PRELIMINARY

Installation and Operation Manual

IPmux-11

Ethernet Multiservice Gateway

IPmux-11

Ethernet Multiservice Gateway

Installation and Operation Manual

Notice

For further information contact RAD at the address below or contact your local distributor.

International Headquarters
RAD Data Communications Ltd.

24 Raoul Wallenberg St.
Tel Aviv 69719 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com

U.S. Headquarters
RAD Data Communications Inc.

900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100, Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com

Publication No. 352-200-04/04

Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the IPmux-11 to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to DISTRIBUTOR.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR immediately notifies RAD of such defect, RAD shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that RAD requests the return of equipment, each party shall pay one-way shipping costs.

RAD shall be released from all obligations under its warranty in the event that the equipment has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than RAD's own authorized service personnel, unless such repairs by others were made with the written consent of RAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall RAD be liable for consequential damages.

RAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the IPmux-11, and in no event shall RAD's liability exceed the purchase price of the IPmux-11.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to IPmux-11 and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the IPmux-11 are provided "as is" and without warranty of any kind. RAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. RAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above RAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

RAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement and the IPmux-11 shall not exceed the sum paid to RAD for the purchase of the IPmux-11. In no event shall RAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if RAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

General Safety Instructions

The following instructions serve as a general guide for the safe installation and operation of telecommunications products. Additional instructions, if applicable, are included inside the manual.

Safety Symbols

⚠ *Warning*

This symbol may appear on the equipment or in the text. It indicates potential safety hazards regarding product operation or maintenance to operator or service personnel.

⚡

Danger of electric shock! Avoid any contact with the marked surface while the product is energized or connected to outdoor telecommunication lines.

.

⏚

Protective earth: the marked lug or terminal should be connected to the building protective earth bus.

⚠ *Warning*

Some products may be equipped with a laser diode. In such cases, a label with the laser class and other warnings as applicable will be attached near the optical transmitter. The laser warning symbol may be also attached. Please observe the following precautions:

- **Before turning on the equipment, make sure that the fiber optic cable is intact and is connected to the transmitter.**
- **Do not attempt to adjust the laser drive current.**
- **Do not use broken or unterminated fiber-optic cables/connectors or look straight at the laser beam.**
- **The use of optical devices with the equipment will increase eye hazard.**
- **Use of controls, adjustments or performing procedures other than those specified herein, may result in hazardous radiation exposure.**

ATTENTION: The laser beam may be invisible!

Always observe standard safety precautions during installation, operation and maintenance of this product. Only qualified and authorized service personnel should carry out adjustment, maintenance or repairs to this product. No installation, adjustment, maintenance or repairs should be performed by either the operator or the user.

Handling Energized Products

General Safety Practices

Do not touch or tamper with the power supply when the power cord is connected. Line voltages may be present inside certain products even when the power switch (if installed) is in the OFF position or a fuse is blown. For DC-powered products, although the voltages levels are usually not hazardous, energy hazards may still exist.

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Unless otherwise specified, all products are intended to be grounded during normal use. Grounding is provided by connecting the mains plug to a wall socket with a protective earth terminal. If an earth lug is provided on the product, it should be connected to the protective earth at all times, by a wire with a diameter of 18 AWG or wider. Rack-mounted equipment should be mounted only in earthed racks and cabinets.

Always make the ground connection first and disconnect it last. Do not connect telecommunication cables to ungrounded equipment. Make sure that all other cables are disconnected before disconnecting the ground.

Connection of AC Mains

Make sure that the electrical installation complies with local codes.

Always connect the AC plug to a wall socket with a protective ground.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Always connect the power cord first to the equipment and then to the wall socket. If a power switch is provided in the equipment, set it to the OFF position. If the power cord cannot be readily disconnected in case of emergency, make sure that a readily accessible circuit breaker or emergency switch is installed in the building installation.

Connection of DC Mains

Unless otherwise specified in the manual, the DC input to the equipment is floating in reference to the ground. Any single pole can be externally grounded.

Due to the high current capability of DC mains systems, care should be taken when connecting the DC supply to avoid short-circuits and fire hazards.

DC units should be installed in a restricted access area, i.e. an area where access is authorized only to qualified service and maintenance personnel.

Make sure that the DC supply is electrically isolated from any AC source and that the installation complies with the local codes.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Before connecting the DC supply wires, ensure that power is removed form the DC circuit. Locate the circuit breaker of the panel board that services the equipment and switch it to the OFF position. When connecting the DC supply wires, first connect the ground wire to the corresponding terminal, then the positive pole and last the negative pole. Switch the circuit breaker back to the ON position.

A readily accessible disconnect device that is suitably rated and approved should be incorporated in the building installation.

Connection of Data and Telecommunications Cables

Data and telecommunication interfaces are classified according to their safety status.

The following table lists the status of several standard interfaces. If the status of a given port differs from the standard one, a notice will be given in the manual.

Ports	Safety Status	
V.11, V.28, V.35, V.36, RS-530, X.21, 10 BaseT, 100 BaseT, Unbalanced E1, E2, E3, STM, DS-2, DS-3, S-Interface ISDN, Analog voice E&M	SELV	Safety Extra Low Voltage: Ports which do not present a safety hazard. Usually up to 30 VAC or 60 VDC.
xDSL (without feeding voltage), Balanced E1, T1, Sub E1/T1	TNV-1	Telecommunication Network Voltage-1: Ports whose normal operating voltage is within the limits of SELV, on which overvoltages from telecommunications networks are possible.
FXS (Foreign Exchange Subscriber)	TNV-2	Telecommunication Network Voltage-2: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are not possible. These ports are not permitted to be directly connected to external telephone and data lines.
FXO (Foreign Exchange Office), xDSL (with feeding voltage), U-Interface ISDN	TNV-3	Telecommunication Network Voltage-3: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are possible.

Always connect a given port to a port of the same safety status. If in doubt, seek the assistance of a qualified safety engineer.

Always make sure that the equipment is grounded before connecting telecommunication cables. Do not disconnect the ground connection before disconnecting all telecommunications cables.

Some SELV and non-SELV circuits use the same connectors. Use caution when connecting cables. Extra caution should be exercised during thunderstorms.

When using shielded or coaxial cables, verify that there is a good ground connection at both ends. The earthing and bonding of the ground connections should comply with the local codes.

The telecommunication wiring in the building may be damaged or present a fire hazard in case of contact between exposed external wires and the AC power lines. In order to reduce the risk, there are restrictions on the diameter of wires in the telecom cables, between the equipment and the mating connectors.

Caution To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cords.

Attention Pour réduire les risques s'incendie, utiliser seulement des conducteurs de télécommunications 26 AWG ou de section supérieure.

Some ports are suitable for connection to intra-building or non-exposed wiring or cabling only. In such cases, a notice will be given in the installation instructions.

Do not attempt to tamper with any carrier-provided equipment or connection hardware.

Electromagnetic Compatibility (EMC)

The equipment is designed and approved to comply with the electromagnetic regulations of major regulatory bodies. The following instructions may enhance the performance of the equipment and will provide better protection against excessive emission and better immunity against disturbances.

A good earth connection is essential. When installing the equipment in a rack, make sure to remove all traces of paint from the mounting points. Use suitable lock-washers and torque. If an external grounding lug is provided, connect it to the earth bus using braided wire as short as possible.

The equipment is designed to comply with EMC requirements when connecting it with unshielded twisted pair (UTP) cables. However, the use of shielded wires is always recommended, especially for high-rate data. In some cases, when unshielded wires are used, ferrite cores should be installed on certain cables. In such cases, special instructions are provided in the manual.

Disconnect all wires which are not in permanent use, such as cables used for one-time configuration.

The compliance of the equipment with the regulations for conducted emission on the data lines is dependent on the cable quality. The emission is tested for UTP with 80 dB longitudinal conversion loss (LCL).

Unless otherwise specified or described in the manual, TNV-1 and TNV-3 ports provide secondary protection against surges on the data lines. Primary protectors should be provided in the building installation.

The equipment is designed to provide adequate protection against electro-static discharge (ESD). However, it is good working practice to use caution when connecting cables terminated with plastic connectors (without a grounded metal hood, such as flat cables) to sensitive data lines. Before connecting such cables, discharge yourself by touching earth ground or wear an ESD preventive wrist strap.

FCC-15 User Information

This equipment has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Installation and Operation manual, may cause harmful interference to the radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Emission Requirements

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulation.

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

Warning per EN 55022 (CISPR-22)

Warning This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.

Avertissement Cet appareil est un appareil de Classe A. Dans un environnement résidentiel, cet appareil peut provoquer des brouillages radioélectriques. Dans ces cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

Achtung Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkströrungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Quick Start Guide

Installation of IPmux-11 should be carried out only by an experienced technician. If you are familiar with IPmux-11, use this guide to prepare the units for operation.

1. Installing IPmux-11

Connecting the Interfaces

1. Connect the network to the RJ-45 connector designated ETH 1.
2. Connect the user LAN(s) to the RJ-45 connector(s) designated ETH 2 or ETH 3.
3. Connect the E1 or T1 line to the RJ-45 connector designated E1 or T1.

Caution When connecting balanced E1 or T1 equipment, make sure to use only 4-wire RJ-45 connectors with the following pins used for receiving and transmitting data: 1, 2, 4, 5. Do not use 8-pin RJ-45 connectors.

4. Connect the control terminal to the rear panel CONTROL connector.

   or

   Connect a Telnet host, or a PC running a Web browsing application to one of the user LAN ports.

Connecting the Power

- Connect the power cable to the power connector on the IPmux-11 rear panel.

  The unit has no power switch. Operation starts when the power is applied to the rear panel power connector(s).

2. Configuring IPmux-11

Configure IPmux-11 to the desired operation mode via an ASCII terminal connected to the rear panel CONTROL port. Alternatively, you can manage IPmux-11 over Telnet, or via a PC running a Web browsing application connected to one of the user LAN ports.

Starting Terminal Session for a First Time

➤ **To start a terminal session:**

1. Connect a terminal to the CONTROL connector of IPmux-11.
2. Start a terminal application and configure the terminal link as follows to 115,200 baud, 8 bits/character, 1 stop bit, no parity. Set the terminal emulator to ANSI VT100 emulation (for optimal view of system menus).
3. Power IPmux-11 up and proceed with management session.

Configuring the IP Management Parameters

The host IP address, subnet mask and default gateway IP address must be configured via an ASCII terminal.

➤ **To configure the IP management parameters:**

- From the Host IP menu (**Main** > **Configuration** > **System** > **Host IP**), select the set an IP address of the IPmux-11 host.

Configuring E1 and T1 at the Physical Level

E1 and T1 interface must be configured at the physical level first.

➤ **To configure E1 and T1 at the physical level:**

- From the TDM Configuration menu (**Configuration** > **Physical layer** > **TDM configuration**), configure the necessary parameters of the E1 or T1 services.

Configuring Bundle Connections

The E1/T1 timeslots must be assigned to a bundle. The bundle must be sent to the remote IP address and be connected to one of the destination bundles.

➤ **To assign timeslots to a bundle:**

- From the DS0 Bundle Configuration menu (**Main** > **Configuration** > **Connection** > **DS0 bundle configuration**), assign desired timeslots to a bundle by setting them to **1**.

➤ **To connect a bundle:**

- From the Bundle Connection Configuration menu (**Main** > **Configuration** > **Connection** > **Bundle connection configuration**), set the following:
  - Destination IP Address
  - Destination Bundle.

Configuring Internal Bridge

➤ **To configure the Ethernet policy for the internal bridge ports:**

- From the ETH Policy Configuration menu (**Main** > **Configuration** > **Bridge** > **Bridge policy configuration**), do the following:
  - Specify bridge port operation mode
  - Set default VLAN ID
  - Set default VLAN priority
  - Select rate limit for each port.

➤ **To configure VLANs for the internal bridge ports:**

- From the VLAN Table Configuration menu (**Main** > **Configuration** > **Bridge** > **VLAN table configuration**), assign VLANs for each bridge port, if necessary.

Contents

Chapter 1. Introduction

Chapter 2. Installation and Setup

Chapter 3. Operation

Chapter 4. Diagnostics and Troubleshooting

Appendix A. Connector Wiring

Appendix B. Boot Sequence and Downloading Software

Appendix C. SNMP Management

Appendix D. Configuration Menus

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview

IPmux-11 offers a solution for extending traditional E1/T1 transparently over packet switched networks (PSNs) such as IP, Ethernet, and MPLS networks. The device converts the data stream coming from its TDM ports into configurable sized packets that are extended over the Fast Ethernet network port, and vice versa. IPmux-11 offers end-to-end synchronization for voice/leased line applications. IPmux-11 also features two Fast Ethernet user ports for data (Ethernet) connectivity to the IP/Ethernet network. Management is performed locally by a terminal, or remotely via Web, Telnet, or SNMP.

The IPmux family implements TDMoIP technology to carry TDM transport over IP.

Applications

Figure 1-1 illustrates a typical IPmux-11 multiplexing voice and Ethernet traffic over an IP link.

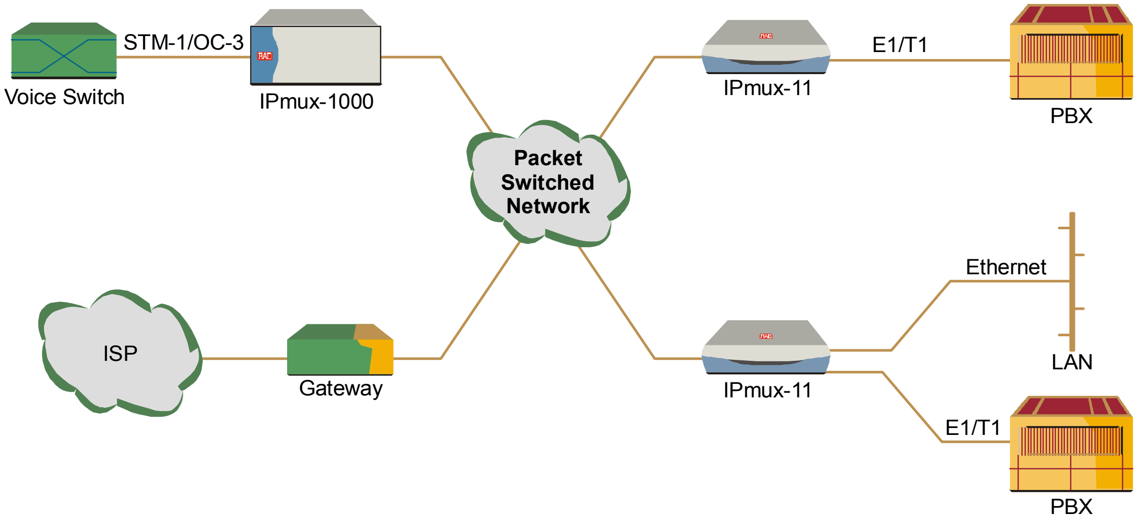


Figure 1-1. Multiplexing Voice and Ethernet over a Packet Switched Network

Features

E1

The E1 port complies with G.703, G.704, and G.823 standards. E1 framers comply with G.704. The E1 framers support unframed, framed, CRC-4 MF and CAS MF framing. The E1 port supports long haul and short haul input signals and can be monitored for alarms and error statistics.

T1

The T1 port and framers comply with ANSI T1.403, G.703, and G.704 standards. T1 jitter performance is according to G.824 and TR-62411. The T1 framers support unframed, SF, ESF and Robbed Bit signaling. The T1 port supports long haul and short haul input/output signals and can be monitored for alarms and error statistics. FDL and transmit performance monitoring for T1/ESF are also supported.

Ethernet Ports

IPmux-11 is available with three Ethernet ports (two user and one network port). The Ethernet ports work in the following bridge modes:

- Transparent
- Tagged
- Untagged
- Double Tagged.

Note *Half-duplex operation in the IPmux-11 network port is not recommended when transmitting small-size packets, because collisions and backoffs cause large delay variation and may exceed the delay variation buffer tolerance at the receiving end, resulting in buffer underflows and errors.*

IP

The data stream coming from the E1 or T1 port is converted into IP packets that are transported over the Fast Ethernet ports, and vice versa.

TDM bytes are encapsulated in a UDP frame that runs over IP and over Ethernet.

The number of TDM bytes in an IP frame is configurable for throughput/delay tradeoff.

Each device has a single IP address (Host IP). A configurable destination IP address is assigned to the IP packets. IP ToS field support can be configured for IP Level Priority.

The Ethernet ports can be either UTP or fiber.

- **Fiber option** – standard 100BaseFx full-duplex port (see *Table 1-1*).
- **UTP option** – A standard 10/100BaseT half/full-duplex port with auto-negotiation support. If auto-negotiation is disabled, Ethernet mode should be configured.

Table 1-1. Fiber Optic Interface Options

Wavelength [nm]	**Fiber Type** [μm]	**Transmitter Type**	**Power** [dBm]		**Receiver Sensitivity** [dBm]	**Loss** [km/miles]		**Budget** [dBm]	**Connector Type**
			Min	Max		Min	Max		
1310	62.5/125 multimode	VCSEL	-20	-14	-31	1	4	8*	SC
1310	9/125 single mode	Laser	-20	-14	-31	0.5	0.8	8*	SC
1310	62.5/125 multimode	VCSEL	-19	-14	-32	1	4	10*	LC
1310	9/125 single mode	Laser	-15	-8	-32	0.5	0.8	14*	LC

* Permitted fiber optic cable length differs according to fiber characteristics, splices, and connectors.

➤ **To calculate optical budget:**

Optical Budget [dB] =
│Receive Sensitivity│–│Optical Power│–3 (Aging) – Connectors/Patch Panels Loss

➤ **To calculate distance:**

Distance = Optical Budget/Maximum Loss

TDMoIP Operation Modes

E1/T1 operation modes are:

- Unframed E1/T1 over UDP over IP over Ethernet
- Fractional E1/T1 over UDP over IP over Ethernet
- Fractional E1/T1 with CAS over UDP over IP over Ethernet.

QoS

QoS supports:

- Labeling IP level priority (ToS/Diffserv) for TDMoIP packets
- VLAN tagging and priority labeling according to IEEE 802.1p&Q for TDMoIP packets.

The user can configure the ToS (Type of Service) of the outgoing TDMoIP packets. This allows an en-route Layer 3 router or switch, which supports ToS, to give higher priority to IPmux-11 TDMoIP traffic for delay-sensitive and secure applications. IPmux-11 allows you to configure the **WHOLE** ToS byte field, since different vendors may use different bits to tag packets for traffic prioritization. This also enables operation according to various RFC definitions (for example RFC 2474, RFC 791). The user can also configure VLAN priority bits for Level 2 Priority.

Management

IPmux-11 can be managed locally by connecting an ASCII terminal to the RS-232 port on the rear panel, or via HTTP connection (Web-based management tool, ConfiguRAD), Telnet or SNMP. The SNMP management capability enables fully graphical, user-friendly management using the RADview Service Center TDMoIP network management stations offered by RAD, as well as management by other SNMP-based management systems.

ConfiguRAD

ConfiguRAD is user-friendly Web-based terminal management system serving for remote device configuration and maintenance. It is embedded into IPmux-11 and provided at no extra cost. ConfiguRAD can be run from any standard Web browser.

Timing

IPmux-11 maintains synchronization between TDM devices by deploying advanced clock distribution mechanisms.

Available timing modes are:

- Loopback
- Adaptive
- Internal clock
- External clock.

1.2 Physical Description

IPmux-11 is a compact easy-to-install standalone unit. A rack mounting kit option is available (ordered separately).

Figure 1-2 shows a 3-dimensional view of IPmux-11.

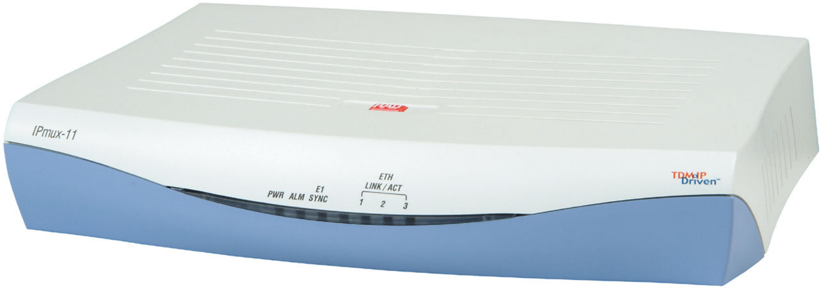


Figure 1-2. IPmux-11 3D View

The front panel includes the IPmux-11 LEDs status. For the detailed LED description, see *Chapter 3*.

User, network, external clock and management ports, and power supply connector are located on the rear panel of unit. For further details, see *Chapter 2*.

1.3 Functional Description

IPmux-11 provides TDM connectivity across the IP/Ethernet network. A single bundle (group of timeslots) can be transmitted to a predefined far-end bundle. IPmux-11 supports ICMP (ping), and generates ARP in case of unknown next hop MAC addresses, answers ARP requests, and supports 802.3 VLAN Ethernet format.

IPmux-11 includes E1 or T1 port. Traffic is transmitted over the network as E1/T1 or fractional E1/T1, using the TDMoIP method.

IPmux-11 supports two Ethernet user ports for user LAN connectivity.

Configuration and management are provided via the IPmux-11 local terminal, Web-based management utility, Telnet or RADview management tool (SNMP).

Operation Modes

This section describes theIPmux-11 operation modes, which are:

- Unframed
- Fractional
- Fractional with CAS.

Unframed (Transparent)

In the transparent mode, the incoming bit stream from each channel (regardless of framing) is converted into IP over Ethernet frames. This option provides clear channel end-to-end service (unframed).

Fractional

In the fractional mode, the incoming bit stream is regarded as a sequence of N × 64 kbps channel groups (according to framing). Each predefined group of channels is converted into a structure block. The structure block is packetized into IP frames and transmitted.

This mode allows transmission of several selected timeslots without the whole E1 or T1 frame, as in transparent mode.

Fractional with CAS

In the fractional-with-CAS mode, the structure block (as described under Fractional Operation Modes, above) also includes Channel Associated Signaling (CAS) from timeslot 16 (E1) or robbed bit (T1). The relevant portion of the signaling channel is packetized and sent to the destination.

Timeslot Assignment in a Bundle

A bundle is a group of timeslots associated with a specific E1 or T1 channel. IPmux-11 places individual or multiple TDM timeslots (up to 31 timeslots for E1 or up to 24 for T1) into bundles with a single IP address destination.

Testing

Diagnostic capabilities include E1/T1 local and remote loopback tests for rapid localization of faults. The E1/T1 traffic can be looped locally, toward the line, or toward the remote end (see *Chapter 4* for more information).

Timing Modes

The E1/T1 Tx clock can operate in several timing modes to provide maximum flexibility for connecting the IPmux-11 E1 or T1 channels.

Each of the clocks must be configured correctly on both the receive and transmit ends to ensure proper operation and prevent pattern slips (see *Figure 1-3*, *Figure 1-4* and *Figure 1-5*).

The E1/T1 available Tx modes are:

- Loopback timing – the E1/T1 Tx clock is derived from the E1/T1 receive (Rx) clock.
- Adaptive timing – in this mode, the E1 or T1 Tx clock is regenerated using the adaptive method. In this method, the fill level of the buffer receiving packets is monitored. If the buffer begins to overfill, the regenerated Tx clock frequency increases to avoid overflow. If the buffer begins to empty, the Tx clock frequency (toward the TDM device) decreases to avoid underflow.
- Internal timing – in this mode, the Tx clock is derived from an internal oscillator.
- External timing – in this mode the Tx clock is derived from the external clock input. The external clock port also outputs the input clock signal to allow connection to other units, if needed.

Note *In adaptive timing the regenerated clock is subject to network Packet Delay Variation and may not comply with jitter and wander specifications.*

Network Timing Schemes

The following paragraphs describe typical timing schemes and the correct timing mode settings for achieving end-to-end synchronization.

External Network Timing

When the edges of the network are synchronized by an external network clock source, all the IPmux-11 units should be configured to work in loopback timing mode (see *Figure 1-3*). This topology enables any-to-any connectivity.

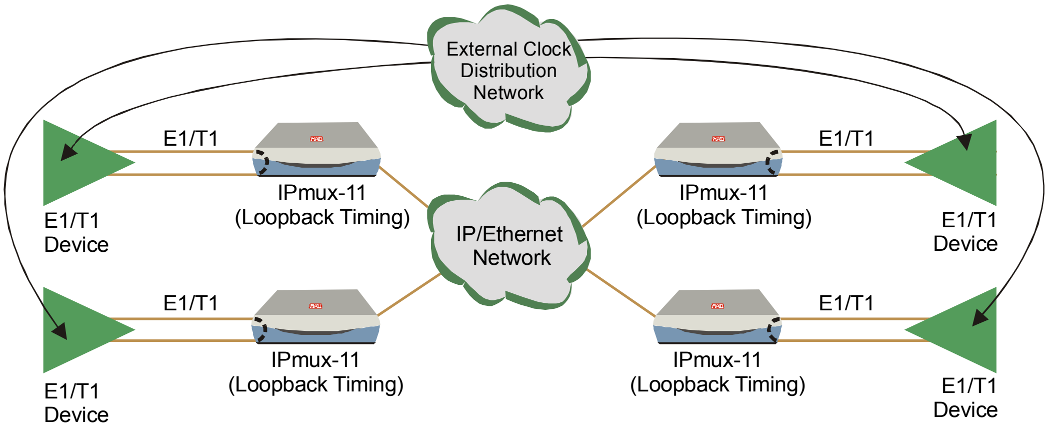

External Clock Distribution Network
E1/T1
IPmux-11 (Loopback Timing)
E1/T1 Device
IP/Ethernet Network
E1/T1
IPmux-11 (Loopback Timing)
E1/T1 Device
E1/T1
IPmux-11 (Loopback Timing)
E1/T1 Device
E1/T1
IPmux-11 (Loopback Timing)
E1/T1 Device

Figure 1-3. IPmux-11 in Loopback Timing Mode

External timing from the network can also be issued to IPmux-11 by external clock input.

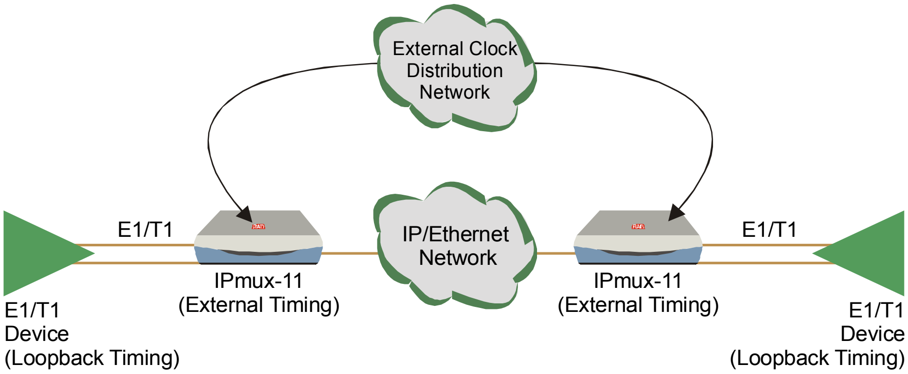

External Clock Distribution Network
E1/T1
IPmux-11 (External Timing)
IP/Ethernet Network
IPmux-11 (External Timing)
E1/T1
E1/T1 Device (Loopback Timing)
E1/T1 Device (Loopback Timing)

Figure 1-4. IPmux-11 in External Clock Mode

Single Source Clock Network

When a common clock is not available on all the ends of the network one of the IPmux-11 devices is configured to work in loopback timing, while the other IPmux-11device is configured to work in adaptive timing (see *Figure 1-5*).

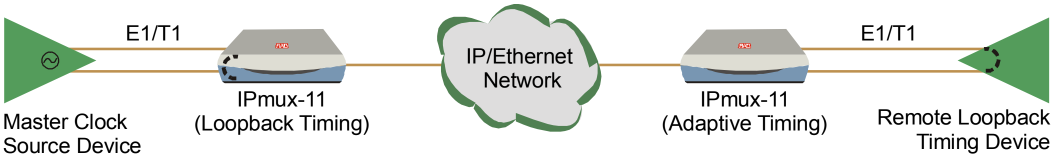

E1/T1
Master Clock Source Device
IPmux-11 (Loopback Timing)
IP/Ethernet Network
IPmux-11 (Adaptive Timing)
E1/T1
Remote Loopback Timing Device

Figure 1-5. IPmux-11 in Adaptive Timing Mode

Frame Format

The Ethernet frame sent by IPmux-11 is a UDP datagram that transfers E1/T1 payload bytes over IP over Ethernet (UDP payload + UDP header + IP header + Ethernet header). The UDP payload is equal to TDM bytes per frame (TDM bytes/frame configuration).

Table 1-2 specifies the structure of the different headers, special fields, and the payload in the Ethernet packet.

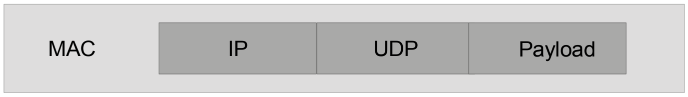


Figure 1-6. TDMoIP Frame Structure

Table 1-2. Ethernet Frame Structure

	Field length (bytes)	**Field**
MAC Layer	7	Preamble
	1	SFD
	6	Destination MAC Address
	6	Source MAC Address
LLC Layer	2	Type
IP Layer	1	Vers/HLEN
	1	Service Type
	2	Total Length
	2	Identification
	1	Flags/Fragment Offset (most)
	1	Fragment Offset (least)
	1	Time to Live
	1	Protocol
	2	Header Checksum
	4	Source IP Address
	4	Destination IP Address
UDP Layer	2	UDP Source Port
	2	UDP Destination Port
	2	UDP Message Length
	2	UDP Checksum
Data Layer	...	Payload
MAC Layer	4	CRC

Note: *IEEE 802.1p&Q VLAN Tagging (additional 4 bytes if enabled)*

Note*: The UDP source port field is used to transfer the destination bundle number in static and dynamic CAS modes.*

VLAN Support

VLAN, according to IEEE 802.1p&Q, adds four bytes to the MAC layer of the Ethernet frame. The user can set the contents of these bytes, MAC layer priority and VLAN ID. In this mode, only VLAN format frames are sent and received by IPmux-11. *Figure 1-7* shows the VLAN tag format.

