.0 and higher use a compressed image format and require different boot and FPGA codes from that used with earlier versions. Upgrading from an older version of the OS requires you to download four separate files:

- r851_10010.bin, an intermediate OS that allows the migration to compressed files
- r851_11000.bin, the new OS (the actual name of the file may be slightly different, depending on the version to which you are upgrading)
- boot.bin, the new boot code
- control_11000.bin, the new FPGA code (the actual name of the file may be slightly different, depending on the version to which you are upgrading)

The following example illustrates how to upgrade from an older OS to version 1.1.0. In the example, the active OS is OS1 and the active FPGA is FPGA1. (To see which versions are currently active on your device, use the “show systeminfo” command.) The software is downloaded through Port 1 of the services line card.

1. Download the intermediate OS into the secondary OS location, OS2, and then activate it using the reset command. Downloading the software may take 5 to 6 minutes to complete.
2. Enable management access for the port that will be used for downloading. In this example, the file is downloaded via Port 1.
3. Download the new OS into the primary OS location, OS1.
4. Download the boot code.
5. Download the new FPGA code into the secondary location, FPGA2.

6. Activate the new OS and FPGA.
7. Download the new OS into the secondary location, OS2. This will set both banks to the new images.
8. Download the new FPGA into the primary location, FPGA1. This will set both banks to the new code.

To verify that the OS and FPGA have been upgraded, use the “show systeminfo” command. The active OS and FPGA versions will be among the parameters shown.

1. Download the Intermediate OS

```
Console> set download 192.168.1.100 filename r851_10010.bin protocol tftp
    server: 192.168.1.100
    filename: r851_10010.bin
    protocol: tftp
    username:

Console> download os2

Console> set os 2
    Active OS image number: 2
Console> reset
```

2. Enable Port Management

```
Console> set port 1 management enable
```

3. Download the New OS

```
Console> set download 192.168.1.100 filename r851_110.bin
    server: 192.168.1.100
    filename: r851_110.bin
    protocol: tftp
    status: Previous Flash burn completed successfully
Console> download os1
Console> Transferring file r851_110.bin
Validating file checksum
Enabling FLASH for burn.
Preparing to burn image in external FLASH
Erasing external FLASH blocks.
Burning image in external FLASH
.....
..
Burn completed. Validating data.
```

4. Download the New Boot Code

```
Console> set download 192.168.1.100 filename boot.bin
    server: 192.168.1.100
```

```
    filename: boot.bin
    protocol: tftp
    status: Previous Flash burn completed successfully
Console> download boot
Warning: It is important that this download not be interrupted.
Do you want to continue (y/n)? Console> Transferring file boot.bin
Validating file checksum
Enabling FLASH for burn.
Writing image to Z80 internal FLASH
.
FLASH verification in progress.
.
Locking Z80 internal FLASH.
```

5. Download the New FPGA Code

```
Console> set download 192.168.1.100 filename control_110.bin
    server: 192.168.1.100
    filename: control_110.bin
    protocol: tftp
    status: Previous Flash burn completed successfully
Console> download fpga2
Transferring file control_110.bin
Validating file checksum
Enabling FLASH for burn.
Writing image to internal FLASH
. . . . . .
FLASH verification in progress.
. . . . . .
Locking internal FLASH.
```

6. Activate the New OS and FPGA

```
Console> set os 1
    OS1 image (1.1.0) will not become active until next reboot.
Console> set fpga 1
    FPGA1 image (1.1.0) will not become active until next reboot.
Console> reset
This command will reset the entire system.
Do you want to continue (y/n)?

Resetting device...
```

7. Download the New OS to the Secondary Location

```
Console> set download 192.168.1.100 filename r851_110.bin
    server: 192.168.1.100
    filename: r851_110.bin
    protocol: tftp
    status: Previous Flash burn completed successfully
Console> download os2
Console> Transferring file r851_110.bin
```

```
Validating file checksum
Enabling FLASH for burn.
Preparing to burn image in external FLASH
Erasing external FLASH blocks.
Burning image in external FLASH
.....
..
Burn completed. Validating data.
```