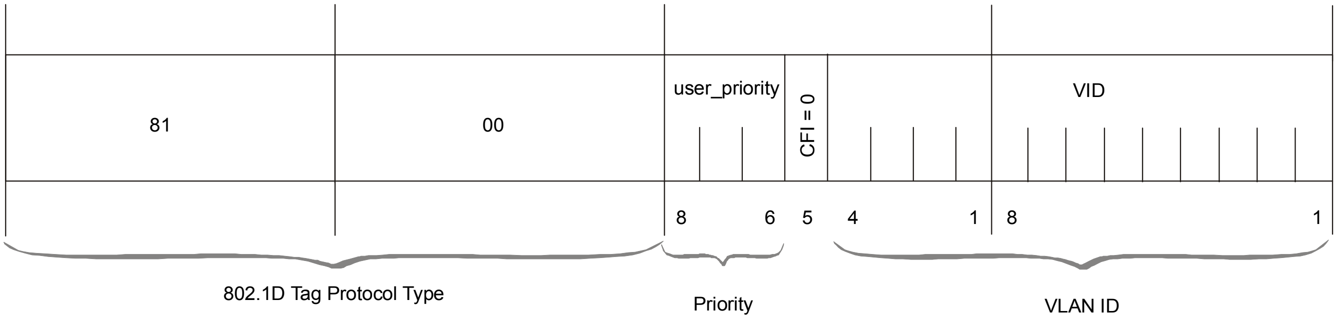


Figure 1-7. VLAN Tag Format (802.1p&Q)

UDP Support

Table 1-3. UDP Ports Definition

Field Length (Bits)	Field Description	Value	Function
2 bytes	UDP Source Port	2–497d*	Destination timeslots bundle
2 bytes	UDP Destination Port	2142d	Standard TDMoIP UDP port

* The MSB of this field can be either 1 or 0 for inband end-to-end proprietary signaling.

Note *The UDP Source Port field is used for destination timeslots bundle indication.*

For more information about VLAN tagging, refer to *IEEE Standard 802.1p&Q*.

Packet Delay Variation

Packets are transmitted at set intervals. Packet Delay Variation is the maximum deviation from the nominal time the packets are expected to arrive at the far end device. IPmux-11 has a buffer that compensates for the deviation from the expected packet arrival time to prevent IPmux-11 buffers from emptying out or overflowing.

Packet Delay Variation is an important network parameter. Large PDV (exceeding the jitter buffer configuration) will cause receive buffer underflows and errors at the TDM level (see *Figure 1-8*).

To compensate for large PDV, configure the PDVT (jitter) buffer to a higher value.

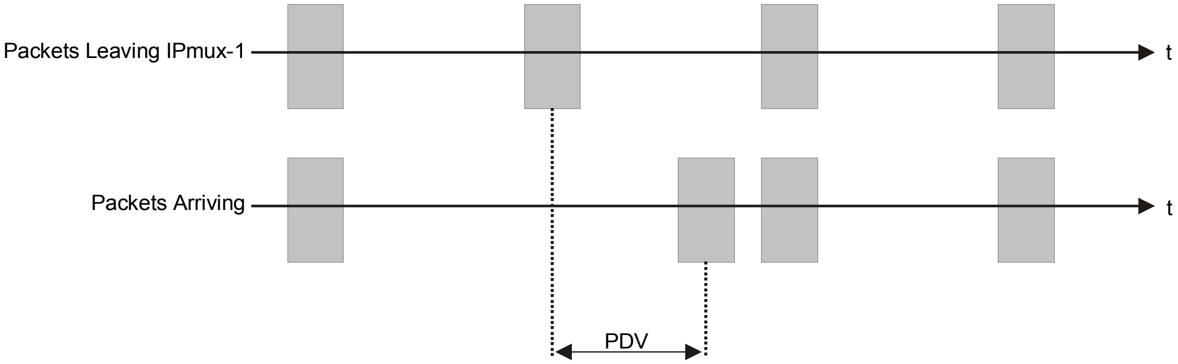


Figure 1-8. Packet Delay Variation

PDVT (Jitter) Buffer

IPmux-11 is equipped with a Packet DVT (Delay Variation Tolerance) buffer. The PDVT buffer or jitter buffer is filled by the incoming IP packets and emptied out to fill the TDM stream. The buffer begins to empty out only after it is half full in order to compensate for packet starvation from the Ethernet side. The time it takes for half of the buffer to empty out is the maximum DVT time. Delay Variation Tolerance is configurable. The PDVT (jitter) buffer is designed to compensate for packet delay variation caused by the network + intrinsic PDV.
It supports a delay variation of up to 300 ms for E1 or T1.

PDVT Buffer Effect on Delay

The PDVT buffer is on the TDM path; it adds to the total end-to-end delay (see delay calculation, below).

Intrinsic PDV in Static Mode

If TDM bytes/frame is greater than 48, there is an intrinsic delay variation (intrinsic PDV). The intrinsic PDV introduced by the module is a function of n>1 in TDM bytes/frame configuration as follows:

I.PDV (ms) = [(n-1) x 1000) / (frames per second × n]

$$\text{where } n = \frac{\text{Configured TDM bytes/frame}}{48} \quad (n = 1 \text{ to } 30).$$

➤ **To configure jitter buffer depth:**

The estimated or measured PDV introduced by the network + intrinsic PDV (if it exists) introduced by the module as a result of configuring the TDM bytes / frame > 48.

Note *For a bundle that contains a few timeslots (i.e. 1 to 3) the minimal jitter buffer should be 6 ms, and the number of TDM bytes/frame should be 48.*

Ethernet Throughput

Increasing payload size reduces the ratio of the TDMoIP header segment in the packet, thus significantly reducing the total Ethernet throughput

Increased payload reduces the IP/Ethernet overhead segment of the total packet and thus can significantly reduce the total Ethernet throughput.

On the other hand, packetization delay and intrinsic packet delay variation (PDVT) are increased; this contributes to a higher end-to-end delay. This effect can be small and negligible when a full E1 (or many timeslots) are transferred, but can be very significant when few timeslots are transferred. In this case, the packetization delay and the intrinsic PDV when configuring a large value of TDM bytes/frame can be very large and may exceed the maximum PDVT (jitter) buffer on the receiving end.

Configuring the TDM bytes per frame (TDM bytes/frame) parameter can reduce Ethernet throughput (bandwidth or traffic traveling through the Ethernet). This parameter controls the number of TDM bytes encapsulated in one frame.

The TDM bytes/frame parameter can be configured to N x 48 bytes where n is an integer between 1 and 30.

➤ **To calculate Ethernet throughput and intrinsic PDV as a function of TDM bytes/frame:**

Ethernet load (bps) =
[(frame overhead (bytes) + TDM bytes/frame) x 8] x frames/second

Frame overhead = Ethernet overhead + IP overhead = 46 bytes

Note *The frame overhead does not include:*

- *Preamble field: 7 bytes*
- *SFD field: 1 byte*
- *Interframe gap: 12 bytes*
- *VLAN field (when used): 4 bytes.*

Frame/second =
Unframed: 5447/**n** for a full E1
4107/**n** for a full T1

Framed: 8000 x **k**/(46.875 x n)

Where **k** = number of assigned timeslots

$$\text{Where } \mathbf{n} = \frac{\text{TDM bytes/frame}}{48}$$

The maximum Ethernet throughput in static mode is calculated by:

Unstructured

$$\underbrace{(\mathbf{VLAN}+\mathbf{frame\ overhead}+\mathbf{payload})}_{\text{frame size}} * \left\{\frac{\overbrace{8000 * \mathrm{TS}}^{\text{data}}}{47 * \mathrm{n}}\right\} * 8\,\text{bits}$$

Structured

$$\underbrace{(\mathbf{VLAN}+\mathbf{frame\ overhead}+\mathbf{payload})}_{\text{frame size}} * \left\{\frac{\overbrace{8000 * \mathrm{TS}}^{\text{data}} + \overbrace{\frac{8000 * \mathbf{TS}}{(47 * 8) - 1}}^{\text{pointer}} + \overbrace{500 * \left\lceil \frac{\mathbf{TS}}{2} \right\rceil}^{\mathbf{CAS}}}{47 * \mathrm{n}}\right\} * 8\,\text{bits}$$

- where **VLAN** is an optional field: if enabled it adds 4 bytes to the frame overhead
- where **payload** = number of TDM bytes in frame, (48, 96, 144, 192, … 1440)
- where **frame overhead** = size of 46 bytes, include MAC, LLC, IP and UDP layer
- where **CAS** is signaling (note: for structured mode only)
- where **TS** is number of configured time slots.

The result in both the equations is in bits per second [bps].

Round Trip Delay

The voice path round-trip delay is a function of all connections and network parameters. The calculation for E1/T1 in each connection mode is described in the following sections.

Round Trip Delay in Static Mode

$$(\pm 2\ \mu\text{s})\ \text{RTDelay}_{(\mu s)} = 2 \times [\frac{47 \times \mathbf{n}}{\mathbf{NTS}} \times 125\ \mu\text{s} + \text{PDVT buffer}\ \mu\text{s} + 1000\ \mu\text{s}] + \text{network round trip delay}$$

- where **n** = $\frac{\text{TDM bytes/frame}}{48}$
- where **NTS** = number of timeslots assigned; in unframed mode NTS is constant: 32 for E1, 24 for T1

Reorder and Duplication of Ethernet Frames

IPmux-11 handles situations in the IP network where:

- Packets are reordered by the network
- Packets are duplicated.

Reordering Frames

The ability to correct problems of reordering is only supported for odd values of payload, i.e. 1, 3, 5, 7, …, 29.

You can reorder up to seven frames; the number depends on the number of TDM bytes/frame size and buffer size.

The number of frames that can be reordered is calculated by:

$$\frac{(\text{jitterbuffer}[\text{msec}] - 1)(\text{Tsx8})}{47\text{xpayload}}$$

- where **Ts** = number of timeslots
- where **payload** = number of TDM bytes in frame, i.e. 1, 3, 5, 7, …, 29.

Note *The maximum number of frames that can be reordered is seven, even if your calculation>7.*

Duplicated Frames

When frames are duplicated, IPmux-11 only uses the later frame.

OAM Connectivity

When a destination IPmux-11 is lost, the traffic load that is transmitted to that IPmux is significantly decreased (several packets per second per connection). The IPmux starts transmitting at full rate only when it detects an IPmux at the remote side.

OAM connectivity is used to detect a valid connection (the remote IPmux will confirm it recognizes the connection and that it is enabled). It prevents flooding by a handshake.

The control packets are run over a unique bundle number that is used for this purpose. The control packets have the same VLAN ID and TOS of the originating connection. The control packet uses the TDMoIP UDP number.

OAM connectivity can be set to Disable/Enable.

Note *For control packets, the UDP check sum is not calculated nor checked.*

End-to-End Alarm Generation

An end-to-end alarm generation mechanism exists in IPmux-11 to facilitate the following alarms:

- Unframed – AIS is transmitted toward the near-end PBX in event of:
  - Far-end LOS, AIS
  - PDVT underflow/overflow.
- Framed – Timeslot/CAS configurable alarm pattern is transmitted toward the near-end PBX in event of:
  - Far-end LOS, LOF, AIS
  - PDVT underflow/overflow.

VLAN Traffic Behavior

Table 1-4 lists the IP and VLAN validity checks that are performed with each Ethernet packet that is received by IPmux-11.

Table 1-4. VLAN Check for Packets that are Received by IPmux-11

Packet Type	Source IP Check	VLAN Check
Management	Performed	Performed
TDM over IP	Performed	Performed
Receiving Ping	Not performed	Not performed, even if it is one of the IPs that is configured for the manager or for the connection
ARP	Not performed	
Telnet	Performed only when Telnet access mark is from manager	Performed only when Telnet access mark is from manager

Table 1-5 lists the IP and VLAN validity checks that are performed with each Ethernet packet that is sent by IPmux-11.

Table 1-5. VLAN Check for Packets Sent by IPmux-11

Packet Type	VLAN Support
Management	As configured for the manager
TDM over IP	As configured for the connection
Answer to Ping	If the IPmux-11 received the packet with VLAN tagging: the IPmux-11 replies with the same VLAN ID (even if it's one of IPs that is configured for the manager or for the connection) If the IPmux-11 received the packet without VLAN tagging: if it's one of the IPs that is configured for the manager or for the connection, the IPmux-11 replies with the VLAN ID that is in the manager or connection configuration
ARP initiated by us	No VLAN value unless it is to one of the managers or the connection's IP address
Telnet	
Ping initiated by us	

Ethernet Ports

The Ethernet user ports allow a user to aggregate both TDMoIP traffic and his private network LAN traffic to a single Ethernet network connection without requiring an access switch. This is a cost-effective solution for MTU or small-office applications. A rate limiter to restrict user port traffic is supported.

IPmux-11 contains an internal bridge where one of its ports is connected to a TDMoIP interworking function, two external bridge ports is used as the user ports, and the fourth is used as an Ethernet network port.

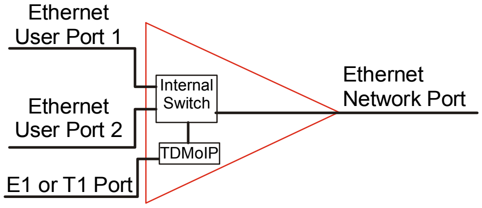


Figure 1-9. IPmux-11 with Two Ethernet User Port

Note *Priority is always given to TDMoIP packets inside the internal switch.*

Internal Switch Operation Modes

IPmux-11 offers two user LAN ports in addition to the LAN port on the network side. The device performs switching at Layer 2. The switch supports both transparent bridging and VLAN-aware bridging. The switch supports rate limiting of traffic going from the user ports to the network port. It supports up to 1024 MAC addresses (depending on their values and the order in which they are learned).

The switch modes are described later in this section. They are:

- Transparent
- Untagged
- Tagged
- Double tagged.

Rate Limiter Option

In this option a rate limiter is available to limit user port traffic. This feature is valuable when a limited bandwidth is used to extend the Ethernet link (generally when the Ethernet link rate is limited/shaped to a lower rate after IPmux). In this case TDMoIP packets will be dropped in the modem even if it was prioritized at the IPmux internal switch. This is prevented by limiting the user port to actual link rate minus TDMoIP bandwidth.

Network and user traffic can be limited to the following data rates:

Table 1-6. Rate Limiter Options

Network Interface	User Interface
128 kbps, 256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps	128 kbps, 256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 16 Mbps, 32 Mbps, 64 Mbps.

Switch Behavior When Handling User and Network Traffic

The way the network and user ports handle the traffic depends on the selected port mode (transparent, untagged, tagged or double tagged) and frame type (untagged, tagged or double tagged). *Table 1-7* lists all operation modes of the network and user ports. The modes are explained in greater detail in *Table 1-8*, *Table 1-9*, *Table 1-10*, *Table 1-11*, *Table 1-12*, *Table 1-13* and *Table 1-14*.

Table 1-7. Switch Behavior (User and Network Traffic)

Network User	Transparent	Untagged	Tagged	Double Tagged
Transparent	Mode A	Mode B	Mode C	Not applicable
Untagged	Mode B	Mode D	Mode E	Not applicable
Tagged	Mode C	Mode E	Mode F	Not applicable
Double Tagged	Mode G	Not implemented	Not implemented	Not applicable

Table 1-8. Mode A

Ingress	Egress
If a tagged frame enters a transparent port, it is switched to the other transparent port	The transparent port transmits the frame unmodified (tagged)
If an untagged frame enters a transparent port, it is switched to the other transparent port	The transparent port transmits the frame unmodified (untagged)

Table 1-9. Mode B

Ingress	Egress
If a tagged frame enters the transparent port, it is switched to the untagged port	The untagged port removes the tag, and transmits the frame untagged
If a tagged frame enters the untagged port, it is switched to the transparent port	The transparent *port* transmits the frame unmodified (tagged)
If an untagged frame enters the transparent port, it is switched to the untagged port	The untagged port transmits the frame unmodified (untagged)
If a untagged frame enters the untagged port, it is switched to the transparent port	The transparent port transmits the frame unmodified (untagged)

Table 1-10. Mode C

Ingress	Egress
If a tagged frame enters the transparent port, it is switched to the tagged port	• If the tagged port is not a member of the frame's VID, the frame is discarded • The tagged *port* is a member of the frame's VID, the frame is transmitted unmodified (tagged)
• If a tagged frame enters the tagged port, which is not a member of its VID, the frame is discarded • If a tagged frame enters the tagged port, which is a member of its VID, the frame is switched to all other members	The transparent port transmits the frame unmodified (tagged)
If an untagged frame enters the transparent port, it is switched to the tagged port	• If the tagged port is not a member of the transparent port default VID, the frame is discarded • If the tagged port is a member of the transparent port default VID, it adds tag (VID is the transparent port default VID and PRI is the transparent port default PRI), and transmits the frame tagged
• If an untagged frame enters the tagged port, which is not a member of its default VID, the frame is discarded • If an untagged frame enters the tagged port, which is a member of its VID, the frame is switched to all other members	The transparent port transmits the frame unmodified (untagged).

Table 1-11. Mode D

Ingress	Egress
If a tagged frame enters an untagged port, it is switched to the other untagged port	The untagged port removes the tag, andtransmits the frame untagged
If an untagged frame enters an untagged port, it is switched to the other transparent port	The untagged port transmits the frame unmodified (untagged)

Table 1-12. Mode E

Ingress	Egress
If a tagged frame enters the untagged port, it is switched to the tagged port	If the tagged port is not a member of the frame VID, the frame is discarded If the tagged port is a member of the frame VID, the frame is transmitted unmodified (tagged)
• If a tagged frame enters the tagged port, which is not a member of its VID, the frame is discarded • If a tagged frame enters the tagged port, which is a member of its VID, the frame is switched to all other members	The untagged port removes the tag and transmits the frame untagged
If an untagged frame enters the untagged port, it is switched to the tagged port	• If the tagged port is not a member of the untagged port default VID, the frame is discarded • If the tagged port is a member of the untagged port default VID, the tagged port adds tag (VID is the untagged port default VID and PRI is the untagged port default PRI), and transmits the frame tagged
If an untagged frame enters the tagged port, which is not a member of its default VID, the frame is discarded If an untagged frame enters the tagged port, which is a member of its default VID, the frame switched to all other members	The untagged port transmits the frame unmodified (untagged)

Table 1-13. Mode F

Ingress	Egress
• If a tagged frame enters the tagged port, which is not a member of the frame VID, the frame is discarded • If a tagged frame enters the tagged port, which is a member of the frame VID, the frame is switched to all other members	The tagged port transmits the frame unmodified (tagged.)
• If an untagged frame enters the tagged portwhich is not a member of its default VID, the frame is discarded • If an untagged frame enters the tagged portwhich is a member of its default VID, the frame is switched to all other members	The tagged port adds tag (VID is the ingress tagged port default VID and PRI is the ingress tagged port default PRI), and transmits the frame tagged

Table 1-14. Mode G

Ingress	Egress
If a double-tagged frame enters the transparent port, it is switched to the double-tagged port	The double-tagged port removes the first tag, and transmits the frame tagged
If a tagged frame enters the transparent port, it is switched to the double-tagged port	The double-tagged port removes the tag, and transmits the frame untagged
If an untagged frame enters the transparent port, it is switched to the double-tagged port	The double-tagged port transmits the frame unmodified (untagged)
If a tagged frame enters the double-tagged port, the port adds tag (VID is the double-tagged port default VID and PRI is the double-tagged port default PRI), and switches the frame to the transparent port	The transparent port transmits the frame unmodified (double tagged)
If an untagged frame enters the double-tagged port, the port adds tag (VID is the double-tagged port default VID and PRI is the double-tagged port default PRI), and switches the frame to the transparent port	The transparent port transmits the frame unmodified (tagged)

Switch Behavior When Handling Management Traffic

Table 1-15 lists operation modes of the network port when handling the management traffic.

Table 1-15. Switch Behavior (Management Traffic)

Network Option	Transparent	Untagged	Tagged	Double Tagged
Manager Tagged (SNMP)	No limitations	Not applicable	CPU and network ports must be members	Not applicable
Manager Untagged (SNMP)	No limitations	No Limitations	Not applicable	Not applicable
TDMoIP Tagged	No limitations	Not applicable	CPU and network ports must be members	Not applicable
TDMoIP Untagged	No limitations	No limitations	Not applicable	Not applicable
Ping Tagged	No limitations	No limitations	CPU and network ports must be members	Not applicable
Ping Untagged	No limitations	No limitations	Network port must be member of CPU port default VID	Not applicable
Telnet Access Enable	No limitations	No limitations	Not applicable	Not applicable
Telnet Access Managers	No limitations	See manager tagged/untagged options	See manager tagged/untagged options	Not applicable

1.4 Technical Specifications

E1 Interface	*Compliance*	ITU-T Rec. G.703, G.704, G.706, G.732, G.823
	Data Rate	2.048 Mbps
	Line Code	HDB3
	Framing	Unframed, CRC4 MF, CAS MF
	Signaling	CAS, CCS (transparent)
	Line Impedance	Balanced: 120Ω; unbalanced: 75Ω
	Signal Levels	Receive: 0 to -36 dB with LTU 0 to -10 dB without LTU
		Transmit balanced: ±3V ±10% Transmit unbalanced: ±2.37V ±10%
	Jitter Performance	Per ITU-T G.823
	Connector	Balanced: RJ-45
		Unbalanced: Two BNC coax (via an adapter cable)
T1 Interface	*Compliance*	ANSI T1.403, ITU-T Rec. G.703, G.704, G.824
	Data Rate	1.544 Mbps
	Line Code	B8ZS, B7ZS, AMI
	Framing	Unframed, SF, ESF
	Signaling	CAS (robbed bit), CCS (transparent)
	Line Impedance	Balanced: 100Ω
	Signal Levels	Receive: 0 to -30 dB
		Transmit: 0 dB, -7.5 dB, -15 dB, -22.5 dB, with CSU ±2.7V ±10%, adjustable, measured in range 0 to 655 feet, with DSU
	Jitter Performance	Per AT&T TR-62411, G.824
	Connector	RJ-45
Ethernet Interface	*Compliance*	IEEE 802.3, 802.3u, Ethernet, 802.1p&Q
	Number of Ports	Network: One, UTP or fiber
		User: Up to two, one of which can be fiber optic
	Data Rate	UTP: 10 Mbps or 100 Mbps, full or half-duplex Fiber: 100 Mbps full-duplex
	Specifications and Ranges	See *Table 1-1*

Timing	*Sources*	• Internal • External (E1 or T1, via dedicated connector) • Loopback • Adaptive
Bundles	*Number of TDM Bytes*	48–1440 TDM bytes per Ethernet frame
	Destination IP Address	User-configurable
	Jitter Buffer Size	3–300 msec
Management Terminal	*Interface*	V.24 (RS-232), DCE
	Data Rate	115.2 kbps
	Connector	9-pin, D-type, female
Diagnostics	*Loopbacks*	• E1/T1 local loopback • E1/T1 remote loopback
Statistics	*E1/T1*	As per G.826 and RFC 2495
	Ethernet	As per RFC 2819
	Receive Buffer Indication	Overflow, underflow, sequence error
Alarm Relay	*Dry Contact*	Via pin 6, pin 7 and pin 8 of the EXT CLK connector
Indicators	*General*	PWR (green) – Power
		ALM (red/yellow) – Alarm
		EXT CLK (red/green) – External clock status
	E1	E1 SYNC (red/green) – E1 synchronization
	T1	T1 SYNC (red/green) – T1 synchronization
	Ethernet	LINK/ACT (green) – Link/activity status
Power	*AC/DC Source*	100–240 VAC or -40 to -72 VDC
	Power Consumption	15W max
Physical	*Height*	43.7 mm / 1.7 in
	Width	240 mm / 9.4 in
	Depth	170 mm / 6.7 in
	Weight	0.5 kg / 1.1 lb
Environment	*Temperature*	0 to 50°C/32 to 122°F
	Humidity	Up to 90%, non-condensing

Chapter 2

Installation and Setup

This chapter describes installation and setup procedures for the IPmux-11 unit.

After installing the unit, refer to *Chapter 3* for the operating instructions.

If a problem is encountered, refer to *Chapter 4* for test and diagnostic instructions.

Warning

Internal settings, adjustment, maintenance, and repairs may be performed only by a skilled technician who is aware of the hazards involved.
Always observe standard safety precautions during installation, operation, and maintenance of this product.

2.1 Site Requirements and Prerequisites

AC-powered IPmux-11 units should be installed within 1.5m (5 ft) of an easily-accessible grounded AC outlet capable of furnishing the voltage in accordance with IPmux-11 nominal supply voltage.

DC-powered IPmux-11 units require a -48 VDC power source, which must be adequately isolated from the main supply.

Allow at least 90 cm (36 in) of frontal clearance for operating and maintenance accessibility. Allow at least 10 cm (4 in) clearance at the rear of the unit for signal lines and interface cables.

The ambient operating temperature of IPmux-11 should be 0 to 50°C (32 to 122°F), at a relative humidity of up to 90%, non-condensing.

2.2 Package Contents

The IPmux-11 package includes the following items:

- One IPmux-11 unit
- Technical documentation CD
- Power cord
- CBL-RJ45/2BNC/E1/X adapter cable for unbalanced E1 interface
- RM-33 rack mount kit (if ordered).

2.3 Installation and Setup

The IPmux-11 standalone unit is designed for desktop or bench installation and is delivered as a fully assembled unit. No provisions are made for bolting the unit to a tabletop.

➤ **To install IPmux-11:**

1. Determine the required configuration of IPmux-11, in accordance with your application.
2. Connect the Ethernet ports (see *Connecting the Ethernet Ports* below).
3. Connect the E1 or T1 ports (see *Connecting the E1 or T1 Ports* below).
4. Connect power to the unit (see *Connecting the Power* below).

Connecting the Interfaces

Figure 2-1 illustrates the rear panel of typical IPmux-11 unit with a balanced E1 port. *Appendix A* specifies the IPmux-11 connector pinouts.

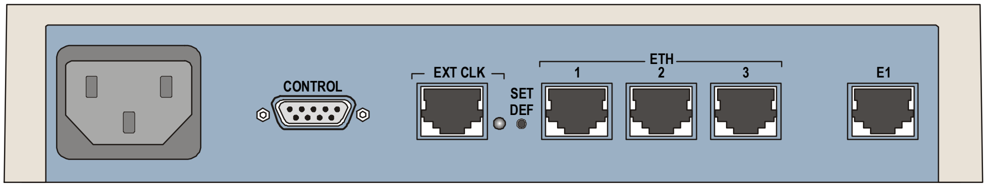


Figure 2-1. IPmux-11 Rear Panel

Connecting the Ethernet Ports

The IPmux-11 user and network interfaces terminate in 8-pin RJ-45 connectors.

➤ **To connect the Ethernet interfaces:**

- Connect the network to the RJ-45 connector designated ETH 1.
- Connect the user LAN(s) to the RJ-45 connector(s) designated ETH 2 or ETH 3.

Connecting the E1 or T1 Ports

The IPmux-11 balanced E1 and T1 interfaces terminate in RJ-45 connector designated **E1** or **T1**. Unbalanced E1 interface in provided via CBL-RJ45/2BNC/E1/X adapter cable (see *Appendix A* for the cable wiring diagram).

Caution When connecting balanced E1 or T1 equipment, make sure to use only 4-wire RJ-45 connectors with the following pins used for receiving and transmitting data: 1, 2, 4, 5. Do not use 8-pin RJ-45 connectors.

➤ **To connect the balanced E1 or T1 interface:**

- Connect the E1 or T1 line to the RJ-45 connector designated E1 or T1.

➤ **To connect the unbalanced E1 interface:**

1. Connect the RJ-45 connector of the adapter cable to the RJ-45 port designated E1.
2. Connect the transmit cable to the red coaxial connector of the adapter cable marked ↑.
3. Connect the receive cable to the green coaxial connector of the adapter cable marked ↓.

Connecting the Power

IPmux-11 is equipped with a dual input AC/DC power supply. AC or DC power is supplied to IPmux-11 via a standard 3-prong power input connector on the rear panel (see *Figure 2-1*).

Warning

Before switching on this unit and connecting or disconnecting any other cable, the protective earth terminals of this unit must be connected to the protective ground conductor of the mains (AC or DC) power cord. If you are using an extension cord (power cable) make sure it is grounded as well.
Any interruption of the protective (grounding) conductor (inside or outside the instrument) or disconnecting of the protective earth terminal can make this unit dangerous. Intentional interruption is prohibited.

Connecting AC Power

AC power should be supplied through the 1.5m (5 ft) standard power cable terminated by a standard 3-prong plug. The cable is provided with the unit.

➤ **To connect AC power:**

1. Connect the power cable to the power connector on the IPmux-11 rear panel.
2. Connect the power cable to the mains outlet.

   The unit turns on automatically upon connection to the mains.

Connecting DC Power

DC power is supplied to IPmux-11 via compatible AC/DC plug for attaching DC power supply lines.

➤ **To connect DC power:**

- Refer to the *DC power supply connection supplement*.

Chapter 3

Operation

This chapter:

- Provides a detailed description of the front panel controls and indicators and their functions
- Explains power-on and power-off procedures
- Provides instructions for using a terminal connected to the IPmux-11 control port
- Describes how to navigate menus
- Illustrates the management menus.

For a detailed explanation of parameters on the menus, see *Appendix D*.

3.1 Front Panel Controls, Connectors, and Indicators

The unit's LEDs are located on the front and rear panels (see *Figure 3-1)*. *Table 3-1* lists the functions of the IPmux-11 LED indicators.

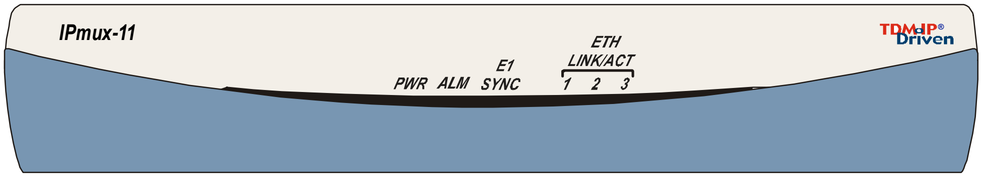


Figure 3-1. IPmux-11 Front Panel

Table 3-1. IPmux-11 LEDs and Controls

Name	Type	Function
PWR	Green LED	ON – Power is ON
ALM	Red/yellow LED	ON (red) – Active alarm is stored in the log file ON (yellow) – Alarm is present in the log file OFF – No alarms are stored in the log file
E1 SYNC	Red/green LED	ON (green) – E1 link is synchronized ON (red) – E1 link has lost synchronization OFF – E1 link is disabled

Table 3-1. IPmux-11 LEDs and Controls (Cont.)

Name	Type	Function
T1 SYNC	Red/green LED	ON (green) – T1 link is synchronized ON (red) – T1 link has lost synchronization OFF – T1 link is disabled
ETH LINK/ACT 1	Green LED	ON – Network Ethernet link is OK Blinks – Data is being transmitted and received on the network Ethernet link
ETH LINK/ACT 2	Green LED	ON – User Ethernet link 1 is OK Blinks – Data is being transmitted and received on the user Ethernet link 1
ETH LINK/ACT 3	Green LED	ON – User Ethernet link 2 is OK Blinks – Data is being transmitted and received on the user Ethernet link 2
EXT CLK	Red/green LED	ON (green) – IPmux-14 is configured to external clock and valid clock input is detected ON (red) – IPmux-14 is configured to external clock and no valid clock input is detected OFF – IPmux-14 is not configured to external clock or the unit is off
SET DEF	Button	Restores default values

3.2 Operating Instructions

Turning IPmux-11 On

➤ **To turn on IPmux-11:**

- Connect the power cord to the mains.

  The PWR indicator lights up and remains lit as long as IPmux-11 receives power.

IPmux-11 requires no operator attention once installed, with the exception of occasional monitoring of front panel indicators. Intervention is only required when IPmux-11 must be configured to its operational requirements, or diagnostic tests are performed.

Turning IPmux-11 Off

➤ **To power off the unit:**

- Remove the power cord from the power source.

3.3 Getting Started

After installation, there are no special operating procedures for IPmux-11. Once it is powered up, the unit operates automatically. The unit operational status can be monitored constantly.

If required, IPmux-11 can be reconfigured. Both the IPmux-11 configuration and monitoring operations are performed locally from an ASCII terminal connected to the control port or from a PC running a Web browser. Detailed configuration procedures are given in *Overview of Menu Operations* and *Appendix D*.

The following functions are supported by the IPmux-11 management software*:*

- Viewing system information
- Modifying configuration and mode of operation, including setting system default values
- Monitoring IPmux-11 performance
- Initiating diagnostic tests
- Upgrading software.

Starting Terminal Control Session

➤ **To start a terminal control session:**

1. Make sure all IPmux-11 cables and connectors are properly connected.
2. Connect IPmux-11 to a PC equipped with an ASCII terminal emulation application (for example, Windows Hyper Terminal or Procomm).
3. Turn on the control terminal PC and set its port parameters to 115.2 kbps, 8 bits/character, 1 stop bit, no parity. Set the terminal emulator to ANSI VT100 emulation (for optimal view of system menus).
4. When the initialization and self-test are over, a menu appears displaying initialization and self-test results. If problems are encountered, refer to *Chapter 4* for instructions.

Login

➤ **To enter as a superuser:**

1. Enter **su** for user name.
2. Enter **1234** for password.

This allows you to configure all the parameters of IPmux-11, and to change the *su* and *user* passwords.

➤ **To view the unit's configuration:**

1. Enter **user** for user name.
2. Enter **1234** for password.

This does not allow you to make configuration changes.

Note *If the password is invalid in three consecutive attempts, the system becomes inaccessible for 15 minutes.*

Choosing Options

➤ **To choose an option:**

- Type the number corresponding to the option, and press **<Enter>**.

  IPmux-11 immediately displays a new value or new menu for the selected option.

Note *When a menu option has only two values, typing the option number and pressing **<Enter>** will toggle between the available values.*

Saving Changes

➤ **To save changes in the configuration:**

- Type **S** to save the changes that were made to the IPmux-11 configuration.

Managing IPmux-11 via Web Browser

Web Browser Requirements

The following Web browsers can be used to access the IPmux-11 supervision utility from any location that enables access to the IPmux-11 using Internet protocols.

- Internet Explorer 6.0, running on Windows™ 98, Windows™ 2000, Windows™ XP
- Netscape Communicator 7.1, running on Windows™ NT or Unix.

Login

➤ **To login via Web browser:**

1. Connect one of the Ethernet ports of IPmux-11 to the LAN.
2. Open the Web browser.
3. Enter the IP address of the IPmux-11 in the address field of the browser in the following format: **http://'IP address'** and then press **<Enter>** to command the browser to connect (**'IP address'** stands for the actual IPmux-11 IP address which has to be assigned via an ASCII terminal).
4. After the opening window is displayed, click **LOGIN**.
5. Enter your user name and password.

   The Main menu is displayed.

Navigating the ConfiguRAD Menus

ConfiguRAD is a Web-based remote access terminal management software. It provides a user-friendly interface for configuring, collecting statistics and performing diagnostic tests on the IPmux-11 units.

➤ **To choose an option:**

1. Click a link in the ConfiguRAD screen to display the next menu.
2. Once the target screen is displayed, select a value from the drop-down box or enter it in a text box.

3.4 Overview of Menu Operations

Use these menu trees as a reference aid while performing configuration and control functions. *Appendix D* illustrates menus and explains parameters. *Table 3-2* lists default values.

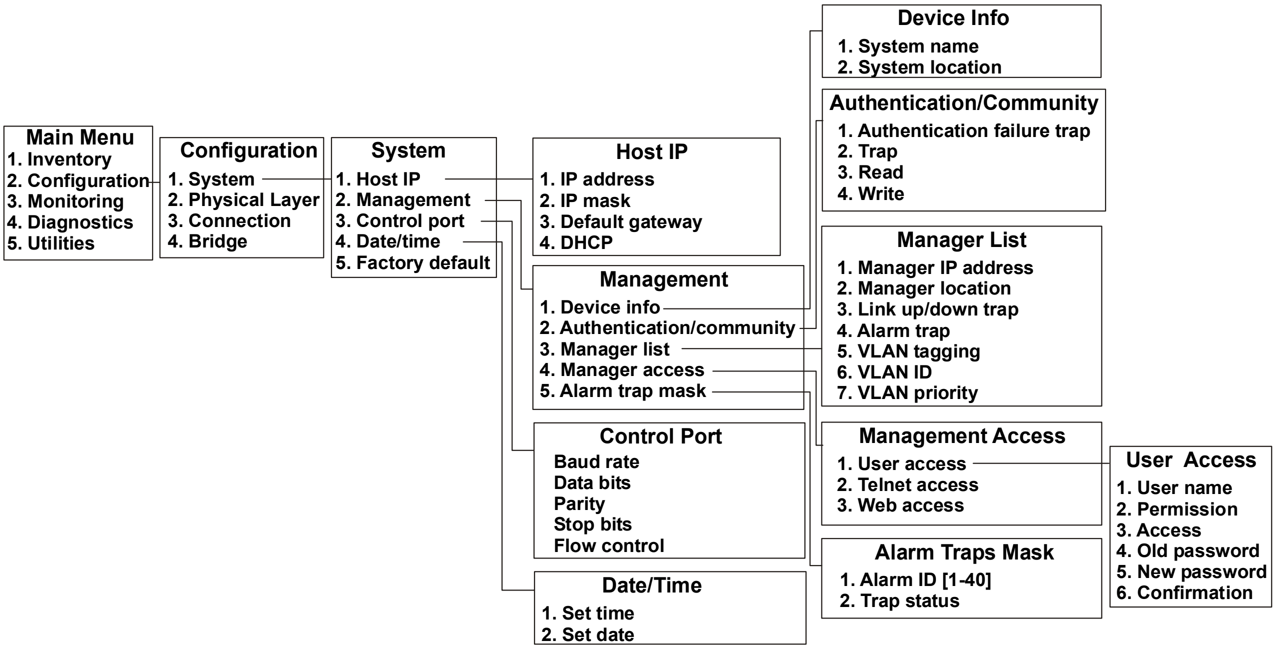


Figure 3-2. Main Menu > Configuration > System

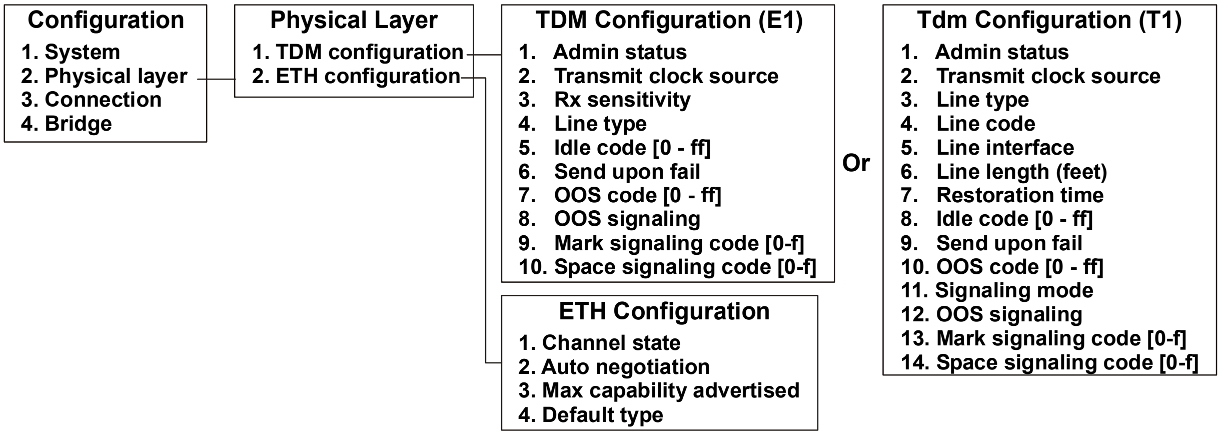


Figure 3-3. Configuration > Physical Layer > TDM and ETH Configuration

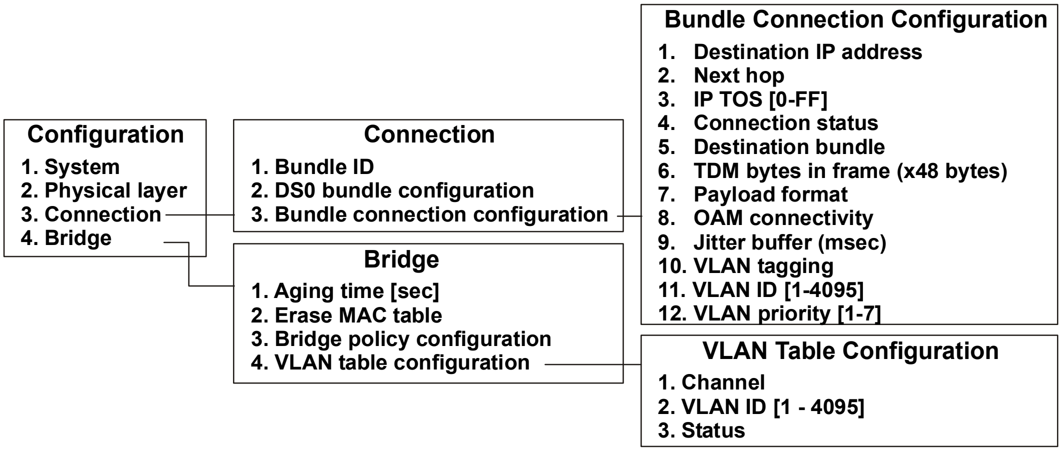


Figure 3-4. Configuration > Connection and Bridge

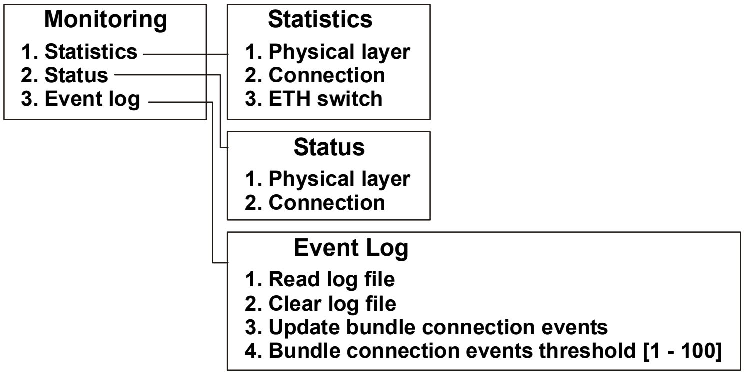


Figure 3-5. Monitoring

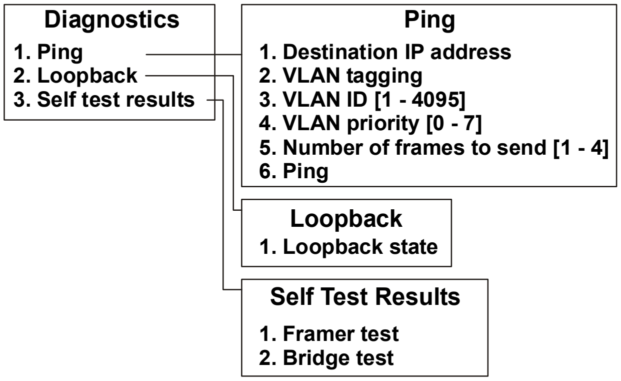


Figure 3-6. Diagnostics

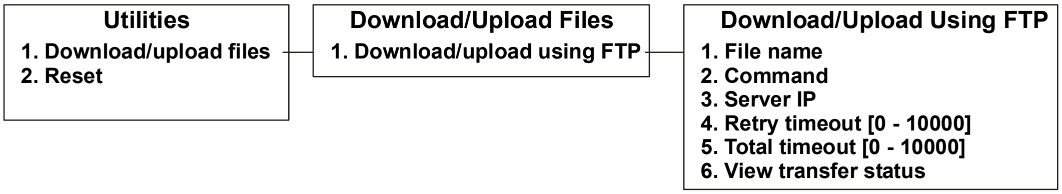


Figure 3-7. Utilities

3.5 Default Settings

Table 3-2 lists the default settings of the IPmux-11 configuration parameters.

Table 3-2. Default Settings

Parameter	Default Value
System	
IP address	Empty
IP mask	Empty
Default gateway	0.0.0.0
DHCP	Disable
Authentication failure trap	Disable
Trap	SNMP_trap
Read	public
Write	private
Manager IP address	0.0.0.0
Manager location	Empty
Link up/down trap	Empty
Alarm trap	Empty
VLAN tagging	Empty
VLAN ID	Empty
VLAN priority	Empty
User name	su
Permission	Full control
Access	All
Telnet access	Enable
Web access	Enable
Alarm ID	–
Trap status	Active
Baud rate (bps)	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Table 3-2. Default Settings (Cont.)

Parameter	Default Value
Physical Layer (TDM, E1)	
Admin status	Enable
Transmit clock source	Adaptive
Loopback state	Disable
Rx sensitivity	Short haul
Line type	Framed G.704
Idle code	7E
Send upon fail	OOS code
OOS code	FF
OOS signaling	Space
Mark signaling code	D
Space signaling code	1
Physical Layer (TDM, T1)	
Admin status	Enable
Transmit clock source	Adaptive
Line type	ESF
Line code	B8ZS
Line interface	DSU
Line length	0–133
Restoration time	TR-6211 (10 seconds)
Idle code	7E
Send upon fail	OOS code
OOS code	FF
Signaling mode	None
OOS signaling	Space
Mark signaling code	D
Space signaling code	1
Physical Layer (ETH)	
Channel state	Enable
Auto negotiation	• Disable for fiber optic interface • Enable for copper interface
Max capability advertised	100baseT full duplex
Default type	10baseT half duplex

Table 3-2. Default Settings (Cont.)

Parameter	Default Value
Connection	
Connection mode	Static
Destination IP address	0.0.0.0
Next hop	0.0.0.0
IP TOS	0
Connection status	Enable
Destination bundle	–
TDM bytes in frame	1
Payload format	Old format
OAM connectivity	Disable
Jitter buffer	3
VLAN tagging	Disable
Bridge	
Aging time	304
VLAN ID	–
Status	Enable

Chapter 4

Diagnostics and Troubleshooting

This chapter describes how to:

- Detect errors
- Display statistics
- Troubleshoot problems
- Perform diagnostic tests.

4.1 Error Detection

Power-Up Self-Test

IPmux-11 performs hardware self-test upon turn-on. The self-test sequence checks the critical circuit functions of IPmux-11 (framer and bridge). The self-test results are displayed via the Diagnostics menu.

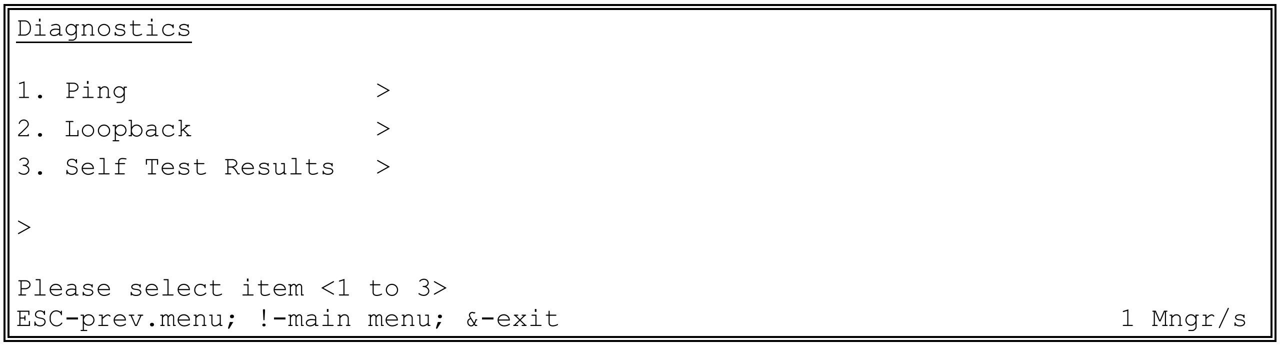
➤ **To display the self-test results:**

1. From the Main menu, select **Diagnostics**.

   The Diagnostics menu appears (see *Figure 4-1*).

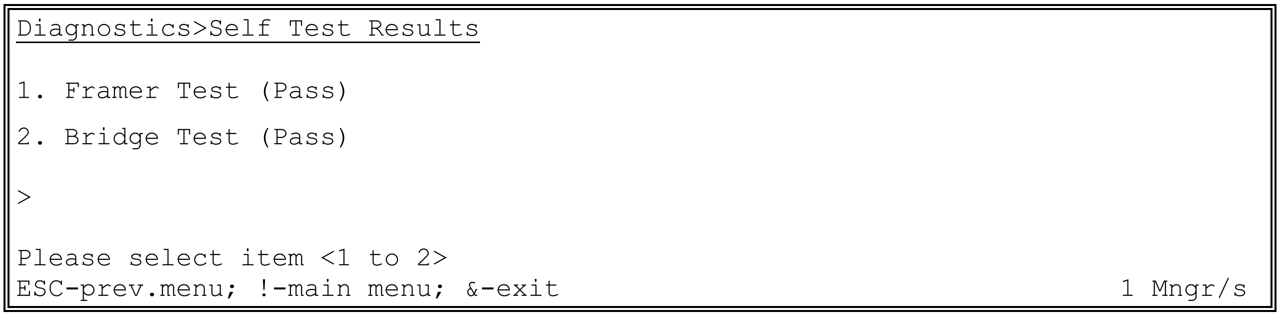
2. From the Diagnostics menu, select **Self Test Results**.

   The Self Test Results screen appears (see *Figure 4-2*).



```
Diagnostics

1. Ping                >
2. Loopback            >
3. Self Test Results   >

>

Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure 4-1. Diagnostics Menu



```
Diagnostics>Self Test Results

1. Framer Test (Pass)

2. Bridge Test (Pass)

>

Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                          1 Mngr/s
```

Figure 4-2. Self Test Results Screen

Using Front Panel LEDs

LED indicators on the front panel IPmux-11 indicate the operating status of the module. The LED indicators are described in *Chapter 3* of this manual.

Working with the Alarm Buffer

IPmux-11 maintains an Event Log file, which can hold up to 2048 events. All events are time-stamped.

Displaying Events

➤ **To access the event log:**

1. From the Main menu, select Monitoring.

   The Monitoring menu is displayed (see *Figure 4-3*).

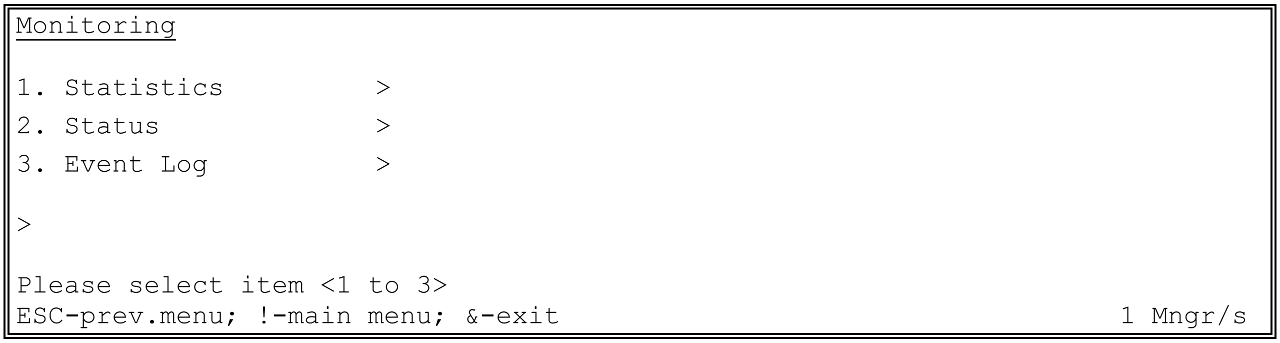
2. From the Monitoring menu, select **Event Log**.

   The Event Log menu is displayed (see *Figure 4-4*).

3. From the Event Log menu, select **Read log file**.

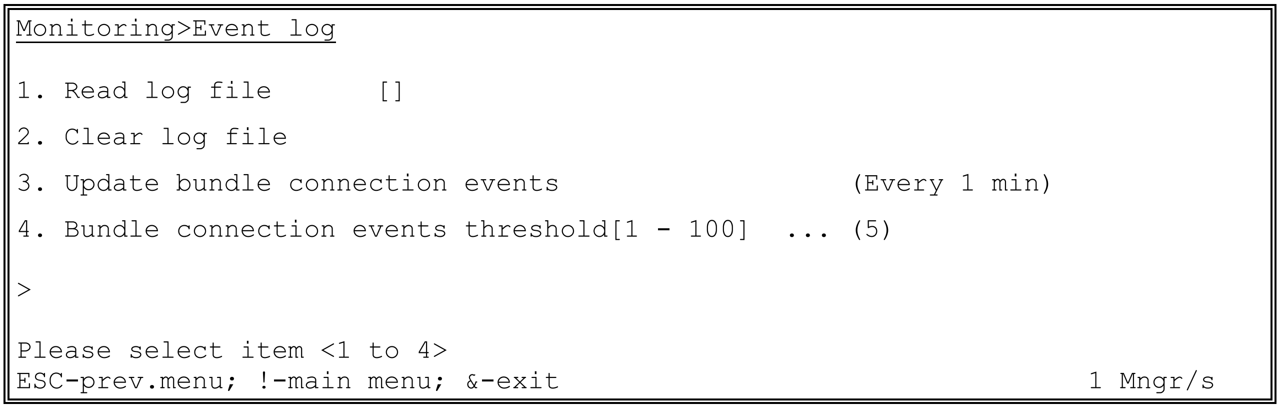
   The Read Log File screen appears (see *Figure 4-5*).

4. In the Read Log File screen, use the **<Ctrl>** + **<U>** and **<Ctrl>** + **<D>** key combinations to scroll the alarm list up and down.



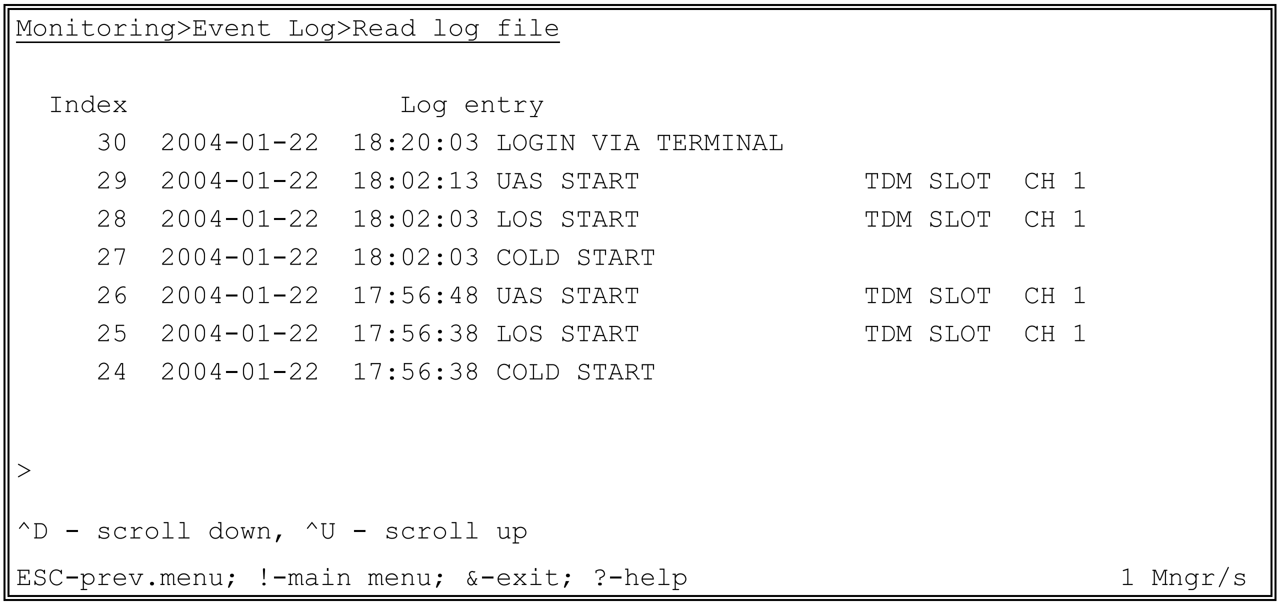
```
Monitoring

1. Statistics          >
2. Status              >
3. Event Log           >

>

Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                          1 Mngr/s
```

Figure 4-3. Monitoring Menu



```
Monitoring>Event log

1. Read log file       []

2. Clear log file

3. Update bundle connection events                  (Every 1 min)

4. Bundle connection events threshold[1 - 100]  ... (5)

>

Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                              1 Mngr/s
```

Figure 4-4. Event Log Menu



```
Monitoring>Event Log>Read log file


  Index                Log entry
     30  2004-01-22  18:20:03 LOGIN VIA TERMINAL
     29  2004-01-22  18:02:13 UAS START              TDM SLOT  CH 1
     28  2004-01-22  18:02:03 LOS START              TDM SLOT  CH 1
     27  2004-01-22  18:02:03 COLD START
     26  2004-01-22  17:56:48 UAS START              TDM SLOT  CH 1
     25  2004-01-22  17:56:38 LOS START              TDM SLOT  CH 1
     24  2004-01-22  17:56:38 COLD START