8. Download the New FPGA to the Primary Location

```
Console> set download 192.168.1.100 filename control_110.bin
    server: 192.168.1.100
    filename: control_110.bin
    protocol: tftp
    status: Previous Flash burn completed successfully
Console> download fpga1
Transferring file control_110.bin
Validating file checksum
Enabling FLASH for burn.
Writing image to internal FLASH
.....
FLASH verification in progress.
.....
Locking internal FLASH.
```

Technical Specifications

Data Rate

Data Rate _____ 1000Mbps full duplex

Power

Input
(R851-1S) _____ 5 V DC @1.0 A, 5.0 W
(R851-SS) _____ 5 V DC @1.6 A, 8.0 W

Environmental

Operating Temperature _____ 0° to 50° C
Storage Temperature _____ -25° to 70° C
Operating Humidity _____ 5% to 95% non-condensing
Weight _____ 3.2 oz (0.09 kg)

Network Connections

Twisted-Pair Interface

Connector _____ Shielded RJ-45, 8-pin jack
Impedance _____ 100 ohms nominal
Supported Link Length _____ 100 m
Signal Level Output (peak differential) _____ 2.2 to 2.8 V (10 Mbps)
_____ 0.95 to 1.05 V (100 Mbps)
Signal Level Input (minimum) _____ 585 mV (10 Mbps)
_____ 200 mV (100 Mbps)
Cable Type _____ CAT 3, 4, 5 UTP (10 Mbps)
_____ CAT 5 UTP (100 Mbps)
_____ CAT 5 or 5E UTP/STP (1000 Mbps)
(For NEBS Level III and EN55024:1998 compliance, use only CAT 5E STP cables.)

Multimode Fiber Optic Plug-in (O211-M5)

Connector _____ LC
Wavelength _____ 850 nm
RX Input Sensitivity _____ -19 dBm (min), -22 dBm (typ), 0 dBm (sat)
Output Power _____ -9 dBm to -3.5 dBm; -6 dBm (typical)
Typical Link Budget _____ 16 dB
Supported Link Length _____ up to 500 m
Cable Type _____ 50/125 or 62.5/125 µm multimode or 9/125 µm

Singlemode Fiber Optic Plug-in (O211-10)

Connector _____ LC
Wavelength _____ 1310 nm
RX Input Sensitivity_____ -20 dBm (min), -23 dBm (typ), -3 dBm (sat)
Output Power _____ -9.5 dBm to -3 dBm; -6 dBm (typical)
Typical Link Budget_____ 17 dB
Supported Link Length _____ up to 10 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O211-25)

Connector _____ LC
Wavelength _____ 1310 nm
RX Input Sensitivity_____ -21 dBm (min), -23 dBm (typ)
Output Power _____ 0 dBm to 5 dBm; 2 dBm (typical)
Typical Link Budget_____ 25 dB
Supported Link Length _____ up to 25 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O211-40)

Connector _____ LC
Wavelength _____ 1550 nm
RX Input Sensitivity_____ -24 dBm (min) -26 dBm (typ), -3 dBm (sat)
Output Power _____ -5 dBm to 0 dBm; -2.5 dBm (typical)
Typical Link Budget_____ 23.5 dB
Supported Link Length _____ up to 40 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O211-70)

Connector _____ LC
Wavelength _____ 1550 nm
RX Input Sensitivity_____ -24 dBm (min), -26 dBm (typ), -3 dBm (sat)
Output Power _____ 0 dBm to 5 dBm; 2 dBm (typical)
Typical Link Budget_____ 28 dB
Supported Link Length _____ up to 70 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O211-1A)

Connector _____ LC
Wavelength _____ 1550 nm
RX Input Sensitivity_____ -32 dBm (min), -34 dBm (typ), -3 dBm (sat)
Output Power _____ 0 dBm to 5 dBm; 2 dBm (typical)
Typical Link Budget_____36 dB
Supported Link Length _____ up to 100 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O311-10-xx) for BWDM