>

^D - scroll down, ^U - scroll up

ESC-prev.menu; !-main menu; &-exit; ?-help                        1 Mngr/s
```

Figure 4-5. Read Log File

Clearing Events

➤ **To clear the event log:**

1. From the Event Log menu, select Clear log file.

   IPmux-11 displays the following message:
   Logfile will be cleared. Continue ??? (Y/N)

2. Type **Y** to confirm the log file clearing.

Table 4-1 presents the event types that appear in the event log alphabetically, as well as the actions required to correct the event (alarm) indication.

To correct the reported problem, perform corrective actions in the given order until the problem is corrected. If the problem cannot be fixed by carrying out the listed actions, IPmux-11 must be checked by the authorized technical support personnel.

Table 4-1. Event List

Event	Description	Corrective Action
COLD START	IPmux-11 has been powered up	None
CON LOCAL FAIL	Ethernet frames are not received by the local IPmux-1 on the specified connection	Check Eth/IP path
CON REMOTE FAIL	Ethernet frames are not received by the remote IPmux-11 on the specified connection	Check Eth/IP path
CON STANDBY	Redundancy bundle connection is not the active connection (only applies when redundancy is used)	None
CON TDM FAIL	LOS/LOF on the TDM line forced redundancy switching (only applies when redundancy is used)	Check the TDM line
CON SYNC	Bundle connection failure has ended (only applicable when OAM is Enabled)	None
CON UNAVAILABLE	Remote IPmux is not available (only applicable when OAM is Enabled)	Check the connection of the remote IPmux
CON VALIDATION FAIL	Connection is invalid (only applicable when OAM is Enabled)	Check the bundle parameters
FATAL ERROR	IPmux-11 has encountered an internal fatal error	The IPmux-11 requires servicing
INVALID LOGIN VIA TERMINAL	Invalid user name or password was entered, when attempting to access IPmux-11 via local terminal	None
INVALID LOGIN VIA WEB	Invalid user name or password was entered, when attempting to access IPmux-11 via Web browser	None
INVALID LOGIN VIA TELNET	Invalid user name or password was entered, when attempting to access IPmux-11 via Telnet	None
IP ADDRESS IS ASSIGNED BY SERVER	Host IP has been learned by the DHCP protocol	None
IP ADDRESS IS RELEASED	Host IP has been relesased by the DHCP protocol	Check the connection with the DHCP server
JIT BUF OFLOWS END BUNDLE 1	Jitter Buffer Overflows END (see *Configuring the Bundle Statistic Collection* below)	–
JIT BUF OFLOWS START BUNDLE 1	Jitter Buffer Overflows START (see *Configuring the Bundle Statistic Collection* below)	Increase jitter buffer size
JIT BUF UFLOWS END BUNDLE 1	Jitter Buffer Underflows END (see *Configuring the Bundle Statistic Collection* below)	–
JIT BUF UFLOWS START BUNDLE 1	Jitter Buffer Underflows START (see *Configuring the Bundle Statistic Collection* below)	Increase jitter buffer size

Table 4-1. Event List (Cont.)

Event	Description	Corrective Action
LINE AIS END	Line AIS state detected has ended	None
LINE AIS START	IPmux-11 has AIS (alarm indicator signal) state on its E1/T1 port	Check for a fault at the PDH network, on the receive direction
LINE FEBE END	LINE FEBE state detected has ended	None
LINE FEBE START	IPmux-11 has LINE FEBE state on its E1/T1 port	Check for errors in the E1/T1 connection on the transmit direction
LINE RAI END	LINE RAI state detected has ended	None
LINE RAI START	IPmux-11 has LINE RAI (remote alarm indication) state on its E1/T1 port	Check for a fault at the E1/T1 connectivity on the transmit direction
LOGIN VIA TERMINAL	The unit was accessed via local terminal	None
LOGIN VIA WEB	The unit was accessed via Web browser	None
LOGIN VIA TELNET	The unit was accessed via Telnet	None
LOF START	IPmux-11 has a LOF (loss of frame) state on its E1/T1 port	1. Check the E1/T1 cable connection 2. Check all framing-related parameters for E1/T1 interface
LOF END	LOF state detected has ended	None
LOS END	LOS state detected has ended	None
LOS START	IPmux-11 has a LOS (loss of signal) state on its E1/T1 port	1. Check the E1/T1 cable connection 2. Check input signal
PS ACTIVE	IPmux-11 power supply unit is powered on	None
SN ERRORS END BUNDLE 1	Sequence Number ERRORS END (see *Configuring the Bundle Statistic Collection* below)	–
SN ERRORS START BUNDLE 1	Sequence Number ERRORS START (see *Configuring the Bundle Statistic Collection* below)	• Check the Ethernet/IP network • Increase jitter buffer size
SYSTEM USER RESET	The user initiated software reset via the system menu	None
UAS START	Ten consecutive severely errored seconds were detected	• Check physical interface connections.
UAS END	Ten consecutive seconds without SES were detected	

Configuring the Bundle Statistic Collection

You can set the interval for the bundle statistics collection, as well the statistics threshold.

➤ **To configure the bundle statistic collection:**

- From the Event Log menu (*Figure 4-4*), configure the following:
  - Update bundle connection events: **1 sec**, **1 min**
  - Bundle connection events threshold (a number of events that cause the alarm to be initiated): **1–100**.

4.2 Performance Monitoring Statistics

IPmux-11 provides powerful performance monitoring tools, which consist of the following three levels:

- E1/T1 statistics – Status of the physical E1/T1 parameters (signal, framing, etc.)
- LAN statistics – Ethernet connection status (speed, duplex mode, bytes transmitted & received, etc.)
- Bundle connection statistics – TDMoIP bundle connection status on the Ethernet/IP network level.

E1/T1 Statistics

E1/T1 statistics refer to the physical status of the E1/T1 traffic reaching IPmux-11 from the adjacent E1/T1 device.

The E1 statistics parameters comply with the G.703, G.704, G.804, G706, G732, and G.823 standards.

The T1 statistics parameters comply with the ANSI T.403, AT&T R62411, G.703, G.704 and G.804 standards.

➤ **To view the E1/T1 statistics:**

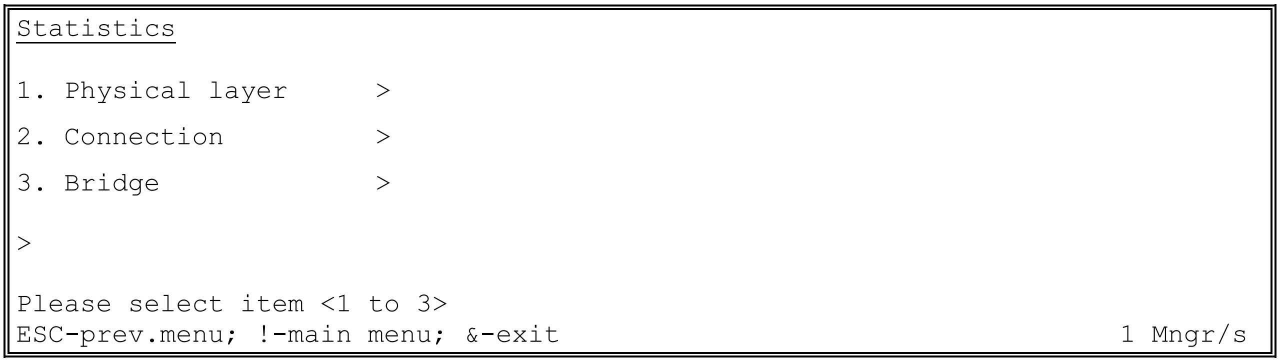
1. From the Monitoring menu (*Figure 4-3*), select **Statistics**.

   The Statistics menu appears (*Figure 4-6*).

2. From the Statistics menu, select **Physical Layer**.
3. The Physical Layer (E1) or Physical Layer (T1) screen appears (see *Figure 4-7*).

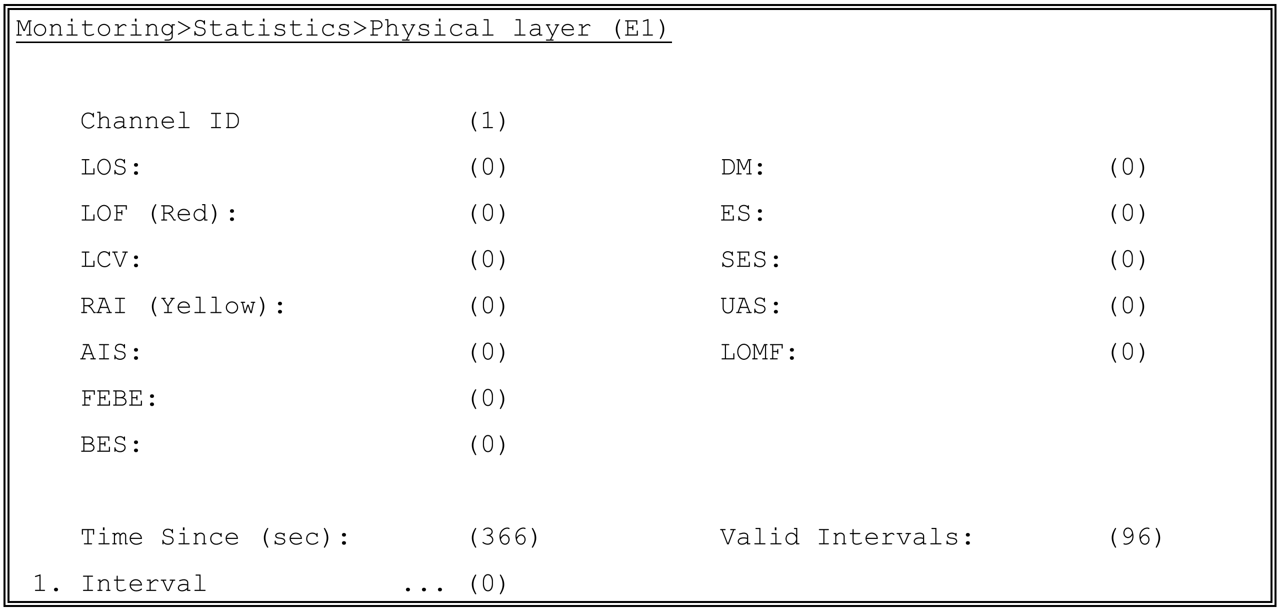
   E1/T1 statistics are monitored and saved under consecutive intervals. Each interval is 15 minutes long. There are 96 intervals, which represent the last 24 hours. Whenever a new interval is started, the counters are reset to zero. The old interval shows the total of events that occurred during its 15-min. period. The current active interval is always marked as interval 0 (you will see that the **Time Since** counter is running). The previous interval is marked as 1 and so on. The E1/T1 statistic counters cannot be reset manually.

4. From the Physical Layer (E1/T1) screen, type **1.**
5. To display statistics for a specific interval, enter its number.



```
Statistics

1. Physical layer      >

2. Connection          >

3. Bridge              >

>

Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                                     1 Mngr/s
```

Figure 4-6. Statistics Menu



```
Monitoring>Statistics>Physical layer (E1)


    Channel ID                (1)
    LOS:                      (0)              DM:                      (0)
    LOF (Red):                (0)              ES:                      (0)
    LCV:                      (0)              SES:                     (0)
    RAI (Yellow):             (0)              UAS:                     (0)
    AIS:                      (0)              LOMF:                    (0)
    FEBE:                     (0)
    BES:                      (0)


    Time Since (sec):         (366)            Valid Intervals:         (96)
 1. Interval              ... (0)
```

Figure 4-7. E1/T1 Statistics

Table 4-2 describes the E1/T1 statistics.

Table 4-2. E1/T1 Statistics

Alarm	Description
LOS	A Loss of Signal indicates that there is either no signal arriving from the adjacent E1/T1 device or no valid E1 voltage mask or no voltage alteration between positive and negative amplitudes. For E1 links, the LOS counter will increase by one for each second during which a consecutive 255 pulses have no pulse of negative or positive polarity. For T1 links, the LOS counter will increase by one for each second during which a consecutive 192 pulses have no pulse of negative or positive polarity. A LOS alarm is also indicated by the front panel E1/T1 SYNC LED (red). The green E1/T1 SYNC LED indicates that the E1/T1 synchronization has been restored). Recommendations: Check the physical layer (connectors, cables, etc.)
LOF (Red)	A Loss of Frame indicates that the IPmux-11 lost E1/T1 synch opposite its adjacent E1/T1 device. In more detail, this is a period of 2.5 seconds for T1 or 100 msec for E1, during which an OOF (Out Of Frame) error persisted and no AIS errors were detected. For E1 links an OOF defect is declared when three consecutive frame alignment signals have been received with an error. For T1 links, an OOF defect is declared when the receiver detects two or more framing errors within a three msec period for ESF signals and 0.75 msec for D4 signals, or two or more errors out of five or fewer consecutive framing-bits. A LOF alarm is also indicated by the front panel E1/T1 SYNC LED (red). When the IPmux enters a red alarm condition, it sends an Yf bit (yellow alarm or RAI) towards the adjacent E1/T1 device. Recommendations: Check all framing related parameters for E1/T1, and physical connections.

Table 4-2. E1/T1 Statistics (Cont.)

Alarm	Description
LCV	A Line Code Violation indicates an error on the pulse structure, either a **Bipolar Violation (BPV)** or an **Excessive Zeros (EXZ) error event**. BPV is the occurrence of a pulse with the same polarity as the previous pulse. EXZ is the occurrence of a zero string greater than 15 for AMI or 7 for B8ZS. For an E1 link, the LCV counter will increase by one, for each second during which a BPV or EXZ errors have occurred. For T1 links, the LCV counter will increase for each second during which two consecutive BPVs of the same polarity are received. Complies with ITU-TI.431, 0.161, G775 and G.821 standards. Recommendations: Check physical link for bad/loose connection, impedance matching (balanced or unbalanced) and noisy environment.
RAI (Yellow)	A Remote Alarm Indicator is sent by a device when it enters RED state (looses synch). **RAI Alarm** indicates that the adjacent E1/T1 device had lost E1/T1 synch and hence sent an RAI towards the IPmux, which entered a Yellow alarm mode (similarly, IPmux sends RAI towards adjacent E1/T1 when IPmux enters LOF state (Red alarm). In both E1/T1 links the RAI counter increases by one for each second during which an RAI pattern is received from the far end framer. The RAI alarm is also indicated by the front panel ALM LED (red). Recommendations: Check reason for E1/T1 device to be in LOF (out of synch state) by checking physical link integrity at the Tx direction of the IPmux towards E1/T1 device and framing related parameters.
AIS	An Alarm Indication Signal implies an upstream failure of the adjacent E1/T1 device. AIS will be sent to the opposite direction of which the Yellow alarm is sent. For E1 links, the AIS counter will increase by one for each second during which a string of 512 bits contains fewer than three zero (0) bits. For T1 links, the AIS counter will increase by one for each second during which an unframed “all 1” signal is received for 3 msec. The AIS condition is indicated by the front panel E1/T1 SYNC LED (red).. Recommendations: Check why the E1/T1 device is sending AIS (all ones) stream towards IPmux, for example, Red alarm on a different interface of E1/T1 device (upstream).
FEBE	A Far End Block Error is sent to transmitting device notifying that a flawed block has been detected at the receiving device. Exists only for E1 MF-CRC4. The FEBE alarm is also indicated by the front panel ALM LED (red). The FEBE counter will increase by one for each second during which the FEBE indication is received. Recommendation: Check physical link integrity.

Table 4-2. E1/T1 Statistics (Cont.)

Alarm	Description
BES	A Bursty Errored Seconds (also known as Errored second type B) is a second during which fewer than 319 and more than one CRC errors occurred with neither AIS nor SEF (Severely Errored Frame) detected. The BES counter will increase by one for each second containing the condition described above. The CRC is calculated for the previous frame in order to prevent processing delay. Complies with AT&T TR-62411 and TR-54016 standards. Not applicable if the line type is set to Unframed. Available only at T1-ESF or E1-CRC4 modes (performance monitoring functionality). Recommendations: Check physical link integrity, G.704 frame format integrity and Sync. (The CRC bits are included in TS0 for E1 multiframe links and in the frame alignment bits for T1 ESF links).
DM	A Degraded Minute is calculated by collecting all the available seconds, subtracting any SES and sorting the result in 60-second groups. The DM counter will increase by one for each 60-second group in which the cumulative errors during the 60-second interval exceed 1E-6. Available in T1-ESF or E1-CRC4 modes only, (performance monitoring functionality). Recommendations: See BES recommendations.
ES	An Errored Second is a second containing one or more of the following: • CRC error • SEF (OOF) • AIS (T1 only) • If SES is active ES runs for 10 seconds and then stops. Recommendations: Check physical link integrity. Follow the recommendation concerning LOF, BEF and AIS.
SES	A Severely Errored Second is a second containing one of the following: • 320 or more CRC errors events • One or more OOF defect • One or more AIS events occurred (T1 only) • The SES counter will be cleared after reaching 10 and an UAS will then be activated. Recommendations: Check physical link integrity. See also ES alarm recommendation.
UAS	Unavailable Second parameter refers to the number of seconds during which the interface is unavailable. The UAS counter will start increasing after 10 consecutive SES occurrences and will be deactivated as a result of 10 consecutive seconds without SES. After SES clearance the UAS counter will then diminish 10 seconds from the overall count. Recommendations: See above recommendations.
LOMF	A Loss of Multi Frame indicates there is no sync on the multi frame mode, i.e., the receiving device is unable to detect the four ABCD bits pattern on. The LOMF alarm is also indicated by the front panel ALM LED (red). TS16 MSB in frame 0 for two consecutive multi frames. Available only for E1 Multi-Frame mode (CAS). Recommendations: Check physical link integrity, signaling method (CAS enable only), and framing-related parameters.

LAN Statistics

You can display statistic data for the network and user Ethernet ports.

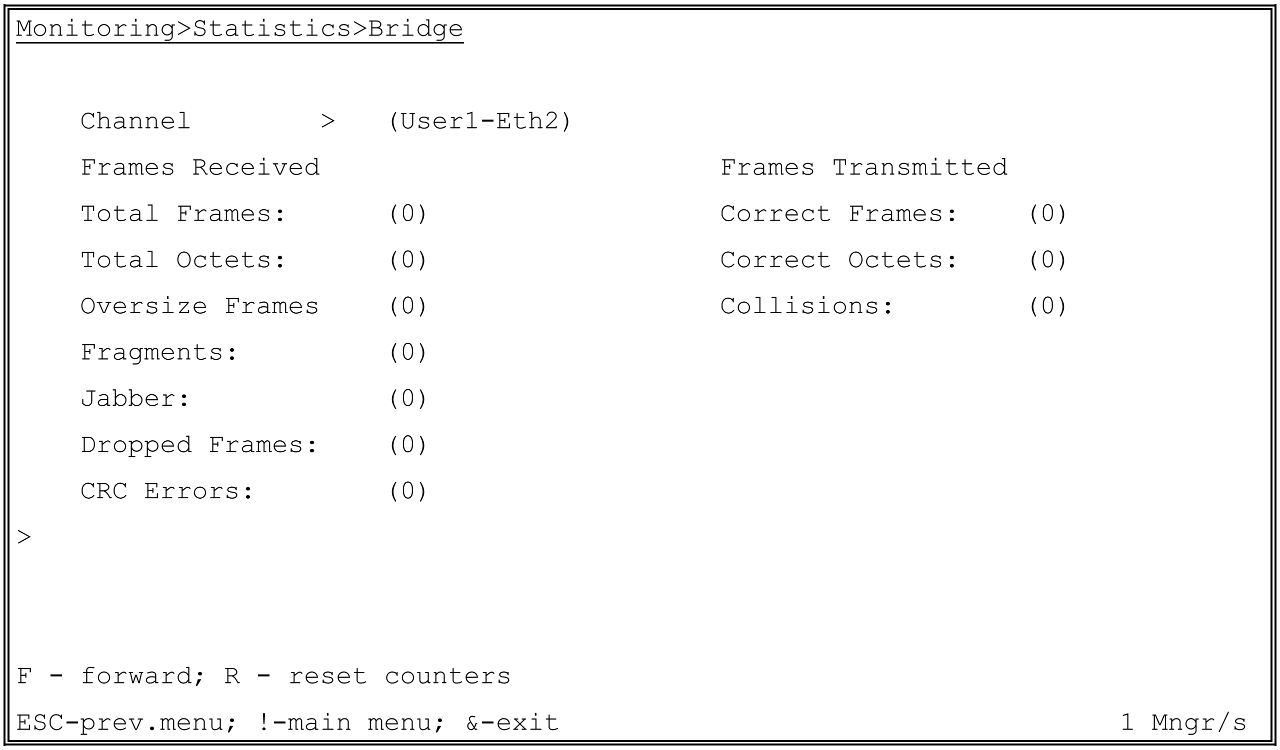
➤ **To view the LAN statistics:**

1. From the Statistics menu, select **Bridge**.

   The Bridge screen appears (see *Figure 4-8*).

2. From the Bridge screen, type **F** to toggle between network and user interfaces. *Table 4-3* describes the LAN statistics data.

3. Type **R** to reset the counters.



```
Monitoring>Statistics>Bridge


    Channel         >  (User1-Eth2)

    Frames Received                         Frames Transmitted

    Total Frames:      (0)                  Correct Frames:    (0)

    Total Octets:      (0)                  Correct Octets:    (0)

    Oversize Frames    (0)                  Collisions:        (0)

    Fragments:         (0)

    Jabber:            (0)

    Dropped Frames:    (0)

    CRC Errors:        (0)

>




F - forward; R - reset counters

ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure 4-8. LAN Statistics

Table 4-3. LAN Statistics Parameters

Parameter	Description
Frames Received	
Total Frames	The total number of correct frames received. When a valid connection is established the number should increase steadily.
Total Octets	The total number of octets (bytes) received. When a valid connection is established the number should increase steadily.
Oversize Frames	Number of frames exceeding the maximum allowed frame size, but are otherwise valid Ethernet frames (good CRC).
Fragments	The number of frames that are shorter than 64 bytes and have an invalid CRC.

Table 4-3. LAN Statistics Parameters (Cont.)

Parameter	Description
Jabber	The number of frames that are too long and have an invalid CRC. A jabber is transmission by a data station beyond the time interval allowed by the protocol, usually affecting the rest of the network. In an Ethernet network, devices compete for use of the line, attempting to send a signal and then retrying in the event that someone else tried at the same time. A jabber can look like a device that is always sending, effectively bringing the network to a halt. Recommendations Check network interface card or any other transmitting devices and external electrical interference.
Dropped Frames	Number of dropped frames due to delivery problems. Recommendations: Check the network interface card.
CRC Errors	The amount of frames with invalid CRCs.
Frames Transmitted	
Correct Frames	The number of frames successfully transmitted. When a valid connection is established the number should increase steadily.
Correct Octets	The number of octets successfully transmitted. When a valid connection is established the number should increase steadily.
Collisions	The number of successfully transmitted frames which transmission is inhibited by a collision event. A collision occurs in half-duplex connection when two devices try to transmit at the same time. This counter tracks the number of times frames have collided. This event exists only in Half Duplex mode, which is not recommended in an IPmux-11 application. Recommendations: Many collisions indicate that the traffic is too heavy for a half-duplex media. Set to a Full-Duplex environment if possible.

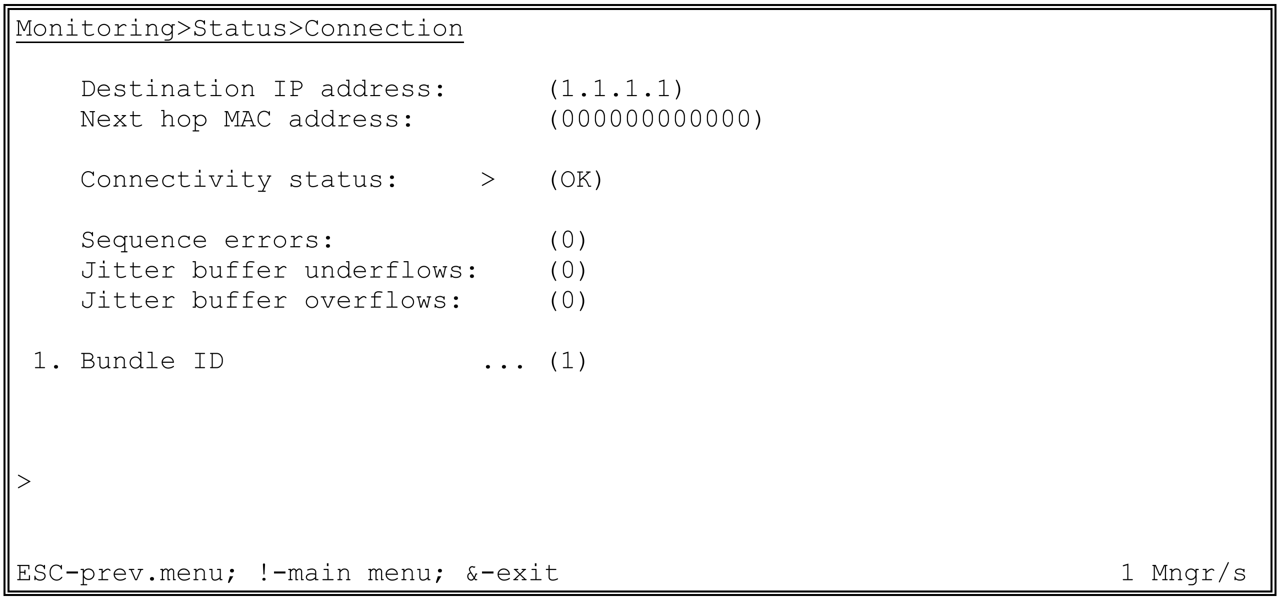
Bundle Connection Statistics

The Connection screen provides information about the integrity of the TDMoIP connection, including the status of the jitter buffer. (Each bundle has it own independent jitter buffer).

➤ **To display the bundle connection information:**

- From the From the Status menu, select **Connection.**

  The Connection screen is displayed (see *Figure 4-9*).



```
Monitoring>Status>Connection

    Destination IP address:       (1.1.1.1)
    Next hop MAC address:         (000000000000)

    Connectivity status:     >    (OK)

    Sequence errors:              (0)
    Jitter buffer underflows:     (0)
    Jitter buffer overflows:      (0)

 1. Bundle ID                ...  (1)



>


ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure 4-9. Connection Screen

Table 4-4 lists the bundle connection parameters.

Table 4-4. Bundle Connection Parameters

Parameter	Description
Destination IP Address	The IP address of the opposite IPmux, to which the bundle is destined.
Next Hop MAC Address	Layer 2 Applications: the MAC address displayed is the MAC address of the remote IPmux-11. Layer 3 Applications: the MAC address displayed is the MAC address of the connected router.
Connectivity Status	Disabled: No activity in the channel. The channel is disabled. OK: Both the remote and the local IPmux receive Ethernet frames, (however, there may be problems such as sequence errors, underflows, overflows, as explained below). Local Fail: The local IPmux-11 does not receive Ethernet frames. Remote Fail: The remote IPmux-11 does not receive Ethernet frames. Unavailable: The remote IPmux-11 does not reply to OAM messages (only applicable when OAM is enabled). Validation Fail: The remote IPmux-11 replies, but there is a configuration error (only applicable when OAM is enabled). Standby: Redundant bundle is OK and wiaitng for redundancy switching (only applicable when Redundancy is enabled). TDM Fail: There is LOS/LOF at the TDM side (only applicable when Redundancy is enabled). ***Note****: While under Disable or Local Failure or Remote Failure status, the statistic counters will be inactive.*

Table 4-4. Bundle Connection Parameters (Cont.)

Parameter	Description
Sequence Errors	Each packet transmitted by IPmux-11 holds a sequence number. The receiving IPmux-11 checks these numbers at the receive mechanism and expects to see that each new incoming packet is "in sequence" relative to the previous one (i.e., packet no. 5 is received after no. 4). When, for some reason, this is not the case (i.e., next packet is not in sequence relative to the previous one), this means that there had been a problem with packet flow integrity (and hence data/voice integrity). IPmux will indicate this by increasing the "Sequence Errors" counter by one. There may be two reasons for a Sequence Error notification: Packet or packets are lost somewhere along the network. Re-ordering of packets by network. Packet re-ordering may occur due to queuing mechanisms, re-routing by the network, or when the router updates very large routing tables. Recommendations: • Make sure IPmux-11 traffic has sufficient bandwidth. See *Chapter 1* for throughput calculation. • Make sure Ethernet connection is functioning properly. (See *LAN Statistics* above.) • Make sure Ethernet/IP network provides priority (Quality Of Service) to the IPmux traffic. Priority may be achieved by three means: VLAN tagging, IP TOS marking or by using the constant 2142 decimal value at the "UDP destination Port" field of each TDMoIP packet. • Verify that the IP network devices (switches/routers/modems/etc.) are capable of handling the IPmux PPS rate (Packets Per Second). For PPS calculations refer to *Chapter 1*. • Make sure the network devices do not drop/loose/ignore packets. ***Note**: IPmux-11 may support a "reordering mechanism", which can sort packets back to their original order in some situations.*
Jitter Buffer Underflows	IPmux-11 is equipped with a "Packet Delay Variation Tolerance" buffer, also called a "jitter buffer", responsible for compensating for IP networks delay variation (IP jitter). The jitter buffer is configured in milliseconds units and exists for each bundle independently. Explanation: Packets leave the transmitting IPmux-11 at a constant rate, but the problem is that they are reaching the opposite IPmux-11 at a rate which is NOT constant, due to network delay variation (caused by congestion, re-routing, queuing mechanisms, wireless media, half-duplex media, etc.). The TDM devices at both ends require a constant flow of data, so they can't tolerate delay variation. Therefore the jitter buffer is required in order to provide the TDM equipment with a synchronous and constant flow. This is done as follows: • Upon startup, the jitter buffer stores packets up to its middle point (the number of packets correlates to the buffer's configured depth in milliseconds). Only after that point it starts outputting the E1/T1 flow towards its adjacent TDM device. The stored packets assure that the TDM device will be fed with data even if packets are delayed by the IP network. Obviously, if packets are delayed too long, then the buffer is gradually emptied out until it is underflowed. This situation is called buffer starvation. Each underflow event increases the jitter buffer underflow counter by one and indicates a problem in the end-to-end voice/data integrity. The second functionality of the jitter buffer is that in adaptive mode the jitter buffer is also a part of a mechanism being used to reconstruct the clock of the far end TDM side.

Table 4-4. Bundle Connection Parameters (Cont.)

Parameter	Description
Jitter Buffer Underflows (cont.)	An underflow situation can be a cause of: • Buffer starvation: Packets delay variation causes the buffer to empty out gradually until it is underflowed. • Continuous Sequence Errors. The sequence error means a halt in the valid stream of packet arrival into the jitter buffer. • Packets are being stopped/lost/dropped. • Too small jitter buffer configuration that can't compensate for the network delay variation. • When all system elements are not locked on the same master clock, it will lead to a situation in which data is clocked out of the jitter buffer at a rate different from the one it is clocked into. This will gradually result in either an overflow or underflow event, depending on which rate is higher. The event will repeat itself periodically as long as the system clock is not locked. • When an overflow (see below) situation occurs, IPmux-11 instantly flashes the jitter buffer, causing a forced underflow. So when you need to calculate the real underflow events and not the self-initiated ones, subtract the number of overflows from the total number of underflows counted by the device. Recommendations: • Try increasing the jitter buffer size. • Check reasons for sequence errors or lost/dropped packets (if present), system clocking configuration, Ethernet environment (full duplex) and connection, packets drop/loss/ignore by routers/switches or non-uniform packets output by routers/switches due to queuing mechanisms. • Make sure the same amount of TS for bundle is configured on each side of the IPmux-11 application, and that the "TDM bytes in frame" parameter is identical in both IPmux-11 units. • Make sure Ethernet/IP network provides priority (Quality Of Service) to the IPmux-11 traffic. Priority may be achieved by three means: VLAN tagging, IP TOS marking or by using the constant 2142 decimal value at each IPmux "UDP destination Port" field.
Jitter Buffer Overflows	The number of times an overflow situation took place. Explanation: In steady state, the jitter buffer is filled up to its middle point, which means it has the space to hold an additional similar quantity of packets. Overflow is opposite phenomenon of the Underflow, i.e., when a big burst of packets reaches the IPmux (a burst with more packets than the Jitter Buffer can store), the buffer will be filled up to its top. In this case, an unknown number of excessive packets are dropped and hence IPmux initiates a forced underflow by flashing (emptying) the buffer in order to start fresh from the beginning. An overflow situation always results in an immediate Underflow, forced by the IPmux. After the buffer is flashed, the process of filling up the buffer is started again, as explained above ("Underflow" section). An overflow situation can be a cause of: • A big burst of packets, filling up the buffer completely. The burst itself can often be a cause of some element along the IP network queuing the packets and then transmitting them all at once. • Too small jitter buffer configuration. • When system isn't locked on the same clock, it will lead to a situation in which data is clocked out of the jitter buffer at a rate different from the one it is clocked into. This will gradually result in either an overflow or underflow event, depending on which rate is higher. The event will repeat itself periodically as long as the system clock is not locked.

Table 4-4. Bundle Connection Parameters (Cont.)

Parameter	Description
	Recommendations: Check network devices and try increasing jitter buffer configuration. Check system's clocking configuration Make sure the same amount of TS for bundle is configured on each side of the IPmux-11 application, and that the "TDM bytes in frame" parameter is identical in both IPmux-11 units.

4.3 Diagnostic Tests

Diagnostic Loopbacks

Diagnostic capabilities of IPmux-11 include external and internal loopbacks.

External Loopback

IPmux-11 can be set to an external loopback to test the connection between the E1/T1 port and the PBX. In this mode, data coming from the PBX is both looped back to the PBX and transmitted forward to the IP network (see *Figure 4-10*).

This mode can also be achieved by a T1 FDL line loopback command.

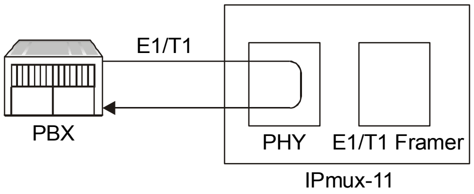


Figure 4-10. IPmux-11 External Loopback

Internal Loopback

The E1/T1 module can be set to an internal loop to test the connection between the E1/T1 port and the IP network. In this mode, data coming from the IP network is both looped back to the IP network and transmitted forward to the PBX connected to the E1/T1 port (see *Figure 4-11*).

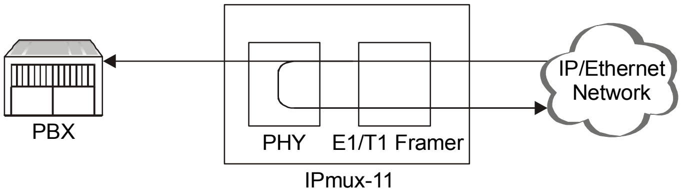


Figure 4-11. IPmux-11 Internal Loopback

➤ **To run a loopback:**

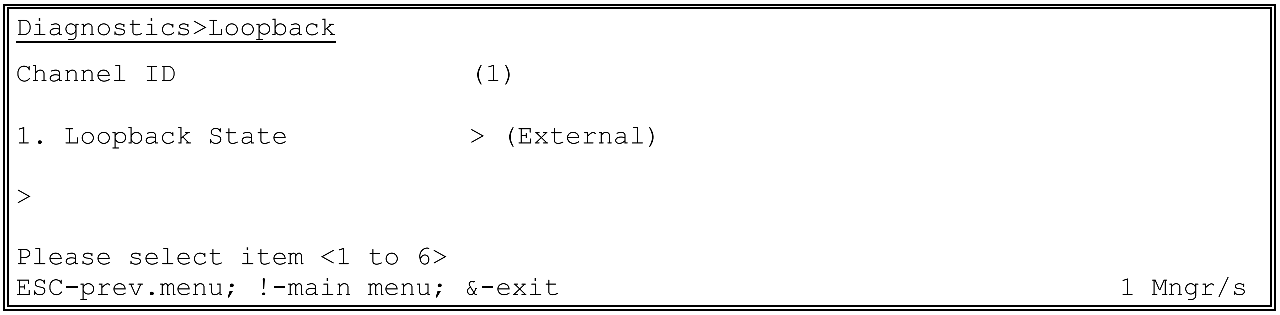
1. From the Diagnostics menu (*Figure 4-1*), select **Loopback**.

   The Loopback menu is displayed (see *Figure 4-12*).

2. From the Loopback menu, select **Loopback state**, and choose loopback that you intend to run (**Internal** or **External**).

➤ **To disable a loopback:**

- From the Loopback menu, select **Loopback state**, and set it to **Disable**.



```
Diagnostics>Loopback

Channel ID                    (1)

1. Loopback State             > (External)

>

Please select item <1 to 6>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure 4-12. Loopback Menu

Ping

You can ping remote IP host to check the IPmux-11 IP connectivity.

➤ **To ping an IP host:**

1. From the Diagnostics menu (*Figure 4-1*), select **Ping**.

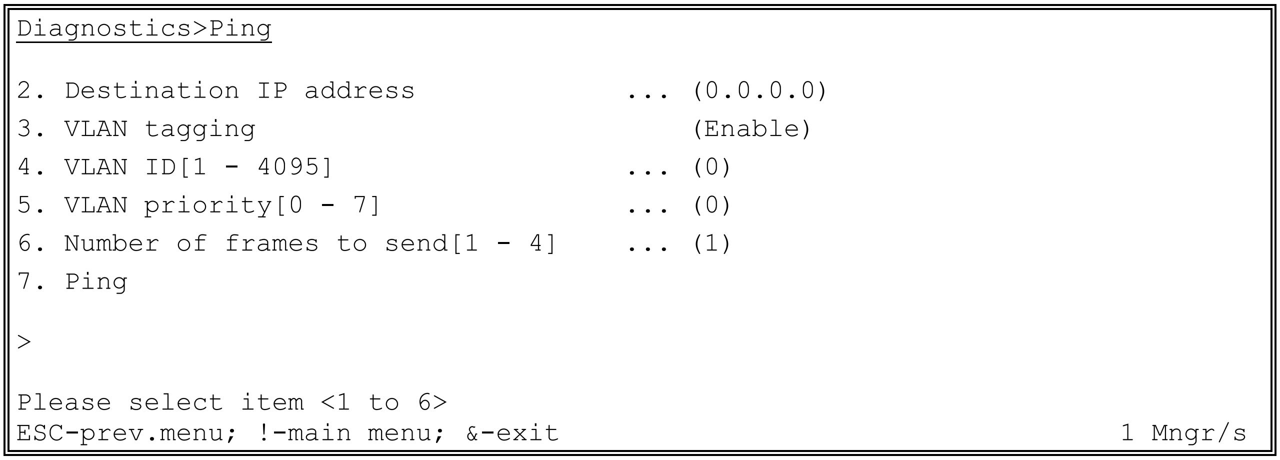
   The Ping menu appears (see *Figure 4-13*).

2. From the Ping menu, configure the following:
   - Destination IP Address (IP address of the host that you intend to ping): **0.0.0.0** to **255.255.255.255**.
   - VLAN Tagging:
     - **Enable** (VLAN tagging is enabled)
     - **Disable** (VLAN tagging is disabled)
   - VLAN ID: **1–4095**
   - VLAN Priority: **0–7**

Note *The VLAN ID and VLAN Priority configuration is available only if the VLAN tagging is enabled.*

   - Number of frames to send: **1–4.**

3. Select **Ping** to start sending pings.



```
Diagnostics>Ping

2. Destination IP address              ... (0.0.0.0)
3. VLAN tagging                            (Enable)
4. VLAN ID[1 - 4095]                   ... (0)
5. VLAN priority[0 - 7]                ... (0)
6. Number of frames to send[1 - 4]     ... (1)
7. Ping

>

Please select item <1 to 6>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure 4-13. Ping Menu

4.4 Troubleshooting

Table 4-5 presents the event types as they appear on the Event Log File and lists the actions required to correct the event (alarm) indication.

Table 4-5. IPmux-11 Troubleshooting Chart

Fault	Probable Cause	Remedial Action
E1/T1 equipment connected to IPmux-11 is not synchronized with IPmux-11.	Configuration or physical layer problems	3. Check cables and physical connectivity. 4. Check IPmux-11 E1/T1 configuration and, if necessary, other IPmux-11 parameters. 5. Check E1/T1 physical connection (use loopbacks).
Slips and errors in E1/T1 equipment	• Ethernet port in switch and IPmux-11 are not in the same rate or duplex mode • Ethernet port is set to work in half duplex mode (may cause extreme PDV because of collisions and backoffs) • Timing configuration is not properly set (periodic buffer under/overflows shown on IP channel status menu) • Network PDV or lost frames	1. Check E1/T1 physical connection (use loopbacks). 2. Check timing settings according to explanation in this manual. 3. Check switch and IPmux-11 port configuration (negotiation, rate, duplex mode). 4. Check PDV introduced by the network, and, if necessary, increase PDVT jitter buffer setting..
Echo in voice	High delay in voice path	1. Check network delay and try to decrease it. 2. Try to decrease PDVT (jitter) buffer.

4.5 Alarm Relay

IPmux-11 supports dry contact alarm relay via dedicated pins of the RJ-45 EXT CLK connector.

Table 4-6. Alarm Relay Pins of the EXT CLK Connector

Pin	Function
6	Dry contact relay (normally shorted to pin 7
7	Dry contact relay (central pin)
8	Dry contact Relay (normally open, closed if ALARM active)

4.6 Frequently Asked Questions

Question: How does the IPmux handle/propagate alarms on the TDM and Ethernet side?

Answer

The IPmux handles alarms on the TDM and Ethernet side in the following manner:

TDM Side Alarms:

Unframed mode:

- In case of LOS (Loss Of Signal) on the local IPmux side, AIS will be sent towards the IP side, and will then be transferred over the E1/T1 to the remote TDM device.
- All other alarms sent from the near-end TDM device (including information on timeslot 0), will be propagated transparently by the local IPmux, to the remote end TDM device (over the IP connection).

Framed mode:
In case of LOS/LOF/AIS detected on the local IPmux side, a user-configurable conditioning pattern (00 to FF) will be sent on the relevant time slots (over the IP connection), to the far-end TDM device. A user-configurable conditioning pattern can also be applied on the ABCD bits (CAS signaling 1 to F) going towards the remote PBX.
The frame synch on the E1/T1 level is maintained in favor of the end TDM devices.

Ethernet Side Alarms:

Unframed mode:
In case of local failure on the IPmux, or a situation of jitter buffer underflow/overflow, an (unframed) AIS will be sent towards the near-end TDM side

Framed mode:
In case of local failure on the IPmux, or situation of jitter buffer underflow/overflow, a conditioning pattern (00 to FF) will be sent towards the near-end TDM device on the time slots related to that specific bundle. A user-configurable conditioning pattern can also be applied on the ABCD bits (CAS signaling 1 to F), going towards the local TDM device.
In this case the synch on the E1/T1 level is maintained in favor of the TDM end devices.

Question: How can I ensure the IPmux TDMoIP traffic priority over an IP Ethernet network?

Answer:

The IPmux family is equipped with three different features that can be implemented in order to give the IPmux TDMoIP traffic priority over an IP/Ethernet network:

- VLAN ID (Layer 2)
- ToS field (Layer 3)
- UDP destination port (Layer 4)

Each QoS feature is based on a different OSI level and can be used individually in order to ensure the TDMoIP traffic priority. When determining which feature to use, it is important to verify that the different elements on the network, (Switches / Routers / etc.), support the selected priority mechanism and are also configured to give the highest priority to the labeled IPmux traffic.
Notice that the priority is given to the TDMoIP traffic by the network elements and the IPmux is merely tagging the packets.

VLAN ID
The IPmux complies with standards IEEE 802.1p&q. This enables the user to set both VLAN ID and VLAN Priority. It adds four bytes to the MAC layer (Layer 2) of the Ethernet frame. These bytes contain information about the VLAN ID, and the VLAN priority, which runs from 0-7. The IPmux only tags the packets, while the Switches are responsible for giving the priority according to the VLAN info. Verify that the IPmux traffic has the highest priority in the relevant Ethernet network.

ToS
There are several RFCs (RFC791, RFC1349, RFC2474) that define how the IP ToS should be configured. The ToS is a byte located in the IP header (Layer 3).
In general the Type of Service octet, in most cases, consists of three fields:
The first field, labeled "PRECEDENCE", is intended to denote the importance or priority of the datagram.
The second field, labeled "TOS", denotes how the network should make tradeoffs between throughput, delay, reliability, and cost.
The last field, labeled "MBZ" (for "must be zero") above, is currently unused.
The IPmux enables configuring the whole IP ToS byte, and therefore it is adaptable to each RFC in the market. The IP ToS parameter in the IPmux is user-configured in terms of decimal value. However, on the frame itself it of course appears in binary format. The decimal value varies between 0 and 255 (8 bits).

A configuration example:
Setting IP precedence of 101 and IP ToS of 1000 will give us the byte 10110000, which means that the IPmux IP-ToS parameter should be configured to 176 decimals.

UDP Destination Port
The IPmux uses the UDP protocol (Layer 4) in order to transfer the TDMoIP traffic. In the UDP protocol, the ¿Destination port¿ field is always set to the decimal value of 2142, hence all the packets leaving the IPmux are tagged accordingly. This unique value was assigned to RAD by the IANA organization for TDMoIP applications.
The network elements may be used to give priority to the TDMoIP traffic according to the UDP destination field.

Question: Does allocating a sufficient bandwidth ensure the proper functionality of an IPmux-based application?

Answer

A sufficient bandwidth is not enough to ensure a steady environment for the IPmux, since networks loaded with additional non-IPmux LAN traffic (e.g. PCs traffic) or incompetent Ethernet/IP network may cause several problems:

- Jitter - The IPmux packets may suffer a delay variation (although all the traffic will eventually pass through due to that fact that there is sufficient bandwidth). Packets will be delayed for different periods of time due to overloaded networks, queuing mechanisms, etc. IPmux can compensate for some jitter (IPmux-1 up to 300 msec, IPmux-4/8/16 up to 32 msec for E1 and 24 msec for T1) but bigger jitter will cause problems.
- Misordering - Packets might be sent in different order than the order in which they were originally sent from the IPmux.
  Note that a certain IPmux version which fixes misordering is available, contact Tech support.
- Packet Loss - Packets might be dropped/ignored by some elements in the network (Routers/Switches) due to insufficient processing power to handle the load, queuing mechanisms, buffer overflows, etc.

Normally these problems are solved by giving priority to the IPmux traffic over all other traffic.
As can be shown, even though there is sufficient bandwidth, there might still be cases in which the traffic will be transmitted from all the sources at the same time and thus create a momentary load on the network element (router/switch), even when this load that does not exceed the available bandwidth. Since the IPmux is constantly transmitting, the TDMoIP traffic will always be a part of such a load.
When no priority is given to the TDMoIP traffic, the network elements will handle the TDMoIP traffic as any other type of traffic.
All the above degrade the performance of the IPmux unit, although an adequate amount of bandwidth is provided for the IPmux.
Refer to FAQ 3338 to understand how to check the IPmux and network performance and how to solve problems.

Appendix A

Connector Wiring

A.1 E1 and T1 Connector

Balanced Connector

The E1 and T1 interfaces of IPmux-11 terminate in an 8-pin RJ-45 connector, wired in accordance with *Table A-1*.

Table A-1. E1/T1 Port Connector Pinout

Pin	Designation	Direction	Function
1	RD (R)	Input	Receive data (ring)
2	RD (T)	Input	Receive data (tip)
3, 6	–	–	FGND
4	TD (R)	Output	Transmit data (ring)
5	TD (T)	Output	Transmit data (tip)
7, 8	–	N/A	Not connected

Balanced-to-Unbalanced Adapter Cable

When IPmux-11 is ordered with unbalanced E1 interface, it is necessary to convert RJ-45 connector to the standard pair of BNC female connectors used by unbalanced E1 interfaces. For that purpose, RAD offers a 150-mm long adapter cable, CBL-RJ45/2BNC/E1/X, wired in accordance with *Figure A-1*.

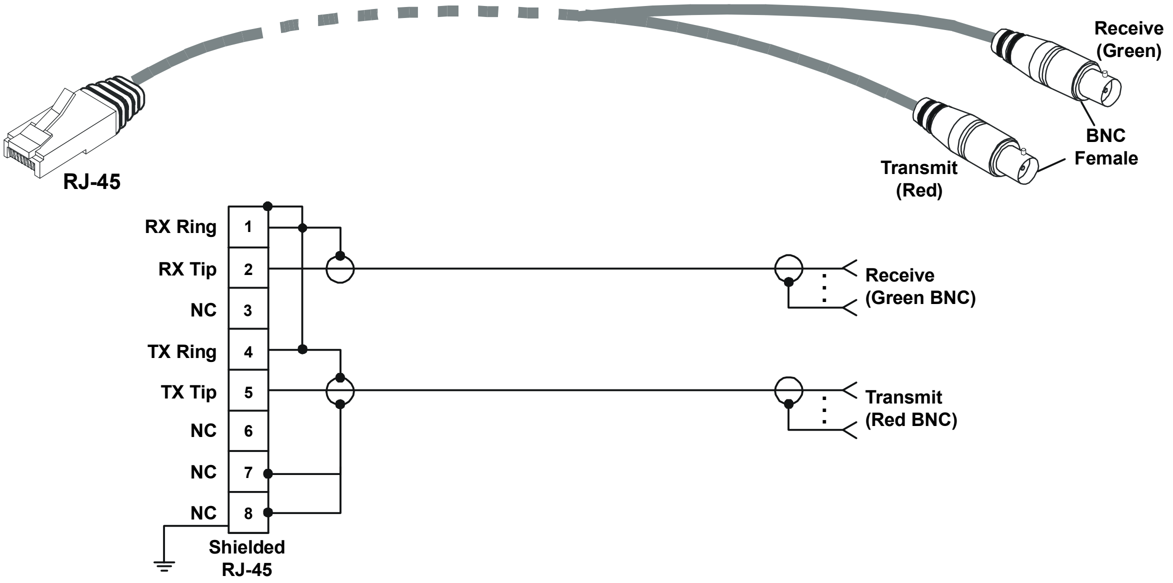


Figure A-1. CBL-RJ45/2BNC/E1/X Cable Wiring Diagram

A.2 Ethernet Connectors

The network and user Ethernet electrical interfaces terminate in 8-pin RJ-45 connectors, wired in accordance with *Table A-2*.

Table A-2. Ethernet Connector Pinout

Pin	**Function**
1	Tx+
2	Tx–
3	Rx+
4	–
5	–
6	Rx–
7	–
8	–

A.3 CONTROL Connector

The control terminal interface terminates in a V.24/RS-232 9-pin D-type female DCE connector. *Table A-3* lists the CONTROL connector pin assignments.

Table A-3. CONTROL Connector Pinout

Pin	**Function**
1	–
2	Rx
3	Tx
4	–
5	GND
6	–
7	–
8	–
9	–

A.4 External Clock Connector

The external clock interface terminates in an 8-pin RJ-45 connector, which also serves for alarm relay. *Table A-4* lists the connector wiring.

Table A-4. EXT CLK Connector Pinout

Pin	Function
1	RxRing (clock in)
2	RxTip (clock in)
3	Alarm In (RS-232 level signal)
4	TxRing (clock out, optional)
5	TxTip (clock out, optional)
6	Dry contact relay (normally shorted to pin 7)
7	Dry contact relay (central pin)
8	Dry contact Relay (normally open, closed if ALARM active)

Appendix B

Boot Sequence and Downloading Software

This appendix provides a description of the IPmux-11 boot procedure via an ASCII terminal for downloading software.

The file system can hold two compressed copies of the IPmux-11 code. One copy is called the operating file, and the other is called the backup file. The operating file is the default-executable IPmux-11 code. The backup file is used whenever the operating file is absent or corrupted.

B.1 Booting IPmux-11

IPmux-11 boots up automatically. After powering up, no user intervention is required, except when the user wants to access the file system to modify or update the software or the IPmux-11 configuration.

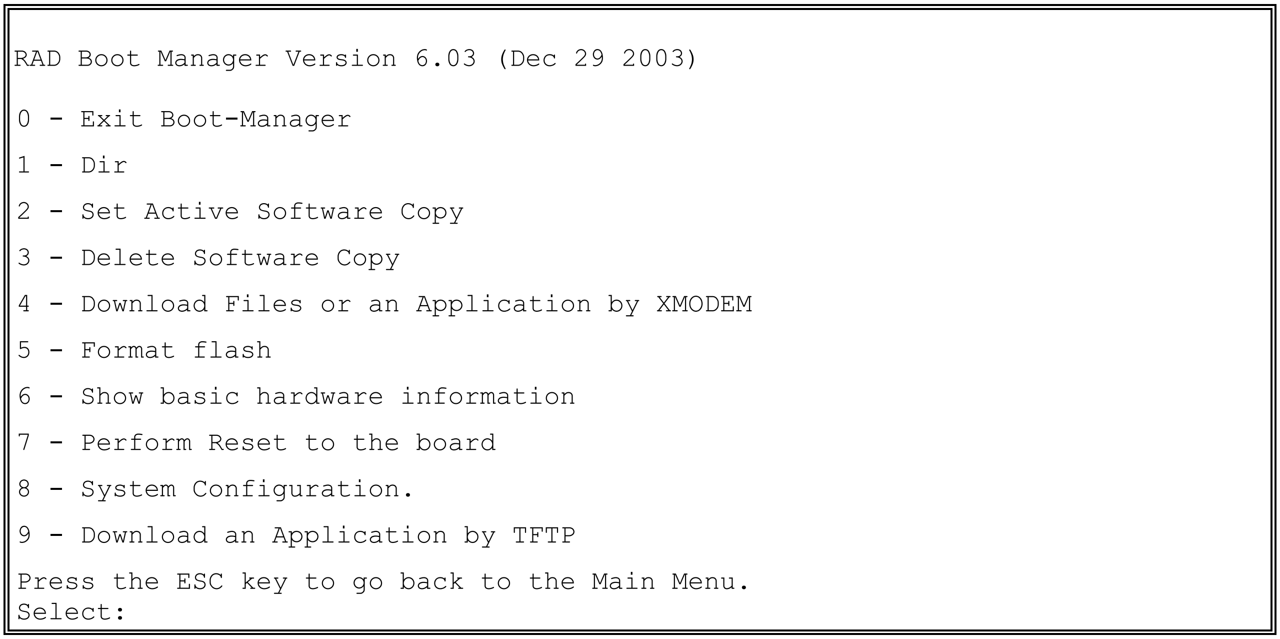
Accessing the Boot Manager

The Boot Manager menu is an option that allows the user to perform basic file transfer operations. These operations are all optional.

➤ **To access the Boot Manager menu:**

- Press **<Enter>** several times immediately after powering up the IPmux-11.

  The Boot Manager menu is displayed (see *Figure B-1*).



```
RAD Boot Manager Version 6.03 (Dec 29 2003)

0 - Exit Boot-Manager

1 - Dir

2 - Set Active Software Copy

3 - Delete Software Copy

4 - Download Files or an Application by XMODEM

5 - Format flash

6 - Show basic hardware information

7 - Perform Reset to the board

8 - System Configuration.

9 - Download an Application by TFTP

Press the ESC key to go back to the Main Menu.
Select:
```

Figure B-1. Boot Manager Menu

From the Boot Manager menu, you can:

- List all files stored in the flash memory
- Exchange the operating and backup files
- Delete the operating file; the backup file becomes the operating file
- Download a new operating file (via XMODEM or TFTP); the previous operating file is saved as the backup file
- Delete all software and configuration files
- Display the basic hardware information (RAM, ROM size etc)
- Reset the IPmux-11 board
- Configure the IPmux-11 IP address, IP mask and default gateway for the consecutive file download via TFTP.

If you choose to exchange or delete a file, you are prompted for confirmation.

B.2 Downloading the Application and Configuration Software

New application software releases are distributed as separate files, which are downloaded to IPmux-11 using the XMODEM protocol or TFTP from the Boot Manager menu. Alternatively, you can download a new software release via TFTP, when the IPmux-11 management software is already running (**Main menu** > **Utilities** > **File Utilities** > **Download/Upload using TFTP**).

The TFTP protocol can also be used for uploading configuration files which contain the IPmux-11 database to the management station. Administrators can use this capability to distribute verified configuration files to all other units which use the similar configuration.

Downloading Application Files via XMODEM

Downloading application files using the XMODEM protocol is performed from the Boot Manager menu.

➤ **To download application file via XMODEM:**

1. Configure your ASCII terminal or terminal emulation utility running on your PC to the 115.2 kbps data rate.
2. Access the Boot Manager menu.

   The Boot Manager menu appears (see *Figure B-1*).
3. From the Boot Manager menu, type **4**.

   IPmux-11 displays the following message:
   `Select Copy number for download ( 0 )`
4. Select the backup partition by typing its number, **0** or **1**.

   IPmux-11 responds with the following string:
   `Please start the XMODEM download.`
5. Send the software release file to IPmux-11 using the XMODEM utility of you terminal application.

   Once the downloading is completed, IPmux-11 saves the new release as an active partition, the former active partition turns into backup, and the boot sequence continues normally.

   If a failure occurs during the download, the partially downloaded software is erased. In this case, only active software is left in the flash memory.

Downloading Application Files via TFTP

The application software is downloaded when IPmux-11 has been already completed the boot-up procedure and the management software is running.

➤ **To download application file via TFTP:**

1. From the Boot Manager menu, select **System Configuration**.
2. Configure the IP parameters of IPmux-11 (IP address, IP mask and default gateway). These parameters are valid only for the TFTP file transfer via the Boot Manager.
3. Start a TFTP application.
4. Configure the communication parameters as follows:
   - Connection timeout – more than 30 seconds to prevent an automatic disconnection during the backup partition deletion (about 25 seconds).
   - Block size – 512 bytes.
   - UDP port – 69.
5. Select a local software release file to download.

6. Enter the IPmux-11 IP address.
7. Start downloading.

   IPmux-11 automatically erases the backup partition (it takes about 25 seconds). Once the downloading is completed, IPmux-11 saves the new release as an active partition, the former active partition turns into backup.

Uploading/Downloading Configuration Files via TFTP

You can upload a IPmux-11 configuration file to the management station for further distribution to all other units which use the similar configuration.

➤ **To upload application file via TFTP:**

1. Start a TFTP application.
2. Select the configuration to upload.
3. Enter the IPmux-11 IP address.
4. Start uploading.

   When the uploading is completed, you can download the configuration file to other IPmux-11 units.

Appendix C

SNMP Management

This appendix provides specific information for IPmux-11 management by SNMP (Simple Network Management Protocol).

The SNMP management functions of IPmux-11 are provided by an internal SNMP agent. The SNMP management communication uses UDP (User Datagram Protocol), which is a connectionless-mode transport protocol, part of the IP (Internet Protocol) protocol suite.

This appendix covers the information related to the SNMP environment.

C.1 SNMP Environment

SNMP Principles

The SNMP is an asynchronous command-response polling protocol. All management traffic is initiated by the SNMP-based network management station, which addresses the managed entities in its management domain. Only the addressed managed entity answers the polling of the management station (except for trap messages).

The managed entities include a function called an SNMP agent, which is responsible for interpretation and handling of the management station requests to the managed entity, and the generation of properly formatted responses to the management station.

SNMP Operations

The SNMP protocol includes four types of operations:

- **getRequest**: Command for retrieving specific management information from the managed entity. The managed entity responds with a **getResponse** message.
- **getNextRequest**: Command for retrieving sequentially specific management information from the managed entity. The managed entity responds with a **getResponse** message.
- **setRequest**: Command for manipulating specific management information within the managed entity. The managed entity responds with a **getResponse** message.
- **trap**: Management message carrying unsolicited information on extraordinary events, which are events that occurred not in response to a management operation reported by the managed entity.

Management Information Base (MIB)

The MIB includes a collection of managed objects. A managed object is defined as a parameter that can be managed, such as a performance statistics value. The MIB includes the definitions of relevant managed objects. Various MIBs can be defined for various management purposes or types of equipment.

An object definition includes the range of values (also called instances) and the following access rights:

- **Read-only**: Instances of that object can be read, but cannot be set.
- **Read-write**: Instances of that object can be read or set.
- **Write-only**: Instances of that object can be set, but cannot be read.
- **Not accessible**: Instances of that object cannot be read, or set.

MIB Structure

The MIB has an inverted tree-like structure, with each definition of a managed object forming one leaf, located at the end of a branch of that tree.

Each leaf in the MIB is reached by a unique path. Thus, by numbering the branching points starting with the top, each leaf can be uniquely defined by a sequence of numbers.

The formal description of the managed objects and the MIB structure is provided in a special standardized format, called ASN.1 (Abstract Syntax Notation 1). Since the general collection of MIBs can also be organized in a similar structure, under IAB (Internet Activities Board) supervision, any parameter included in a MIB that is recognized by the IAB is uniquely defined.

To provide the flexibility necessary in a global structure, MIBs are classified in various classes (branches). One is the experimental branch and another the group of private (enterprise-specific) branch.

Under the private enterprise-specific branch of MIBs, each enterprise (manufacturer) can be assigned a number, which is its enterprise number. The assigned number designates the top of an enterprise-specific sub-tree of non-standard MIBs. Within this context, RAD has been assigned the enterprise number **164**. Therefore, enterprise MIBs published by RAD can be found under **1.3.6.1.4.1.164**.

MIBs of general interest are published by the IAB in the form of a Request for Comment (RFC) document. In addition, MIBs are also often assigned informal names that reflect their primary purpose. Enterprise-specific MIBs are published and distributed by their originator, who is responsible for their contents.

MIBs Supported by the IPmux-11 SNMP Agent

The interpretation of the relevant MIBs is a function of the SNMP agent of each managed entity. The general MIBs supported by the IPmux-11 SNMP agent are:

- rfc1213.mib (except the interfaces view which is supported via RFC 2233)
- ianaiftype.mib (defines the ifType)

- rfc2233.mib (IF-MIB)
- rfc2011.mib
- rfc2012.mib
- rfc2013.mib
- rfc1907.mib
- rfc2683.mib
- rfc1215.mib
- rfc1493.mib
- rfc1643.mib
- rfc2239.mib
- rfc2494.mib
- rfc2261.mib
- rfc1695.mib
- rfc2674.mib
- rfc2819.mib
- rfc2495.mib (except Far End objects and RW configuration objects which are different for each configuration) - replaces RFC 1406; which is now obsolete.
- IPmux RAD private mib.

The IPmux-11 object ID is
iso (1).org(3).dod(6).internet(1).private(4).enterprises(1).rad(164).radGen(6). systems(1).radSysIPMux(3).IPmux11(106)

Enterprise-specific MIBs supported by RAD equipment, including IPmux-1/1E6, are available in ASN.1 format from the RAD Technical Support department.

Management Domains under SNMP

In principle, SNMP allows each management station that recognizes the MIBs supported by a device to perform all the management operations available on that device. However, this is not desirable in actual practice, it is necessary to provide a means to delimit management domains.

SNMP Communities

SNMP delimits management domains by defining communities. Each community is identified by a name, which is an alphanumeric string of up to 255 characters defined by the user.

The IPmux-11 SNMP agent defines strings of up to 10 characters (case sensitive, numeric and alphabetical).

Any SNMP entity (both managed entities and management stations) is assigned a community name by its user. In parallel, the user defines a list of the communities for each SNMP entity that are authorized to communicate with the entity, and the access rights associated with each community (this is the SNMP community name table of the entity).

In general, SNMP agents support two types of access rights:

Read-Only: The SNMP agent accepts and processes only SNMP **getRequest** and **getNextRequest** commands from management stations which have a Read-Only community name.

Read-Write: The SNMP agent accepts and processes all the SNMP commands received from a management station with a Read-Write community name.

Authentication

In accordance with SNMP protocol, the SNMP community of the originating entity is sent in each message.

When an SNMP message is received by the addressed entity, it first checks the originator's community. Messages with community names not included in the SNMP community names table of the recipient are discarded. SNMP agents of managed entities usually report this event by means of an authentication failure trap.

The SNMP agents of managed entities evaluate messages originated by communities appearing in the agent's SNMP community names table in accordance with the access rights, as previously explained. Thus, a **setRequest** for a MIB object with read-write access rights will nevertheless be rejected if it comes from a management station whose community has read-only rights with respect to that particular agent.

Network Management Stations

The IPmux-11 SNMP agent stores the IP address of the Network Management Station (NMS) that is intended to manage it.

Appendix D

Configuration Menus

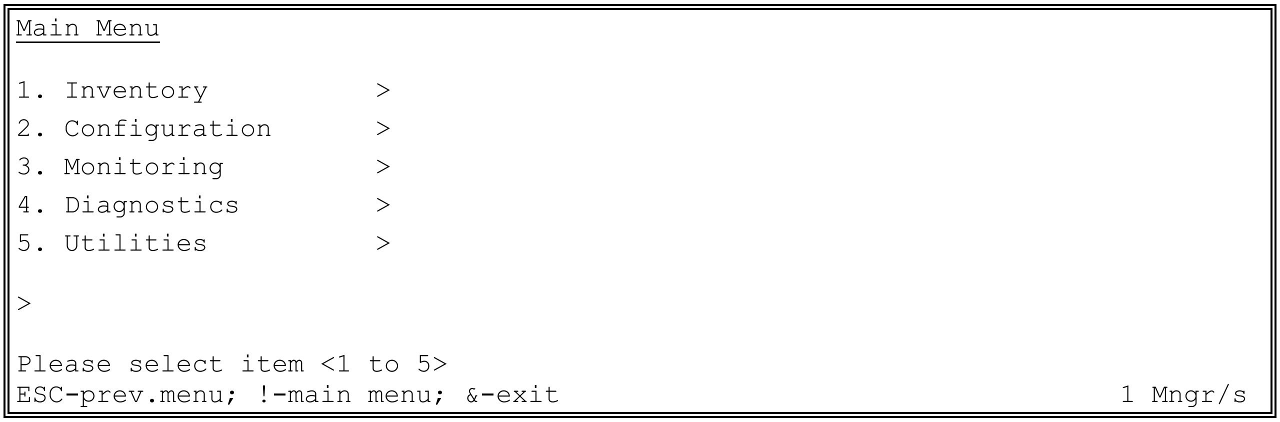
This appendix illustrates the configuration IPmux-11 screens and explains their parameters.

Menu trees of the IPmux-11 management software are shown in *Chapter 3*.

D.1 Main Menu

The Main menu options are:

- **Inventory –** displays information on the functional blocks of the unit
- **Configuration –** defines parameters for the IPmux-11 system, physical layer, connections and internal switch.
- **Monitoring** – monitors system performance
- **Diagnostics** – initiates diagnostic tests (loopbacks and ping)
- **Utilities** – manages new software transfers.