Connector _____ SC
Wavelength (O311-10-31)_____ 1310 nm TX / 1490 nm RX
Wavelength (O311-10-49)_____ 1490 nm TX / 1310 nm RX
RX Input Sensitivity_____ -22 dBm (min), -24 dBm (typ), -3 dBm (sat)
Output Power _____-9 dBm to -3 dBm; -6 dBm (typical)
Typical Link Budget_____18 dB
Supported Link Length _____ up to 10 km
Cable Type _____ 9/125 µm singlemode

Singlemode Fiber Optic Plug-in (O411-80-xx) for CWDM

Connector _____ LC
Wavelength _____(see table below)
RX Input Sensitivity_____ -24 dBm (min), -26 dBm (typ), -3 dBm (sat)
Output Power _____ 0 dBm to 5 dBm; 2 dBm (typical)
Typical Link Budget_____28 dB
Supported Link Length _____ up to 80 km
Cable Type _____ 9/125 µm singlemode

Model Number	Wavelength
O411-80-31	1310 nm
O411-80-33	1330 nm
O411-80-35	1350 nm
O411-80-37	1370 nm
O411-80-39	1390 nm
O411-80-41	1410 nm
O411-80-43	1430 nm
O411-80-45	1450 nm
O411-80-47	1470 nm
O411-80-49	1490 nm

Model Number	Wavelength
O411-80-51	1510 nm
O411-80-53	1530 nm
O411-80-55	1550 nm
O411-80-57	1570 nm
O411-80-59	1590 nm
O411-80-61	1610 nm

Abbreviations and Acronyms

AN	Auto-Negotiation
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
BWDM	Bidirectional Wavelength Division Multiplexing
CLI	Command Line Interface
CPE	Customer Premises Equipment
CWDM	Coarse Wavelength Division Multiplexing
dB	Decibel
dBm	Decibel relative to 1 mW of power (0 dBm equals 1 mW)
DHCP	Dynamic Host Configuration Protocol
DIS	Disable management on a port
DUP	Duplex
E-LAN	Ethernet Local Area Network
E-Line	Ethernet Line
FD	Full Duplex
FEF	Far End Fault
FPGA	Field Programmable Gate Array
GARP	Generic Attribute Registration Protocol
GbE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol

ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISP	Internet Service Provider
km	Kilometer
L2	Layer 2
LACP	Link Aggregation Control Protocol
LBK	Loopback
LK	Link
LLCF	Link Loss Carry Forward
LLR	Link Loss Return
MAC	Media Access Control
MAN	Managed
Mbps	Megabits per second
MIB	Management Information Base
ms	Millisecond
MSTP	Multiple Spanning Tree Protocol
mV	Millivolt
NID	Network Interface Device
nm	Nanometer
OAM	Operation, Administration, and Maintenance
OAMPDU	Operation, Administration, and Maintenance Protocol Data Unit
OS	Operating System
OUI	Organizational Unique Identifier
PWR	Power
PDU	Protocol Data Unit
RFC	Request for Comments
RMON	Remote Monitoring

RSTP	Rapid Spanning Tree Protocol
RX	Receive
SFP	Small Form-factor Pluggable optical transceiver
SNMP	Simple Network Management Protocol
SPD	Speed
STP	Shielded Twisted Pair; Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
TX	Transmit
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VID	VLAN identifier
VLAN	Virtual Local Area Network
zeroconf	zero configuration

Product Safety and Compliance Statements

This product complies with the following requirements:

- UL
- CSA
- CE
- CB
- NEBS Level III
- EN60950 (safety)
- FCC Part 15, Class B
- DOC Class B (emissions)
- EN55022 Class B (emissions)
- EN55024: 1998 (immunity)
- IEC 825-1 Classification (eye safety)
- Class 1 Laser Product (eye safety)

This product shall be handled, stored and disposed of in accordance with all governing and applicable safety and environmental regulatory agency requirements.

The following FCC and Industry Canada compliance information is applicable to North American customers only.