```
Main Menu

1. Inventory          >
2. Configuration      >
3. Monitoring         >
4. Diagnostics        >
5. Utilities          >

>

Please select item <1 to 5>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-1. Main Menu

The following sections in this appendix explain the parameters in each of the menu options.

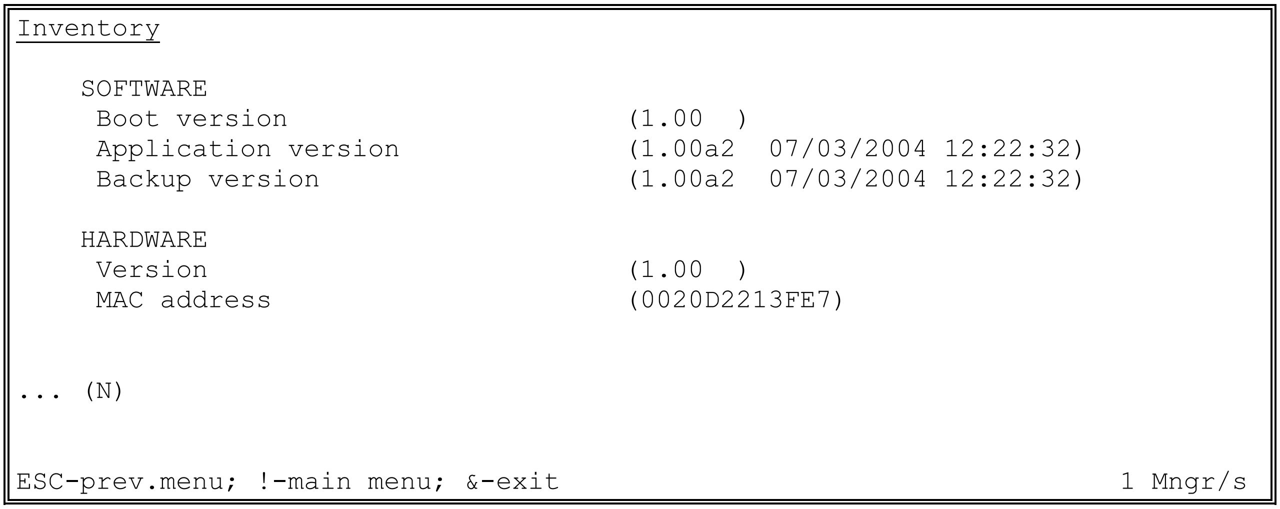
D.2 Displaying the IPmux-11 Inventory

The IPmux-11 inventory displays information on current software and hardware revisions of the unit. It also provides the IPmux-11 interface description.

➤ **To display the IPmux-11 inventory:**

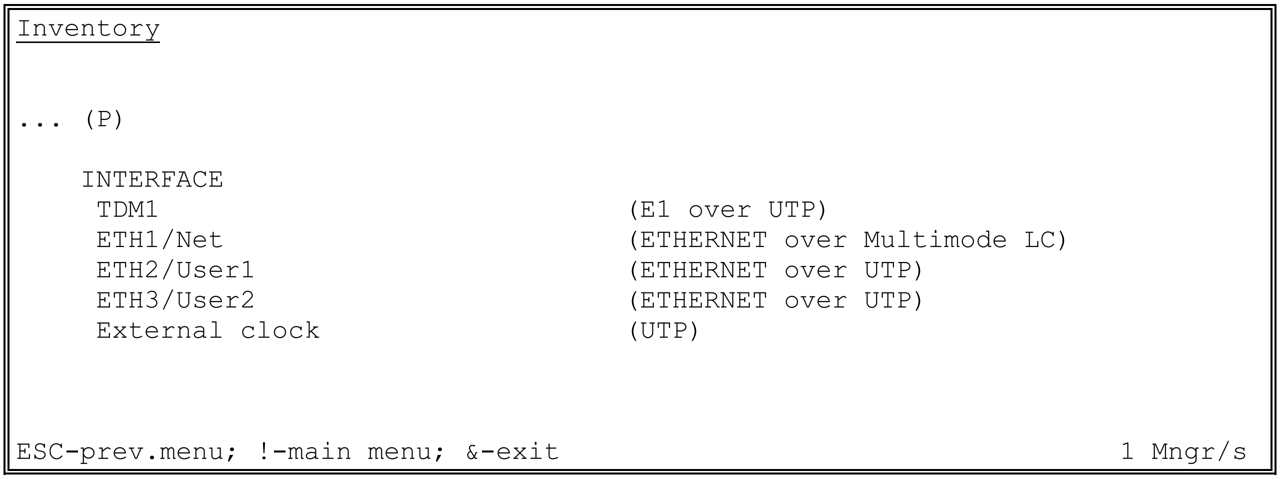
- From the Main menu, select **Inventory**.

  The Inventory menu appears (see *Figure D-2*).



```
Inventory

    SOFTWARE
     Boot version                       (1.00  )
     Application version                (1.00a2  07/03/2004 12:22:32)
     Backup version                     (1.00a2  07/03/2004 12:22:32)

    HARDWARE
     Version                            (1.00  )
     MAC address                        (0020D2213FE7)


... (N)


ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-2. Inventory Screen (Page 1)



```
Inventory


... (P)

    INTERFACE
     TDM1                               (E1 over UTP)
     ETH1/Net                           (ETHERNET over Multimode LC)
     ETH2/User1                         (ETHERNET over UTP)
     ETH3/User2                         (ETHERNET over UTP)
     External clock                     (UTP)



ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-3. Inventory Screen (Page 2)

D.3 Configuring System Parameters

The IPmux-11 management software allows you to perform the following:

- Defining IP parameters of the IPmux-11 host
- Configuring management access
- Setting data and time
- Resetting IPmux-11 to the default values.

IPmux-11 systems parameters are configured via System menu.

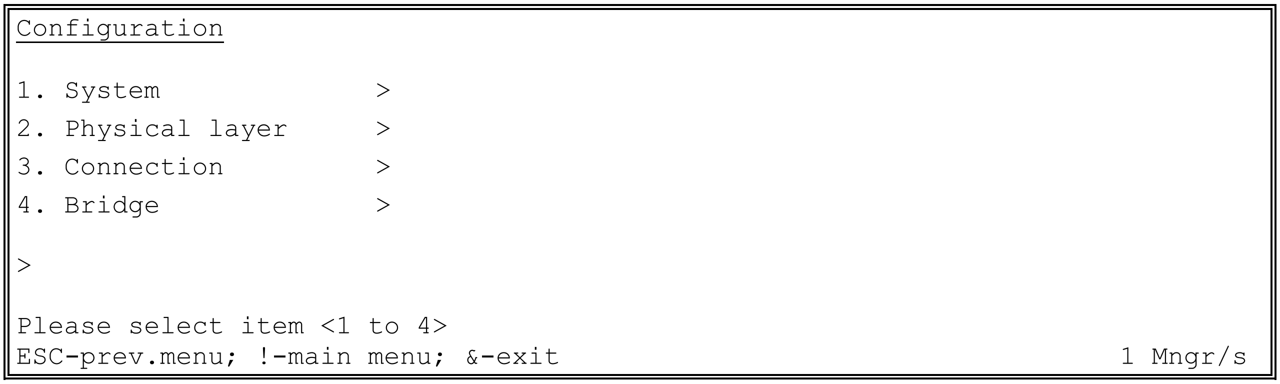
➤ **To access System menu:**

1. From the Main menu, select **Configuration**.

   The Configuration menu is displayed (see *Figure D-4*).

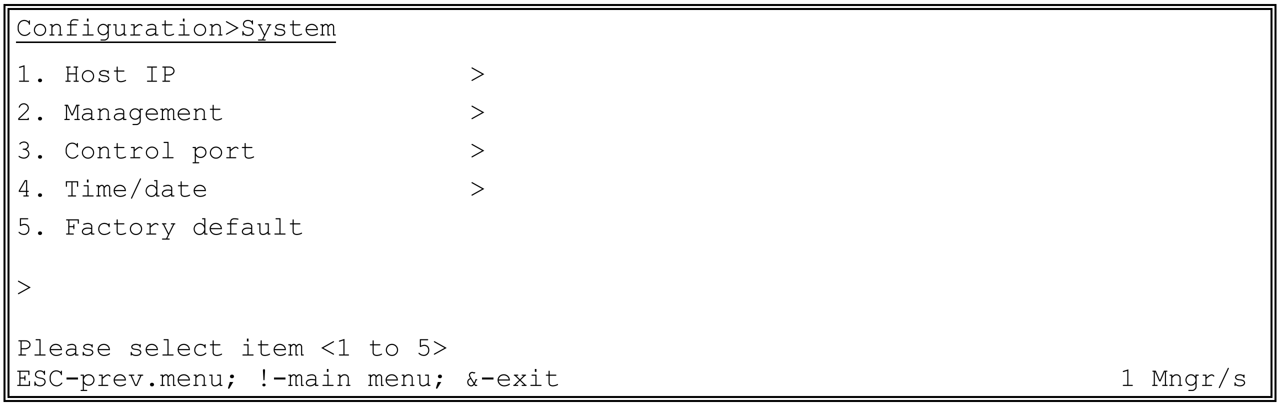
2. From the Configuration menu, select **System**.

   The System menu appears (see *Figure D-5*).



```
Configuration

1. System              >
2. Physical layer      >
3. Connection          >
4. Bridge              >

>

Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                1 Mngr/s
```

Figure D-4. Configuration Menu



```
Configuration>System
1. Host IP                   >
2. Management                >
3. Control port              >
4. Time/date                 >
5. Factory default

>

Please select item <1 to 5>
ESC-prev.menu; !-main menu; &-exit                                1 Mngr/s
```

Figure D-5. System Menu

Configuring IP Host Parameters

IPmux-11 can be managed by a network management station, which is located on the LAN connected to the one of the unit's Ethernet ports. In order to establish a proper connection, it is necessary to configure the following: host IP address, subnet mask, default gateway, its trap, read and write communities.

Note *DHCP client configuration is currently unavailable.*

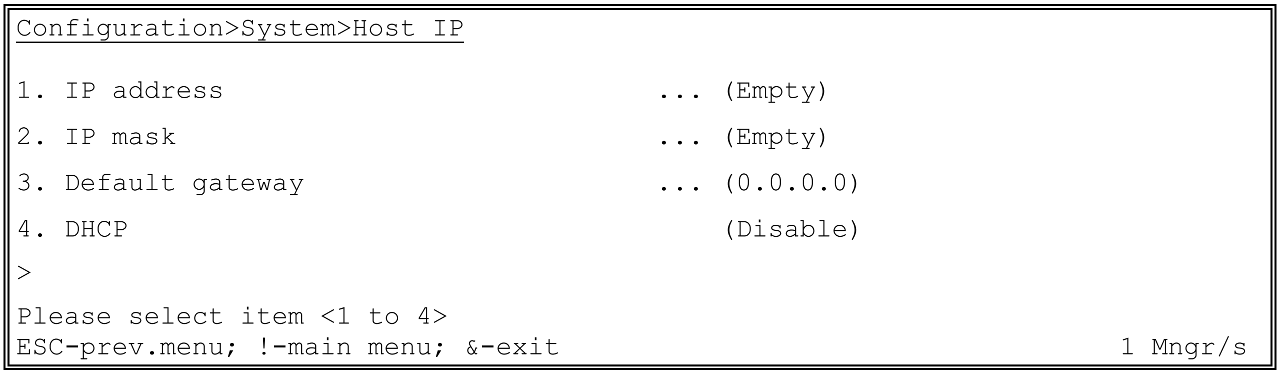
➤ **To define the IP parameters:**

1. From the System menu, select **Host IP**.

   The Host IP menu appears (see *Figure D-6*).

2. From the Host IP menu, perform the following:
   - Select **Host IP list** to define the host IP address
   - Select **IP mask** to define the host IP mask.
   - Select **Default gateway** to set the default gateway IP address.

Note *The default gateway must be in the same subnet as the host.*



```
Configuration>System>Host IP

1. IP address                             ... (Empty)
2. IP mask                                ... (Empty)
3. Default gateway                        ... (0.0.0.0)
4. DHCP                                       (Disable)
>

Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
```

Figure D-6. Host IP Menu

Configuring Management Parameters

You can configure the following management parameters:

- Define system name and location
- Define read, write and trap communities
- Specify network managers
- Enable or disable management access via Telnet or Web browser
- Define alarm masks.

Assigning a Name to IPmux-11 and Its Location

The IPmux-11 management software allows you to assign a name to the unit and its location to distinguish it from the other devices installed in your system.

➤ **To assign a name to IPmux-11 and its location:**

1. From the System menu (*Figure D-5*), select **Management**.

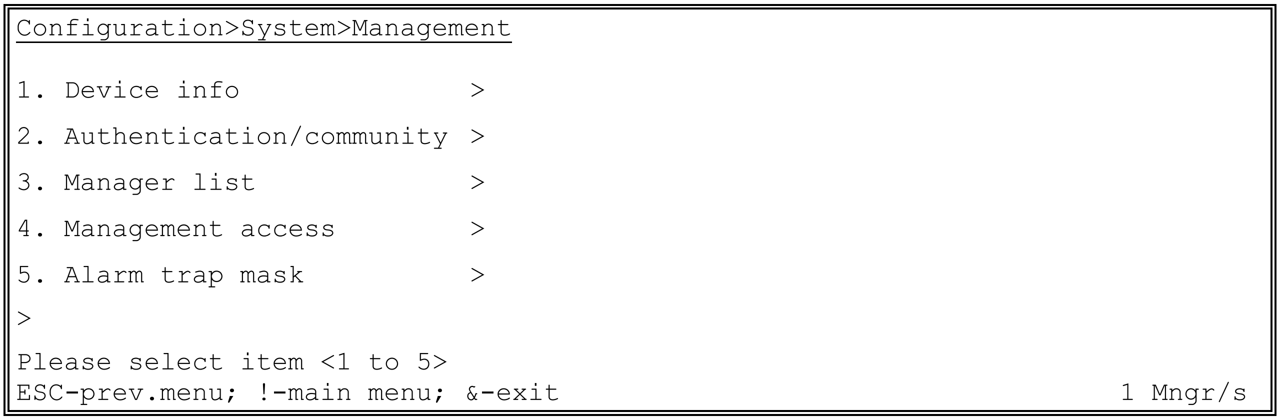
   The Management menu is displayed (see *Figure D-7*).

2. From the Management menu, select **Device info**.

   The Device Info menu appears (see *Figure D-8*).

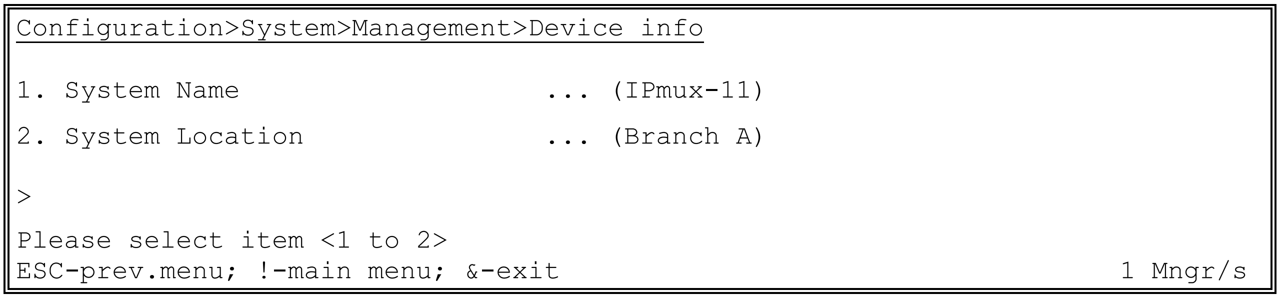
3. From the Device Info menu, select **System name** and enter the desired name for the IPmux-11 device.

4. Select **System location**, and enter the desired name for the current IPmux-11 location.



```
Configuration>System>Management

1. Device info              >
2. Authentication/community >
3. Manager list             >
4. Management access        >
5. Alarm trap mask          >
>
Please select item <1 to 5>
ESC-prev.menu; !-main menu; &-exit                         1 Mngr/s
```

Figure D-7. Management Menu



```
Configuration>System>Management>Device info

1. System Name                      ... (IPmux-11)
2. System Location                  ... (Branch A)

>
Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                         1 Mngr/s
```

Figure D-8. System Info Menu

Defining Read, Write and Trap Communities

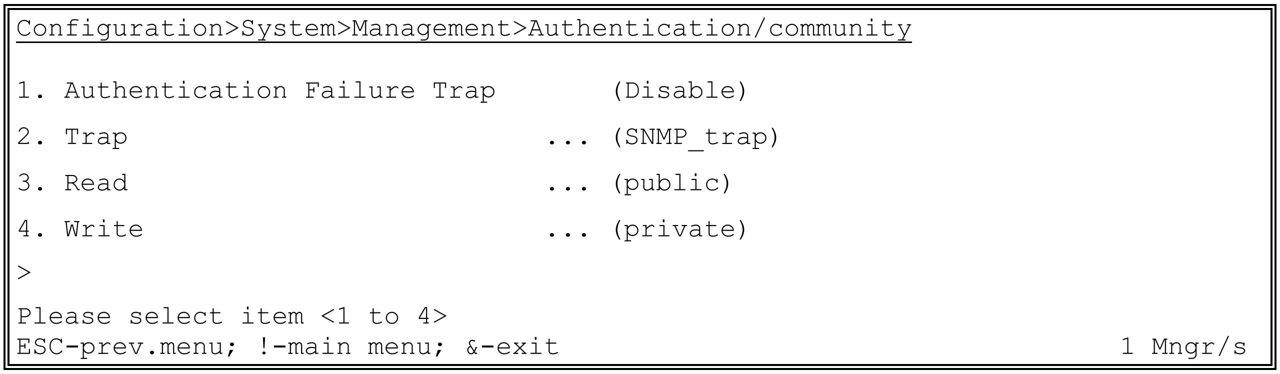
You have to assign names for the read, write and trap communities. In addition, you can enable sending the authentication failure trap, if a network manager from an unauthorized community attempts to access IPmux-11.

➤ **To define read, write and trap communities:**

1. From the Management menu, select **Authentication/community**.

   The Authentication/Community menu appears (see *Figure D-9*).

2. From the Authentication/Community menu, do the following:
   - Select **Authentication failure trap** to enable or disable sending this trap in case of an unauthorized access attempt.
   - Select **Trap** to enter the name of a community to which IPmux-11 will send traps (up to 10 alphanumeric characters, case-sensitive).
   - Select **Read** to enter the name of a community with read-only authorization (up to 10 alphanumeric characters, case-sensitive).
   - Select **Write** to enter the name of a community with write authorization (up to 10 alphanumeric characters, case-sensitive).



```
Configuration>System>Management>Authentication/community

1. Authentication Failure Trap       (Disable)
2. Trap                          ... (SNMP_trap)
3. Read                          ... (public)
4. Write                         ... (private)
>

Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-9. Authentication/Community Menu

Defining Network Managers

Define or modify the network management stations to which the SNMP agent of IPmux-11 will send traps. Up to 16 managers can be defined. In addition, you can enable or disable manager stations to receive traps.

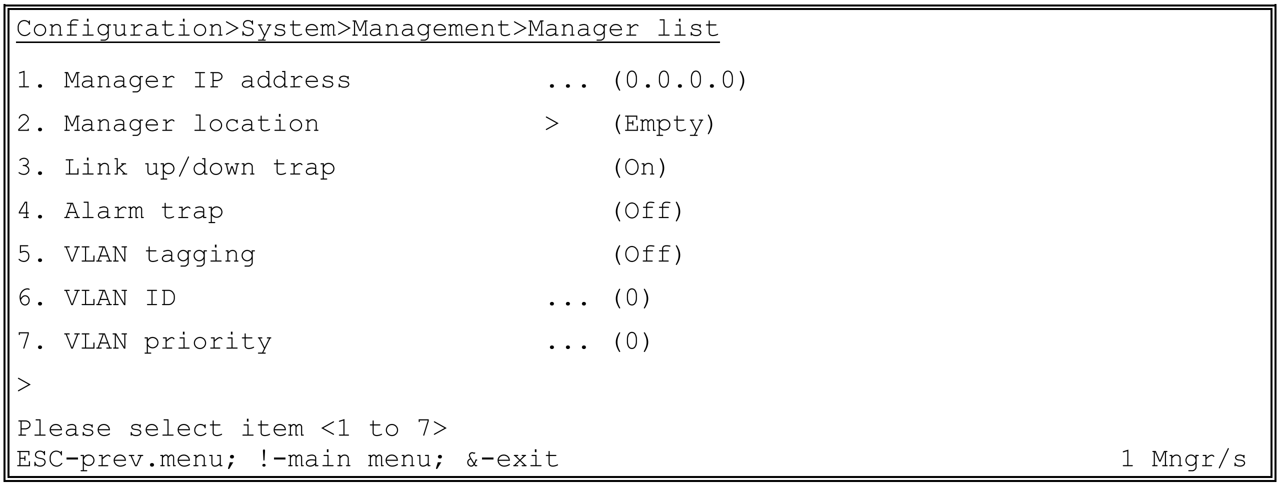
➤ **To define network managers:**

1. From the Management Access menu (see *Figure D-5*), select **Manager list**.

   The Manager List menu appears (see *Figure D-9*).

2. From the Manager List menu, perform the following:
   - Select **Manager IP address**, and enter an IP address of the manager station.
   - Select **Manager location**, and from the Manager Location menu, choose the IPmux-11 port to which the current management station is connected (**Network-Eth1** – network Ethernet port, **User1-Eth2** – user Ethernet port 1, **User2-Eth3** – user Ethernet port 2, or **All** if the management station location is not relevant).
   - Select **Link up/down trap**, and choose **On** to enable the management station to receive a trap, when a link failure (link down) or link recovery (link up) occurs. Choose **Off** to disable Link Up/Down trap receipt.

- Select **Alarm trap**, and choose **On** or **Off** to enable or disable alarm trap receipt by the manager station.
  - **On** – The alarm trap is sent to the management station informing of the occurrence of any alarm which is not masked (see *Masking Alarms* below). Both entry and exit from an alarm state are declared.
  - **Off** – The alarm trap is not sent to the management station, even if the alarm is masked.
  - Select **VLAN tagging**, and choose **On** or **Off** to consider or ignore the VLAN tagging of the management traffic coming from the management station.
  - Select **VLAN ID**, and enter the ID of the management station VLAN (**1**–**4095**).
  - Select **VLAN priority**, and enter the priority of the management station VLAN (**0**–**7**).



```
Configuration>System>Management>Manager list

1. Manager IP address              ... (0.0.0.0)
2. Manager location                >   (Empty)
3. Link up/down trap                   (On)
4. Alarm trap                          (Off)
5. VLAN tagging                        (Off)
6. VLAN ID                         ... (0)
7. VLAN priority                   ... (0)
>
Please select item <1 to 7>
ESC-prev.menu; !-main menu; &-exit                           1 Mngr/s
```

Figure D-10. Manager List Menu

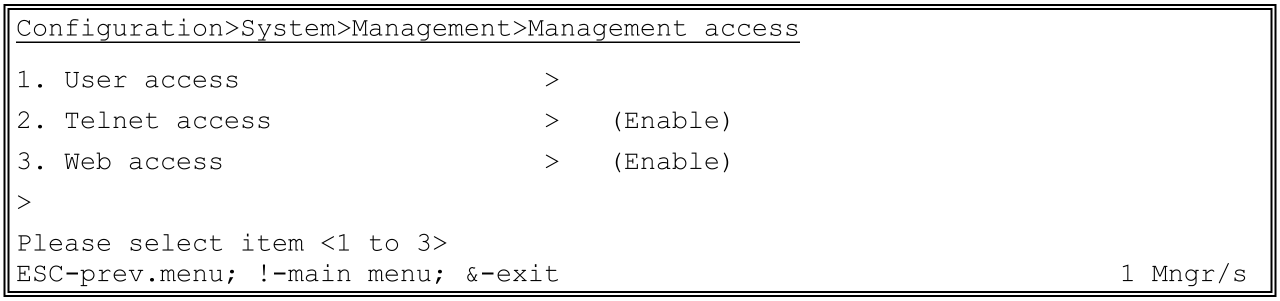
Defining Management Access

The user access rights, as well as Telnet and Web access authorization are configured via the Management Access menu.

➤ **To access The Management Access menu:**

- From the Management menu (*Figure D-7*), select **Management access**.

The Management Access menu is displayed (*Figure D-11*).



```
Configuration>System>Management>Management access

1. User access                     >
2. Telnet access                   >   (Enable)
3. Web access                      >   (Enable)
>
Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                           1 Mngr/s
```

Figure D-11. Management Access Menu

Configuring User Access

IPmux-11 management software allows you to define new users, their management and access rights. Only superusers (su) can create new users, the regular users are limited to changing their current passwords, even if they were given full management and access rights.

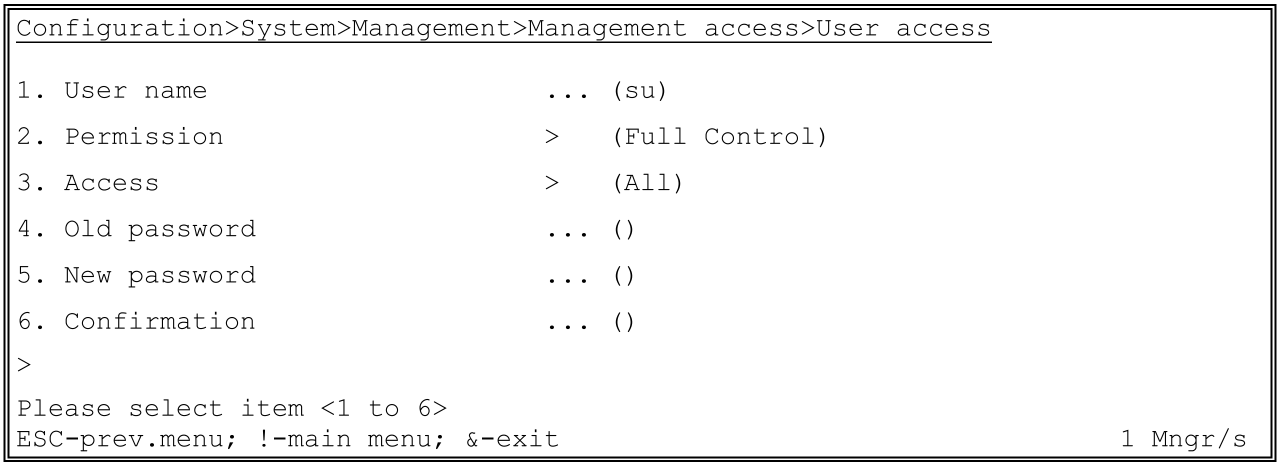
➤ **To add a new user:**

1. Make sure that you logged in as **su**.
2. From the Management Access menu, select **User access**.

   The User Access menu is displayed (see *Figure D-12*).
3. From the User Access menu, do the following:
   - Select **User name**, and enter a name for a new user.
   - Select **Permission**, and specify the user's access rights (full control or read-only).
   - Select **Access**, and specify the user's access methods (ASCII terminal, Telnet, Web browser, Telnet and Web browser, or all of them).
   - Select **Old password**, and enter your current superuser password.
   - Select **New password**, and assign a password to a new user name.
   - Select **Confirm** and re-enter the new user password to confirm it.
   - Save new settings by typing **S**, when asked.

➤ **To delete an existing user:**

- From the User Access menu, do the following:
  - Type **F** or **B** to display a user that you intend to delete.
  - Select **Old password**, and enter your current superuser password.
  - Type **D** to delete the current user.



```
Configuration>System>Management>Management access>User access

1. User name                        ... (su)
2. Permission                       >   (Full Control)
3. Access                           >   (All)
4. Old password                     ... ()
5. New password                     ... ()
6. Confirmation                     ... ()
>
Please select item <1 to 6>
ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
```

Figure D-12. User Access Menu

Controlling Telnet and Web Access

You can enable or disable access to the IPmux-11 management system via Telnet or Web-based applications. By disabling Telnet or Web, you prevent unauthorized access to the system when security of the IPmux-11 IP address has been compromised. When Telnet and Web access is disabled, IPmux-11 can be managed via an ASCII terminal only. In addition, you can allow Telnet and Web access only for the network management stations defined via the Manager List menu (*Figure D-10*).

➤ **To enable or disable Telnet and Web access:**

1. From the Management Access menu, select **Telnet access** or **Web access**.

   The Telnet Access or Web Access menu appears.

2. From the Telnet Access or Web Access menu, select **Disable** to disable access via Telnet or Web, **Enable** to enable the access, or **Managers** to allow access for the previously defined network management stations only.

Masking Alarms

You can mask any IPmux-11 alarms to prevent it from being reported to the management stations.

➤ **To mask alarms:**

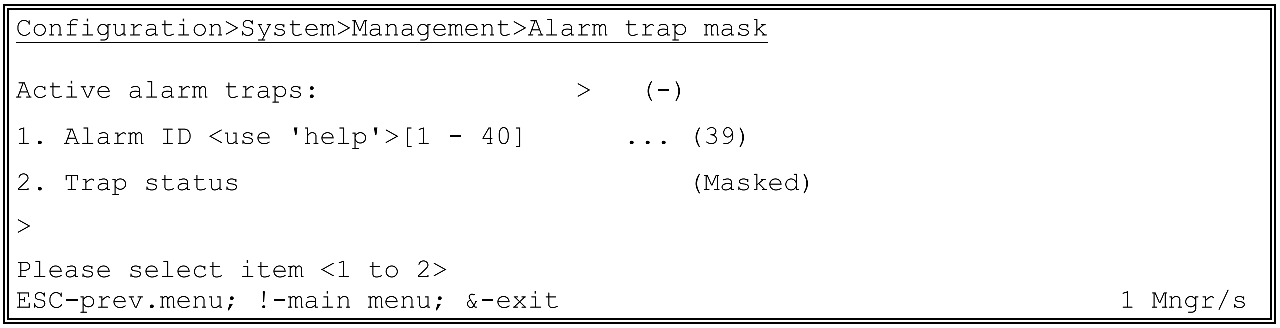
1. From the Management menu, select **Alarm trap mask**.

   The Alarm Trap Mask menu appears (see *Figure D-13*).

2. From the Alarm Traps Mask menu, select **Alarm ID** to choose alarm that you intend to mask:
   - alarmLOS
   - alarmLOF
   - alarmAIS
   - alarmRDI
   - alarmFEBE
   - alarmExtClk
   - bundleConnectionStatus.

Note *List of the alarm traps can be displayed by typing **H**.*

3. Select **Trap Status** to enable or disable masking of the selected alarm.



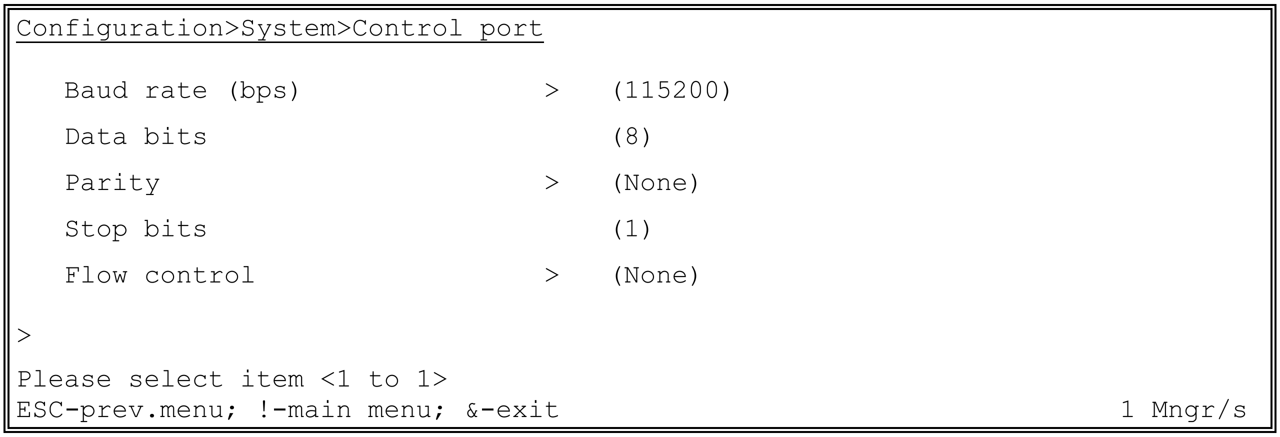
```
Configuration>System>Management>Alarm trap mask

Active alarm traps:                 >   (-)

1. Alarm ID <use 'help'>[1 - 40]      ... (39)

2. Trap status                            (Masked)

>

Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                          1 Mngr/s
```

Figure D-13. Alarm Trap Mask Menu

Control Port Parameters

Configuration parameters of the IPmux-11 control port are set at the factory and cannot be changed by the user (see *Figure D-14*). These parameters have the following values:

- Baud rate – 155200 baud
- Data bits – 8
- Parity – None
- Stop bits – 1
- Flow control – None.



```
Configuration>System>Control port

   Baud rate (bps)              >    (115200)
   Data bits                         (8)
   Parity                       >    (None)
   Stop bits                         (1)
   Flow control                 >    (None)

>
Please select item <1 to 1>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-14. Control Port Screen

Setting Date and Time

You can set the time for the IPmux-11 internal real-time clock.

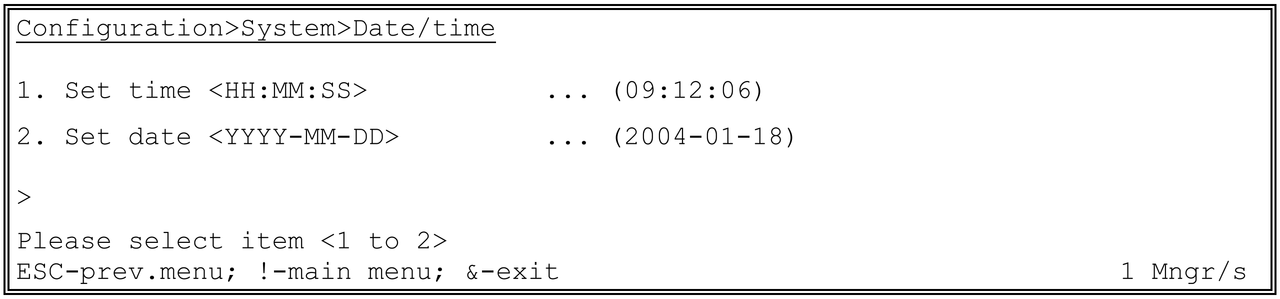
➤ **To set date and time:**

1. From the System menu (*Figure D-5*), select **Date/time**.

   The Date/Time menu appears (see *Figure D-15*).

2. From the Date/Time menu, select **Set time**, and enter the current time in the hh:mm:ss format.

3. Select **Set date**, and enter the current date in the yyyy:mm:dd format.



```
Configuration>System>Date/time

1. Set time <HH:MM:SS>          ... (09:12:06)
2. Set date <YYYY-MM-DD>        ... (2004-01-18)

>
Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-15. Date/Time Menu

D.4 Configuring IPmux-11 at the Physical Level

The TDM (E1 or T1) and Ethernet interfaces of IPmux-11 must be configured at the physical level.

Configuring the E1 TDM Interface

The E1 and T1 interfaces of IPmux-11 is configured via the TDM Configuration menu. IPmux-11 automatically detects whether the interface is E1 or T1, and displays the appropriate menu.

➤ **To configure the E1 interface:**

1. From the Configuration menu (*Figure D-4*), select **Physical layer**.

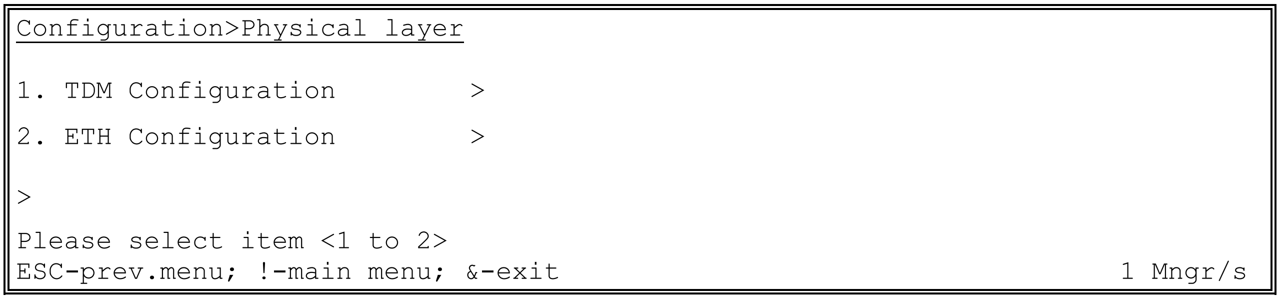
   The Physical Layer menu appears (see *Figure D-16*).

2. From the Physical Layer menu, select **TDM configuration**.

   The TDM (E1) Configuration menu appears (see *Figure D-17*).

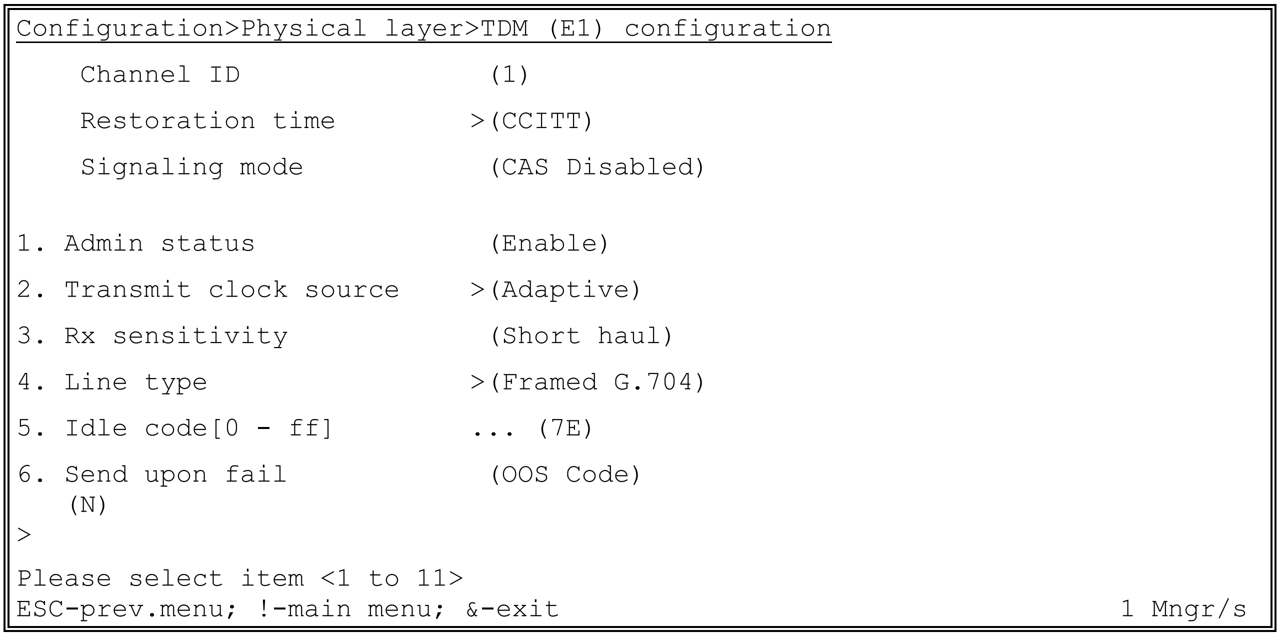
3. From the TDM (E1) Configuration menu, configure the following:
   - Admin Status:
     - **Enable** (E1 link is enabled)
     - **Disable** (E1 link is disabled)
   - Transmit clock source:
     - **Adaptive** (adaptive clock regeneration)
     - **Loopback** (E1 recovered Rx clock is used as the Tx clock)
     - **Internal** (Tx clock is received from an internal oscillator)
     - **External** (Tx clock is received from the external clock input)
   - Rx sensitivity (Maximum attenuation of the receive signal that can be compensated for by the interface receive path):
     - **Short haul** (-10 dB)
     - **Long haul** (-32 dB)
   - Line type (E1 framing mode):
     - **Unframed G.703** (Framing is not used)
     - **Framed G.704** (G.704 framing, CRC-4 function disabled)
     - **Framed G.704 CRC4** (G.704 framing, CRC-4 function enabled)
     - **Framed MF** (CAS enabled, CRC-4 function disabled)
     - **Framed MF CRC4** (CAS enabled, CRC-4 function enabled).
   - Idle Code (code transmitted to fill unused timeslots in the E1 frames): **00** to **ff**.

4. If you configure the Line type to Framed MF or Framed MF CRC4, type **N** to display the next page of E1 parameters (*Figure D-18*):
    - Send Upon Fail (Notification sent to the E1 side if Ethernet link fails):
        - **OOS Code** (Out-of-service code)
        - **AIS** (alarm indication signal)
    - OOS code (Code to be sent to the E1 side if Ethernet link fails): **0–ff**
    - OOS signaling (Out-of-service signaling method. OOS signal is sent toward the IP path when loss of signal, loss of frame, or AIS is detected at the E1 line. The OOS signal is also sent toward the E1 line when packet receive buffer overrun or underrun occur.):
        - **Space** (code specified by the Space Signaling Code parameter is sent)
        - **Mark** (code specified by the Mark Signaling Code parameter is sent)
        - **Space Mark** (space code is sent in the first 2.5 seconds, then mark code is sent)
        - **Mark Space** (mark code is sent in the first 2.5 seconds, then space code is sent)
    - Mark Signaling Code: **0–f**
    - Space Signaling Code: **0–f**
5. Type **S** to save the changes.



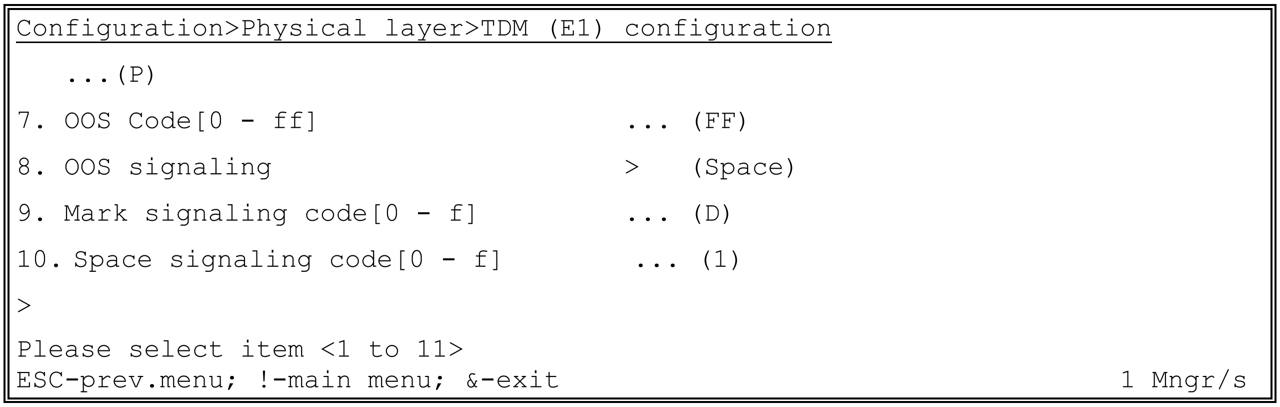
```
Configuration>Physical layer

1. TDM Configuration        >
2. ETH Configuration        >

>

Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                           1 Mngr/s
```

Figure D-16. Physical Layer Menu



```
Configuration>Physical layer>TDM (E1) configuration
    Channel ID                (1)
    Restoration time         >(CCITT)
    Signaling mode            (CAS Disabled)

1. Admin status               (Enable)
2. Transmit clock source     >(Adaptive)
3. Rx sensitivity             (Short haul)
4. Line type                 >(Framed G.704)
5. Idle code[0 - ff]         ... (7E)
6. Send upon fail             (OOS Code)
   (N)
>
Please select item <1 to 11>
ESC-prev.menu; !-main menu; &-exit                                     1 Mngr/s
```

Figure D-17. TDM (E1) Configuration Menu (Page 1)



```
Configuration>Physical layer>TDM (E1) configuration
   ...(P)
7. OOS Code[0 - ff]                   ... (FF)
8. OOS signaling                      >   (Space)
9. Mark signaling code[0 - f]         ... (D)
10. Space signaling code[0 - f]        ... (1)
>
Please select item <1 to 11>
ESC-prev.menu; !-main menu; &-exit                                     1 Mngr/s
```

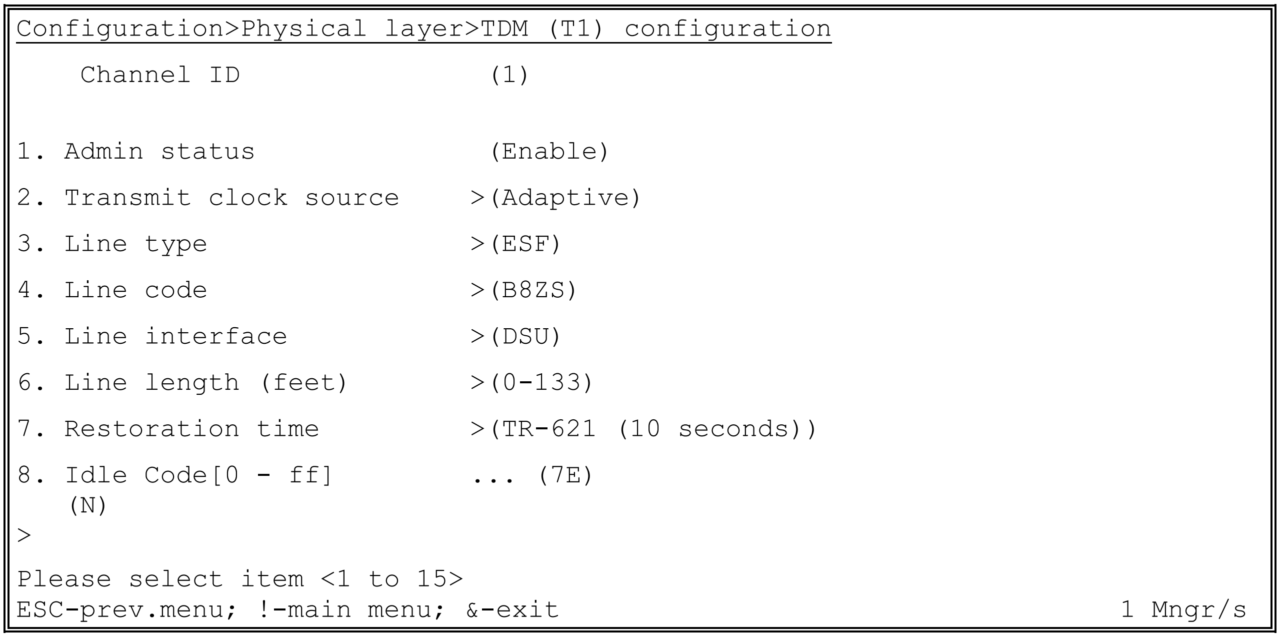
Figure D-18. TDM (E1) Configuration Menu (Page 2)

Configuring the T1 TDM Interface

The procedure for configuring the T1 port is similar to the procedure described above for configuring the E1 port. The following parameters are unique to the T1 links:

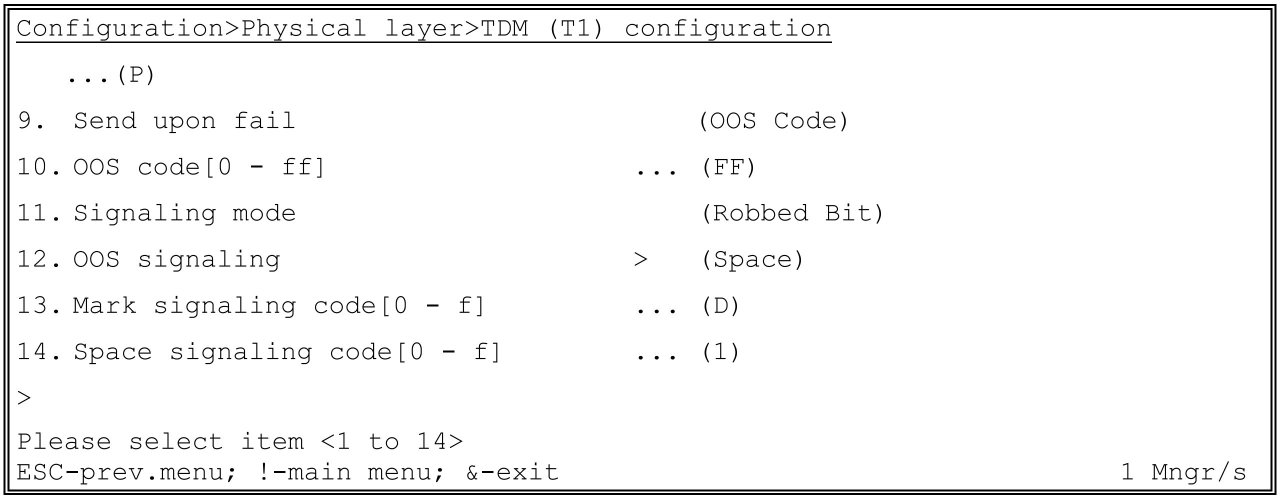
- Line type (T1 framing mode):
  - **Esf** (24 frames per multiframe)
  - **SF (D4)** (12 frames per multiframe)
- Line code (line code and zero suppression method used by the port):
  - **B7ZS**
  - **B8ZS**
  - **AMI**

- Line interface:
  - **DSU** (DSU interface)
  - **CSU** (CSU interface)
- Line length (DSU mode only, length of a cable in feet between the IPmux-11 T1 port connector and the network access point):
  - **0–133**
  - **133–266**
  - **266–399**
  - **399–533**
  - **533–655**
- Restoration time (time required for the T1 port to return to normal operation after sync loss):
    - **TR-6211 (10 seconds)**
    - **Fast (1 Second)**
  - Signaling mode:
    - **None**
    - **Robbed Bit**



```
Configuration>Physical layer>TDM (T1) configuration
    Channel ID                (1)

1. Admin status               (Enable)
2. Transmit clock source     >(Adaptive)
3. Line type                 >(ESF)
4. Line code                 >(B8ZS)
5. Line interface            >(DSU)
6. Line length (feet)        >(0-133)
7. Restoration time          >(TR-621 (10 seconds))
8. Idle Code[0 - ff]         ... (7E)
   (N)
>
Please select item <1 to 15>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-19. TDM (T1) Configuration Menu (Page 1)



```
Configuration>Physical layer>TDM (T1) configuration

   ...(P)
9.  Send upon fail                        (OOS Code)
10. OOS code[0 - ff]                  ... (FF)
11. Signaling mode                        (Robbed Bit)
12. OOS signaling                     >   (Space)
13. Mark signaling code[0 - f]        ... (D)
14. Space signaling code[0 - f]       ... (1)
>
Please select item <1 to 14>
ESC-prev.menu; !-main menu; &-exit                              1 Mngr/s
```

Figure D-20. TDM (T1) Configuration Menu (Page 2)

Configuring Ethernet Interfaces

IPmux-11 includes one network and up to two user Ethernet ports.

➤ **To configure Ethernet interface:**

1. From the Physical Layer menu (*Figure D-16*), select **ETH Configuration**.

   The ETH Configuration menu appears (see *Figure D-21*).

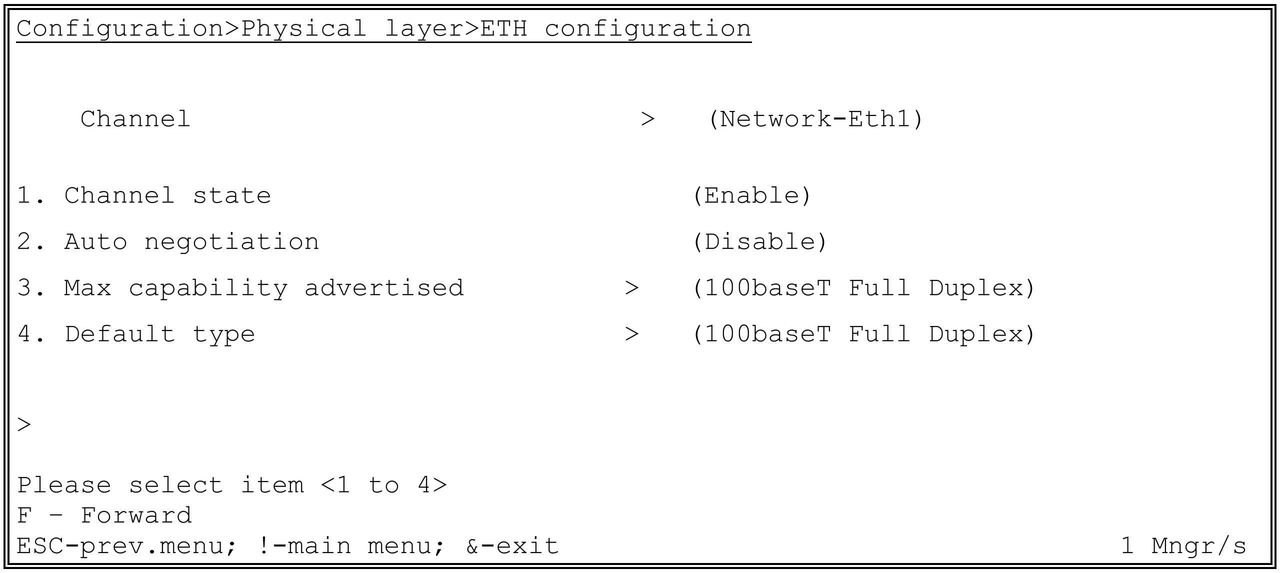
2. From the ETH Configuration menu, type **F** to select the Ethernet interface that you intend to configure (**Network-Eth1**, **User1-Eth2** or **User2-Eth3**).

3. When the required Ethernet interface is displayed, configure the following:

   - Channel state:
     - □ **Enable** (Current Ethernet interface is enabled)
     - □ **Disable** (Current Ethernet interface is disabled)
   - Auto negotiation:
     - □ **Enable** (Autonegotiation is enabled)
     - □ **Disable** (Autonegotiation is disabled)
   - Max capability advertised (Maximum capability to be advertised during the autonegotiation process):
     - □ **10BaseT Half Duplex**
     - □ **10BaseT Full Duplex**
     - □ **100BaseT Half Duplex**
     - □ **100BaseT Full Duplex**
   - Default type (Rate and duplex mode, if the autonegotiation is disabled)
     - □ **10BaseT Half Duplex**
     - □ **10BaseT Full Duplex**
     - □ **100BaseT Half Duplex**
     - □ **100BaseT Full Duplex**

Note *When autonegotiation protocols do not support each other, this will degrade the connection to a half-duplex mode. In order to avoid this, autonegotiation should be disabled and the ports should be configured manually. Half-duplex degradation will occur also when autonegotiation is enabled at one port and disabled at the opposite port.*

4. Type **S** to save your changes.



```
Configuration>Physical layer>ETH configuration


    Channel                             >    (Network-Eth1)

1. Channel state                            (Enable)
2. Auto negotiation                         (Disable)
3. Max capability advertised          >    (100baseT Full Duplex)
4. Default type                       >    (100baseT Full Duplex)


>

Please select item <1 to 4>
F - Forward
ESC-prev.menu; !-main menu; &-exit                                  1 Mngr/s
```

Figure D-21. ETH Configuration Menu

D.5 Configuring Bundle Connections

IPmux-11 supports one bundle that can include up to 31 E1 or up to 24 T1 timeslots. The bundle can be connected to any bundle of the TDMoIP device that operates opposite IPmux-11. Currently, TDMoIP traffic is sent and received via the network port only.

➤ **To configure bundle connection:**

1. From the Configuration menu (*Figure D-4*), select **Connection**.

   The Connection menu appears (see *Figure D-22*).

2. From the Connection menu, select **Bundle**, and select

3. Select **DS0 bundle configuration**.

   The DS0 Bundle Configuration menu appears (see *Figure D-23*).

4. From the DS0 Bundle Configuration, assign timeslots to the current bundle by selecting a timeslot and choosing **1** (assigned) or **0** (not assigned).

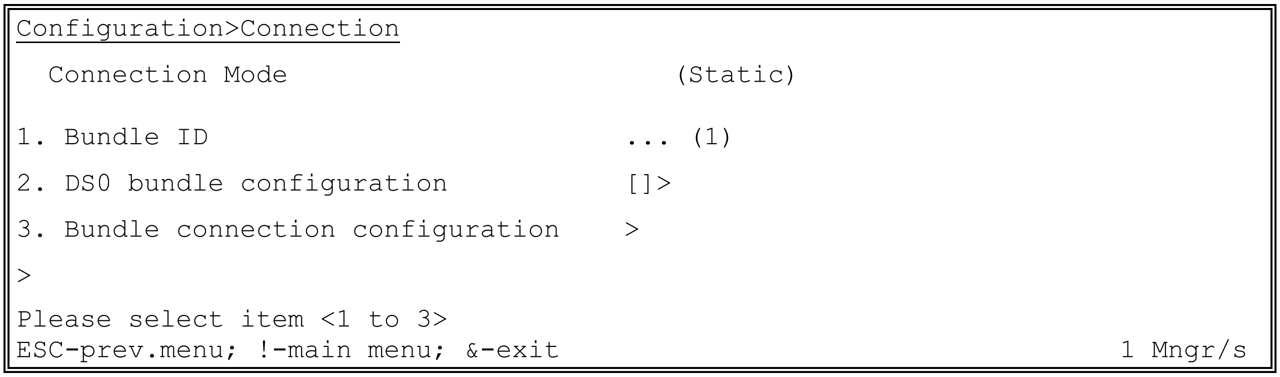
5. From the Connection menu, select **Bundle connection configuration**.

   The Bundle Connection Configuration menu appears (see *Figure D-24*).