USA FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: *Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.*

Canadian Radio Frequency Interference Statement

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

Standards Compliance

This equipment complies with the following standards:

- IEEE 802.1D-1998 Forwarding Aspects
- IEEE 802.1Q-2002 VLAN Bridge Forwarding Aspects
- IEEE 802.3-2002
- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 950 (Internet Standard Subnetting Procedure)
- RFC 1157 (SNMPv1)
- RFC 1213 (MIB-II)
- RFC 1349 (IP) — updates RFC 791

- RFC 1350 (TFTP)
- RFC 1782 (TFTP) — updates RFC 1350
- RFC 1783 (TFTP) — updates RFC 1350
- RFC 1784 (TFTP) — updates RFC 1350
- RFC 1785 (TFTP) — updates RFC 1350
- RFC 2011 (MIB-II) — updates RFC 1213
- RFC 2012 (MIB-II) — updates RFC 1213
- RFC 2013 (MIB-II) — updates RFC 1213
- RFC 2131 (DHCP)
- RFC 2347 (TFTP) — updates RFC 1350
- RFC 2348 (TFTP) — updates RFC 1350
- RFC 2349 (TFTP) — updates RFC 1350
- RFC 2819 (RMON Group 1)
- RFC 2863 (Interfaces Group MIB) — updates RFC 1213
- RFC 3168 (TCP) — updates RFC 793
- RFC 3273 (RMON Group 1)
- RFC 3396 (DHCP) — updates RFC 2131

Warranty and Servicing

Three-Year Warranty for the Radiance Gigabit Ethernet Services Line Card

Metrobility Optical Systems, Inc. warrants that every Radiance **Gigabit Ethernet** services line card will be free from defects in material and workmanship for a period of THREE YEARS from the date of Metrobility shipment. This warranty covers the original user only and is not transferable. Should the unit fail at any time during this warranty period, Metrobility will, at its sole discretion, replace, repair, or refund the purchase price of the product. This warranty is limited to defects in workmanship and materials and does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including overvoltage failures caused by use outside of the product's specified rating, or normal wear and tear of mechanical components.

Metrobility supports only the current released version and the most recent previous minor version of the software embedded on the management card.

To establish original ownership and provide date of purchase, complete and return the registration card or register the product online at www.metrobility.com. If product was not purchased directly from Metrobility, please provide source, invoice number and date of purchase.

To return a defective product for warranty coverage, contact Metrobility Customer Service for a return materials authorization (RMA) number. Send the defective product postage and insurance prepaid to the address provided to you by the Metrobility Technical Support Representative. Failure to properly protect the product during shipping may void this warranty. The Metrobility RMA number must be clearly on the outside of the carton to ensure its acceptance.

Metrobility will pay return transportation for product repaired or replaced in-warranty. Before making any repair not covered by the warranty, Metrobility will estimate cost and obtain authorization, then invoice for repair and return transportation. Metrobility reserves the right to charge for all testing and shipping costs incurred, if test results determine that the unit is without defect.

This warranty constitutes the buyer's sole remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Under no circumstances will Metrobility be liable for any damages incurred by the use of this product including, but not limited to, lost profits, lost savings, and incidental or consequential damages arising from the use of, or inability to use, this product. Authorized resellers are not authorized to extend any other warranty on Metrobility's behalf.

ADDITIONAL IMPORTANT WARRANTY INFORMATION:

The Radiance 1000 Mbps services line card is designed to operate using only the Metrobility-supplied small form-factor pluggable (SFP) transceivers specified in this manual. The use and installation of parts not included in this document will void the product's warranty and may cause damage to the unit.

Product Manuals

The most recent version of this manual is available online at
http://www.metrobility.com/support/manuals.htm

Product Registration

To register your product, go to
http://www.metrobility.com/support/registration.asp

25 Manchester Street, Merrimack, NH 03054 USA
tel: 1.603.880.1833 • fax: 1.603.594.2887
www.metrobility.com

5660-000085 B
9/04