6. From the Bundle Connection Configuration menu, configure the following:
   - IP TOS (IP ToS field in the IP frames transmitted by IPmux-11. ToS configuration configures the **WHOLE** byte, since different vendors may use different bits to tag packets for traffic prioritization. ToS assignment applies to all TDM packets leaving IPmux-11.): **0–255**.
   - TDM Bytes in Frame (x48 bytes) (UDP payload length – this parameter enables reduction of Ethernet throughput): **1–30**
   - Connection Status:
     - **Enable** (connection is enabled)
     - **Disable** (no frames are sent from this connection)
   - Destination IP Address (IP address of the destination device): **0.0.0.0** to **255.255.255.255**.
   - Next Hop (Use the next hop parameter when the destination IP address is not in the device subnet. In such cases the Ethernet frame is sent to the next hop IP. If it is not configured, the default gateway is used.): **0.0.0.0** to **255.255.255.255**.
   - Destination bundle (bundle number in the destination device): **1–2000**.
   - Jitter buffer (desired depth of the jitter (PDVT) buffer): **3–300 msec**
   - OAM connectivity:
     - **Enable** (The device starts transmitting at full rate after it detects an active, properly configured, the unit on the other side of the line.)
     - **Disable** (OAM connectivity is disabled)
   - Payload Format (TDMoIP format):
     - **Old format**
   - VLAN Tagging:
     - **Enable** (VLAN tagging is enabled)
     - **Disable** (VLAN tagging is disabled)
   - VLAN ID: **1–4095**
   - VLAN priority: **0–7**

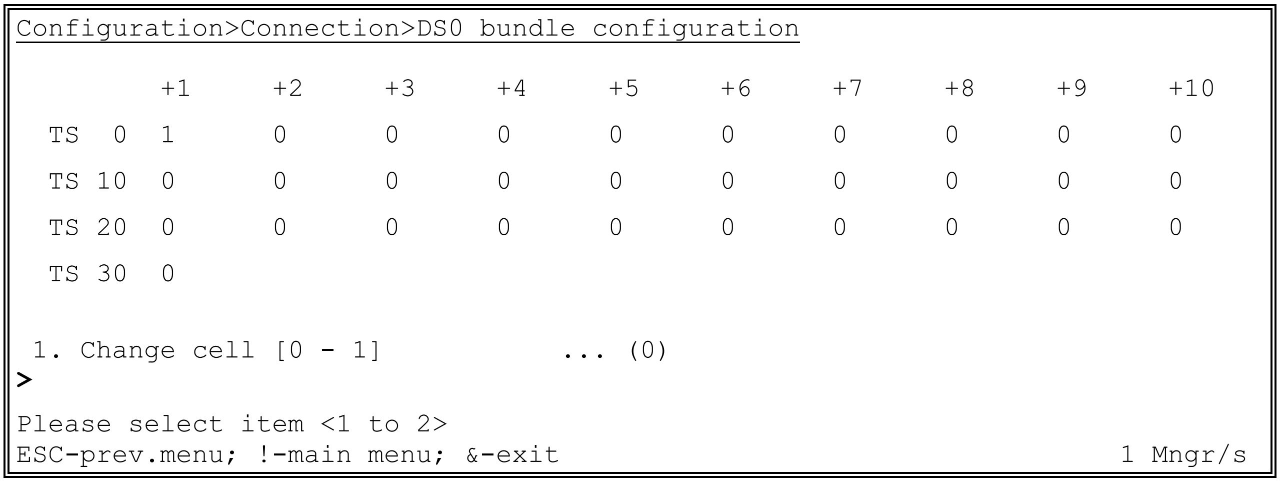
Note *Make sure that selected VLAN is configured as a member of the network port VLANs (see Configuring Ethernet Bridge below).*

7. Type **S** to save the changes.



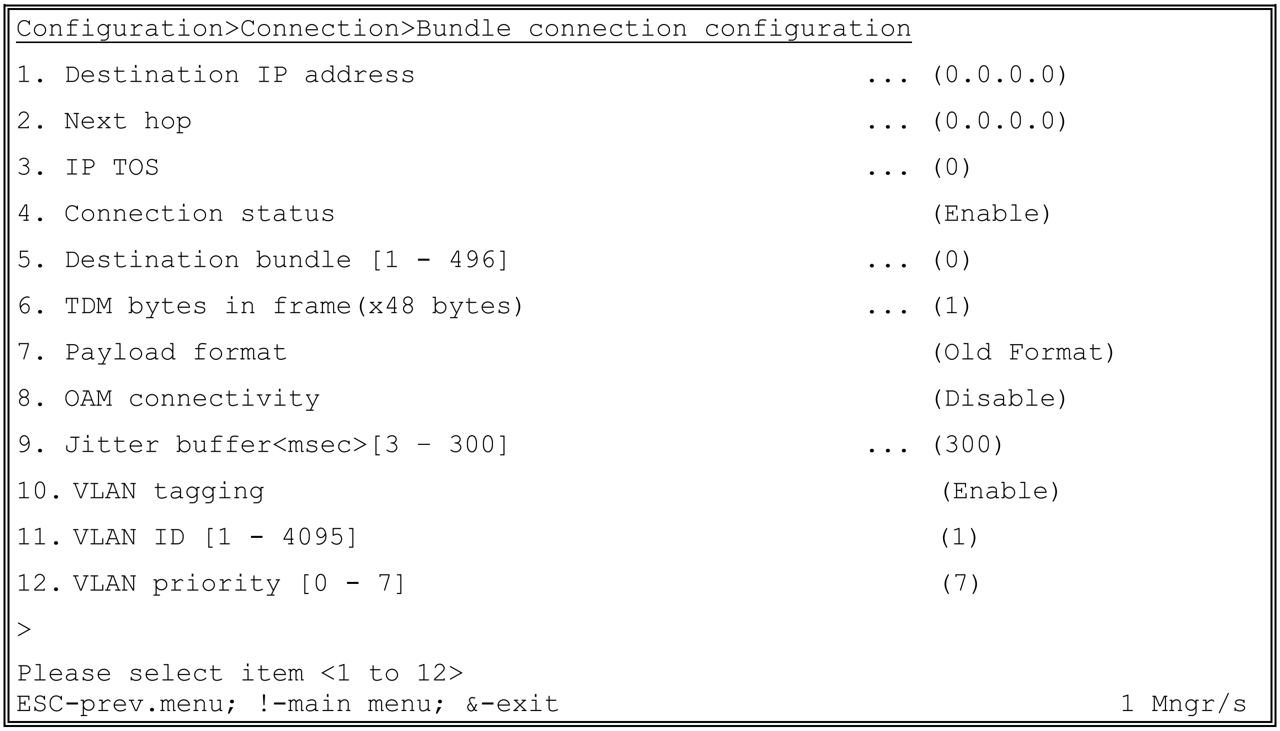
```
Configuration>Connection
  Connection Mode                       (Static)

1. Bundle ID                        ... (1)

2. DS0 bundle configuration         []>

3. Bundle connection configuration    >

>

Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                                1 Mngr/s
```

Figure D-22. Connection Menu



```
Configuration>Connection>DS0 bundle configuration

       +1     +2     +3     +4     +5     +6     +7     +8     +9     +10
  TS  0 1      0      0      0      0      0      0      0      0      0
  TS 10 0      0      0      0      0      0      0      0      0      0
  TS 20 0      0      0      0      0      0      0      0      0      0
  TS 30 0

 1. Change cell [0 - 1]           ... (0)
>
Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                                1 Mngr/s
```

Figure D-23. DS0 Bundle Configuration Menu



```
Configuration>Connection>Bundle connection configuration
1. Destination IP address                         ... (0.0.0.0)

2. Next hop                                       ... (0.0.0.0)

3. IP TOS                                         ... (0)

4. Connection status                                  (Enable)

5. Destination bundle [1 - 496]                   ... (0)

6. TDM bytes in frame(x48 bytes)                  ... (1)

7. Payload format                                     (Old Format)

8. OAM connectivity                                   (Disable)

9. Jitter buffer<msec>[3 - 300]                   ... (300)

10. VLAN tagging                                       (Enable)

11. VLAN ID [1 - 4095]                                 (1)

12. VLAN priority [0 - 7]                              (7)

>

Please select item <1 to 12>
ESC-prev.menu; !-main menu; &-exit                                1 Mngr/s
```

Figure D-24. Bundle Connection Configuration

D.6 Configuring Ethernet Bridge

IPmux-11 contains an internal bridge where one of its ports is connected to a TDMoIP interworking function, two external bridge ports is used as the user ports, and the fourth is used as an Ethernet network port.

➤ **To configure Ethernet bridge:**

1. From the Configuration menu (*Figure D-4*), select **Bridge**.

   The Bridge menu appears (*Figure D-25*).

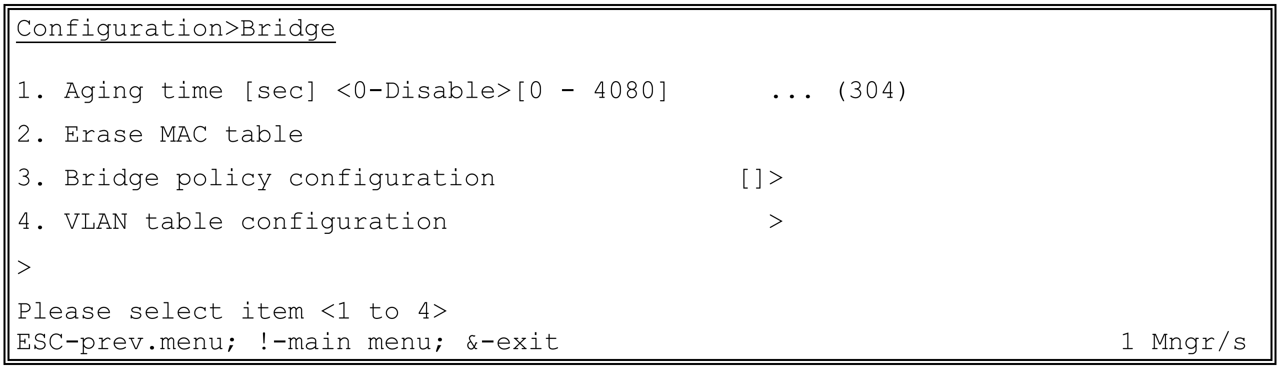
2. From the Bridge menu, select **Aging time** and define a period of time in seconds from the moment when a node is disconnected from the network segment or becomes inactive and removal of the node address from the database.

3. Select **Erase MAC table**, if you intend to delete all learned addresses from the MAC table.

4. Select **Bridge policy configuration**, and from the Bridge Policy Configuration menu (*Figure D-26*) define the following:
   - VLAN tagging (operation mode for the corresponding port of internal switch. Refer to *Ethernet Ports* in Chapter 1 for detailed explanation):
     - **Transparent**
     - **Tag** (Tagged)
     - **Untag** (Untagged)
     - **DoubleTag** (Double Tagged)
   - Default VLAN ID (VLAN associated with untagged frames arriving at the port): **1–4095**
   - Default VLAN Priority: **0–7**
   - Rate limit:
     - Network port: **Disable**, **128 kbps**, **256 kbps**, **512 kbps**, **1 Mbps**, **2 Mbps**, **4 Mbps**, **8 Mbps**
     - Network port: **Disable**, **128 kbps**, **256 kbps**, **512 kbps**, **1 Mbps**, **2 Mbps**, **4 Mbps**, **8 Mbps**, **16 Mbps**, **32 Mbps**, **64 Mbps**

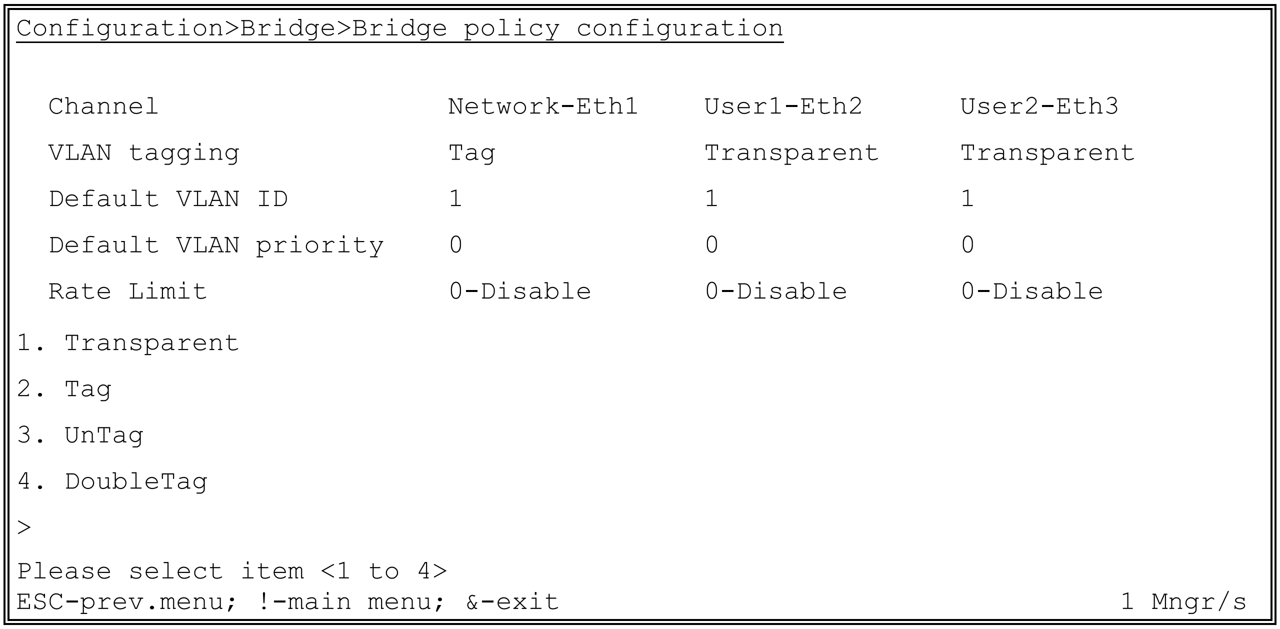
5. Select **VLAN table configuration**, and from the VLAN Table Configuration menu (*Figure D-27*) configure the following:
   - Channel:
     - **Network-Eth1**
     - **User1-Eth2**
     - **User2-Eth3**
   - VLAN ID (Selects the VLAN to edit. Creates a VLAN entry if the VLAN does not exist): **1–4095**

- Status:
  - **Enable** (Adds the current port as a VLAN member)
  - **Disable** (Disables VLAN membership of the current port)



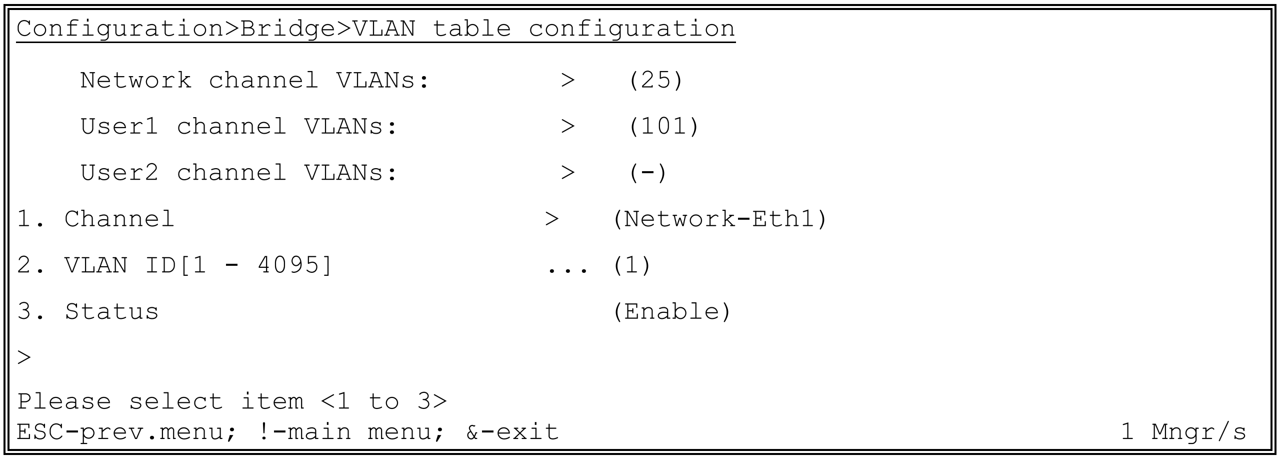
```
Configuration>Bridge

1. Aging time [sec] <0-Disable>[0 - 4080]      ... (304)
2. Erase MAC table
3. Bridge policy configuration               []>
4. VLAN table configuration                    >
>
Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-25. Bridge Menu



```
Configuration>Bridge>Bridge policy configuration

  Channel                  Network-Eth1    User1-Eth2      User2-Eth3
  VLAN tagging             Tag             Transparent     Transparent
  Default VLAN ID          1               1               1
  Default VLAN priority    0               0               0
  Rate Limit               0-Disable       0-Disable       0-Disable
1. Transparent
2. Tag
3. UnTag
4. DoubleTag
>
Please select item <1 to 4>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-26. Bridge Policy Configuration Menu



```
Configuration>Bridge>VLAN table configuration

    Network channel VLANs:        >   (25)
    User1 channel VLANs:          >   (101)
    User2 channel VLANs:          >   (-)
1. Channel                       >   (Network-Eth1)
2. VLAN ID[1 - 4095]             ... (1)
3. Status                            (Enable)
>
Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                                   1 Mngr/s
```

Figure D-27. VLAN Table Configuration Menu

D.7 Displaying IPmux-11 Status

The IPmux-11 software allows to display information on the physical layer and bundle connections. This section describes only status information of the IPmux-11 device. For description of IPmux-11 alarms, refer to *Chapter 5*.

The status information is available via the Status menu.

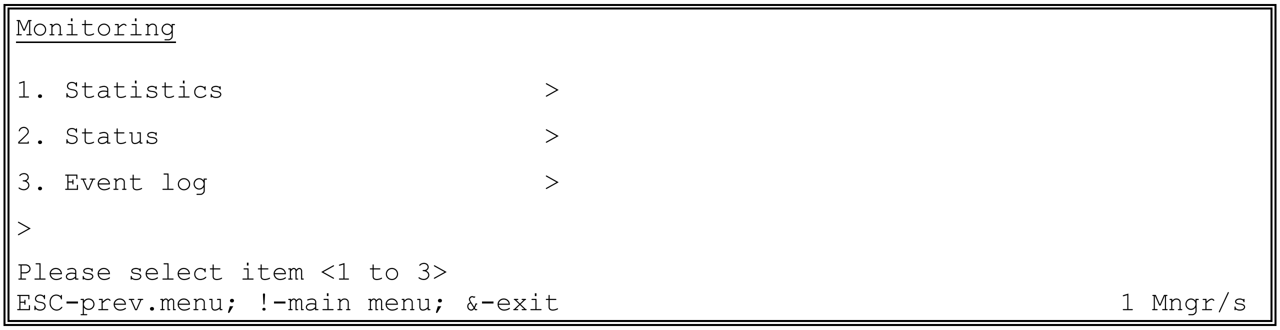
➤ **To access the Status menu:**

1. From the Main menu, select **Monitoring.**

   The Monitoring menu appears (see *Figure D-28*).

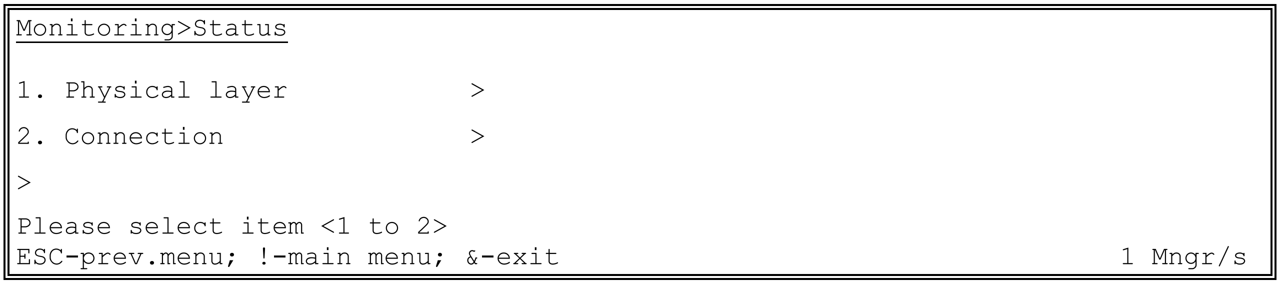
2. From the Monitoring menu, select **Status**.

   The Status menu appears (see *Figure D-29*).



```
Monitoring

1. Statistics                       >

2. Status                           >

3. Event log                        >

>

Please select item <1 to 3>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-28. Monitoring Menu



```
Monitoring>Status

1. Physical layer               >

2. Connection                   >

>

Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                                 1 Mngr/s
```

Figure D-29. Status Menu

Displaying the Physical Layer Information

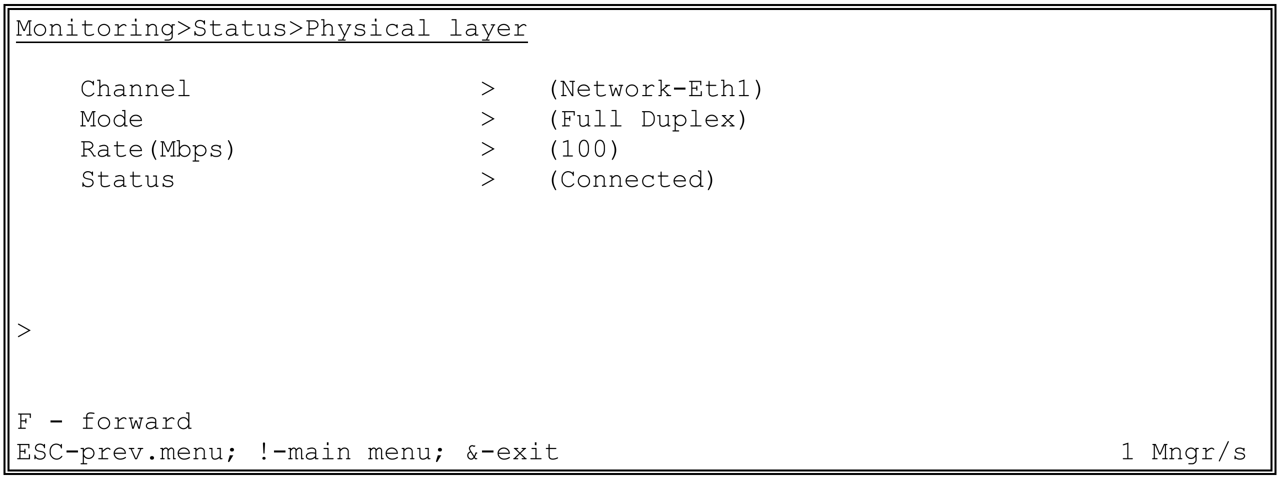
You can view the status of the Ethernet connections at the physical level.

➤ **To display the physical layer information:**

1. From the Status menu, select **Physical layer**.

   The Physical Layer screen is displayed (see *Figure D-30*).

2. From the Physical Layer screen, type **F** to toggle between the available Ethernet interfaces.



```
Monitoring>Status>Physical layer

    Channel                   >    (Network-Eth1)
    Mode                      >    (Full Duplex)
    Rate(Mbps)                >    (100)
    Status                    >    (Connected)





>




F - forward
ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
```

Figure D-30. Physical Layer Screen

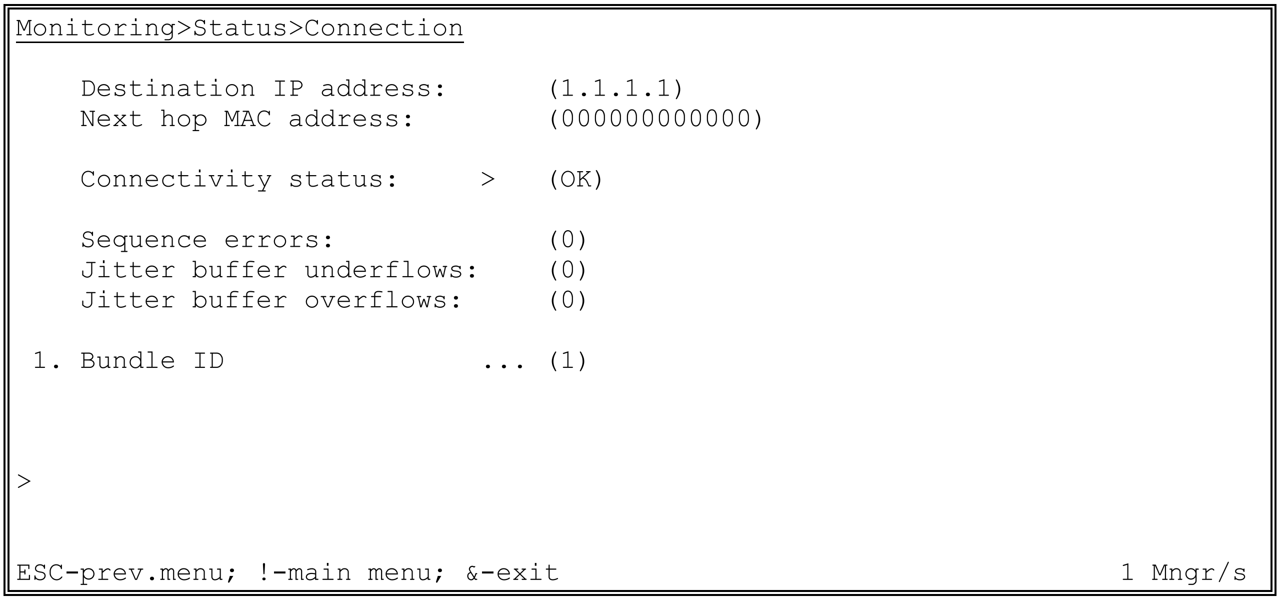
Displaying the Bundle Connection Information

You can display information on the current bundle connection, its connectivity status, collected sequence errors, and statistics for underflows and overflows of the jitter buffer (see *Chapter 4* for details on the bundle statistics).

➤ **To display the bundle connection information:**

- From the From the Status menu, select **Connection.**

The Connection screen is displayed (see *Figure D-31*).



```
Monitoring>Status>Connection

    Destination IP address:        (1.1.1.1)
    Next hop MAC address:          (000000000000)

    Connectivity status:      >    (OK)

    Sequence errors:               (0)
    Jitter buffer underflows:      (0)
    Jitter buffer overflows:       (0)

 1. Bundle ID                 ...  (1)



>




ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
```

Figure D-31. Connection Screen

D.8 Resetting IPmux-11

IPmux-11 supports two types of reset:

- Reset to the default setting
  - Resetting all parameters
  - Resetting all parameters, except for management values
- Overall reset of the device.

Resetting IPmux-11 to the Defaults

You can reset IPmux-11 to its default settings. The reset to the defaults does not affect the master clock setting. In addition, you can reset local IPmux-11 without affecting its management parameters (IP address, mask and default gateway).

➤ **To reset IPmux-11 to the default settings:**

1. From the System menu (*Figure D-5*), select **Factory default**.
2. From the Factory Default menu, perform one the following steps:
   - Select **All** to reset all IPmux-11 parameters to the default settings.
   - Select **Except Management** to reset all parameters, except for IP address, mask and default gateway values.

   IPmux-11 displays the following message:

   ```
   Configuration will be lost and System will be reset.
   Continue ??? (Y/N)
   ```
3. Type **Y** to confirm the reset.

   IPmux-11 performs the requested type of reset.

Alternatively, you can reset IPmux-11 to the defaults by pressing the SET DEF button on the rear panel.

Resetting IPmux-11

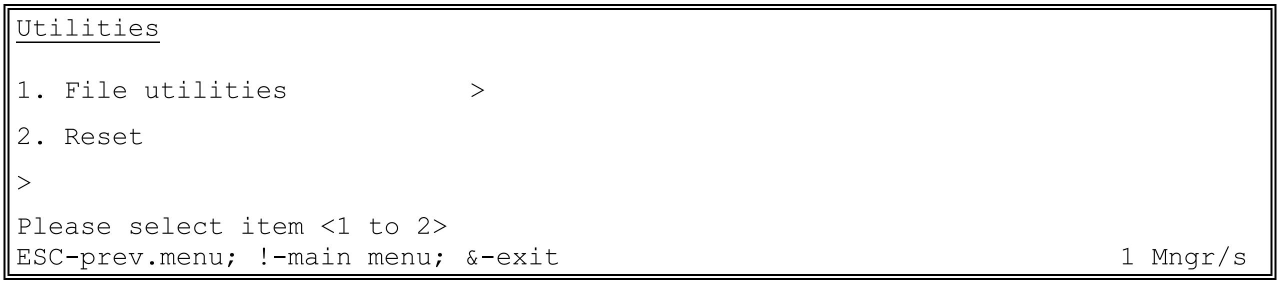
You can perform the overall reset of IPmux-11.

➤ **To reset IPmux-11:**

1. From the Main menu, select **Utilities**.

   The Utilities menu appears (see *Figure D-32*).
2. From the Utilities menu, select **Reset**.

   A confirmation message appears.
3. Type **Y** to confirm the reset.



```
Utilities

1. File utilities           >

2. Reset

>

Please select item <1 to 2>
ESC-prev.menu; !-main menu; &-exit                                    1 Mngr/s
```

Figure D-32. Utilities Menu

RAD

SUPPLEMENT

DC Power Supply Connection – AC/DC Adaptor (AD) Plug

Note: Ignore this supplement if the unit is AC-powered.

Certain units are equipped with a Wide Range AC/DC power supply. These units are equipped with a standard AC-type 3-prong power input connector located on the unit rear panel. This power input connector can be used for both AC and DC voltage inputs.

For DC operation, a compatible AC/DC Adaptor (AD) plug for attaching to your DC power supply lines is used (see *Figure 1*).

Connect the wires of your DC power supply cable to the AD plug, according to the voltage polarity and assembly instructions provided below.

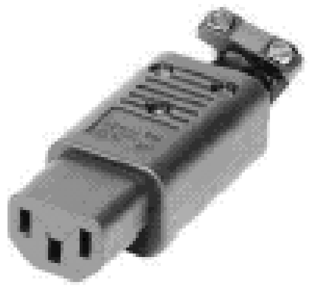


Figure 1

Caution: *Prepare all connections to the AD plug* ***before*** *inserting it into the unit's power connector.*

Preparing and Connecting the Power Supply Cable with the AD Plug

1. Loosen the cover screw on the bottom of the AD plug to open it (see *Figure 2*).
2. Run your DC power supply cable through the removable cable guard and through the open cable clamp.
3. Place each DC wire lead into the appropriate AD plug wire terminal according to the voltage polarity mapping shown. Afterwards, tighten the terminal screws close.
4. Fit the cable guard in its slot and then close the clamp over the cable. Tighten the clamp screws to secure the cable.
5. Reassemble the two halves of the AD plug and tighten the cover screw.
6. Connect the assembled power supply cable to the unit.

Warning:

- *Reversing the wire voltage polarity will* ***not*** *cause damage to the unit, but the internal protection fuse will not function.*
- *Always connect a ground (earth) wire to the AD plug's Chassis (frame) Ground terminal. Connecting the unit without a protective ground, or interruption of the grounding (for example, by using an extension power cord without a grounding conductor) can cause harm to the unit or to the equipment connected to it!*
- *The AD adaptor is not intended for field wiring.*

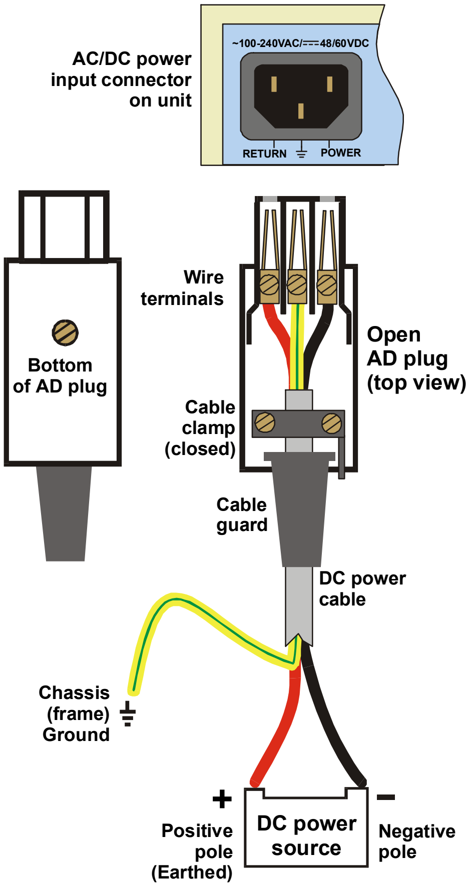


Figure 2

RAD
data communications

24 Raoul Wallenberg St., Tel Aviv 69719, Israel
Tel: +972-3-6458181, Fax: +972-3-6483331, +972-3-6498250
E-mail: erika_y@rad.com, Web site: www.rad.com

Customer Response Form

RAD Data Communications would like your help in improving its product documentation. Please complete and return this form by mail or by fax or send us an e-mail with your comments.

Thank you for your assistance!

Manual Name: IPmux-11

Publication Number: 352-200-04/04

Please grade the manual according to the following factors:

	Excellent	*Good*	*Fair*	*Poor*	*Very Poor*
Installation instructions	□	□	□	□	□
Operating instructions	□	□	□	□	□
Manual organization	□	□	□	□	□
Illustrations	□	□	□	□	□
The manual as a whole	□	□	□	□	□

What did you like about the manual?

____

____

____

____

____

Error Report

Type of Error(s)
or Problem(s):

❒ Incompatibility with product

❒ Difficulty in understanding text

❒ Regulatory information (Safety, Compliance, Warnings, etc.)

❒ Difficulty in finding needed information

❒ Missing information

❒ Illogical flow of information

❒ Style (spelling, grammar, references, etc.)

❒ Appearance

❒ Other _________

Please list the exact page numbers with the error(s), detail the errors you found (information missing, unclear or inadequately explained, etc.) and attach the page to your fax, if necessary.

____

____

____

____

Please add any comments or suggestions you may have.

____

____

____

You are:

❒ Distributor

❒ End user

❒ VAR

❒ Other ________________________

Who is your distributor? ________________________________

Your name and company: ____

Job title: ____

Address: ____

Direct telephone number and extension: ____

Fax number: ____

E-mail: ____

RAD

data communications

www.rad.com

INTERNATIONAL HEADQUARTERS:

24 Raoul Wallenberg Street, Tel Aviv 69719, Israel, Tel: 972-3-6458181
Fax: 972-3-6498250, 972-3-6474436, Email: market@rad.com

U.S. HEADQUARTERS:

900 Corporate Drive, Mahwah, N.J. 07430, Tel: (201) 529-1100
Toll Free: 1-800-444-7234, Fax: (201) 529-5777, Email: market@radusa.com

Publication No. 352-200-04/04