TDMoIP Driven®

RAD data communications

Installation and Operation Manual

IPmux-8, IPmux-16

TDM Pseudowire Access Gateways

Version 6.0

IPmux-8, IPmux-16

TDM Pseudowire Access Gateways

Version 6.0

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

North America 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. 118-200-07/06

Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the IPmux-8, IPmux-16 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-8, IPmux-16, and in no event shall RAD's liability exceed the purchase price of the IPmux-8, IPmux-16.

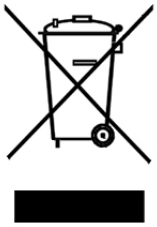
DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to IPmux-8, IPmux-16 and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the IPmux-8, IPmux-16 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-8, IPmux-16 shall not exceed the sum paid to RAD for the purchase of the IPmux-8, IPmux-16. 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.

Product Disposal



To facilitate the reuse, recycling and other forms of recovery of waste equipment in protecting the environment, the owner of this RAD product is required to refrain from disposing of this product as unsorted municipal waste at the end of its life cycle. Upon termination of the unit's use, customers should provide for its collection for reuse, recycling or other form of environmentally conscientious disposal.

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

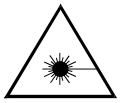
Warning

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!

In some cases, the users may insert their own SFP laser transceivers into the product. Users are alerted that RAD cannot be held responsible for any damage that may result if non-compliant transceivers are used. In particular, users are warned to use only agency approved products that comply with the local laser safety regulations for Class 1 laser products.
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.

In cases when the power distribution system is IT type, the switch must disconnect both poles simultaneously.

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.

If the DC mains are floating, the switch must disconnect both poles simultaneously.

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.

Declaration of Conformity

Manufacturer's Name: RAD Data Communications Ltd.

Manufacturer's Address: 24 Raoul Wallenberg St.
Tel Aviv 69719
Israel

declares that the product:

Product Name: IPMUX-8

conforms to the following standard(s) or other normative document(s):

EMC:	EN 55022: 1998	Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement.
	EN 55024: 1998	Information technology equipment – Immunity characteristics – Limits and methods of measurement.
Safety:	EN 60950: 2000	Safety of information technology equipment.

Supplementary Information:

The product herewith complies with the requirements of the EMC Directive 89/336/EEC, the Low Voltage Directive 73/23/EEC and the R&TTE Directive 99/5/EC. The product was tested in a typical configuration.

Tel Aviv, December 17th, 2002

Haim Karshen
VP Quality

European Contact: RAD Data Communications GmbH, Otto-Hahn-Str. 28-30,
85521 Ottobrunn-Riemerling, Germany

Declaration of Conformity

Manufacturer's Name: RAD Data Communications Ltd.

Manufacturer's Address: 24 Raoul Wallenberg St.
Tel Aviv 69719
Israel

declares that the product:

Product Name: IPMUX-16

conforms to the following standard(s) or other normative document(s):

EMC:	EN 55022 (1994)	Limits and methods of measurement of radio disturbance characteristics of information technology equipment.
	EN 50082-1 (1992)	Electromagnetic compatibility - Generic immunity standards for residential, commercial and light industry.
Safety:	EN 60950/A4 (1996)	Safety of information technology equipment, including electrical business equipment.

Supplementary Information:

The product herewith complies with the requirements of the EMC Directive 89/336/EEC and the Low Voltage Directive 73/23/EEC. The product was tested in a typical configuration.

Tel Aviv, November 5th, 2001

Haim Karshen
VP Quality

European Contact: RAD Data Communications GmbH, Otto-Hahn-Str. 28-30, 85521 Ottobrunn-Riemerling, Germany

Conventions

Note *A note draws attention to a general rule for a procedure, or to exceptions to a rule.*

Caution A caution warns of possible damage to the equipment if a procedure is not followed correctly.

Warning **A warning alerts to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the equipment. If these instructions are not followed exactly, possible bodily injury may occur.**

Quick Start Guide

Installation of IPmux-8/16 should be carried out only by an experienced technician. If you are familiar with IPmux-8/16, use this guide to prepare the units for operation.

1. Installing IPmux-8/16

Connecting the Interface Cables

1. Connect the uplink(s) to the network Ethernet port(s). On 4-port Ethernet modules networks ports designated as 1.
2. Connect the user LAN(s) to the RJ-45 connector(s) of the 4-port Ethernet modules designated 2, 3 or 4.
3. Connect TDM interfaces to the appropriate connectors of the E1, T1, E3, T3, or CT3 modules.
4. Connect the control terminal to the CONTROL DTE connector.

   or

   Connect a network management station to one of the LAN ports or CONTROL ETH connector.

Connecting the Power Cable

1. Connect the power cable to the power connector(s) on the IPmux-8/16 rear panel.
2. Set the POWER switch to the On position.

2. Configuring IPmux-8/16

Configure IPmux-8/16 to the desired operation mode via an ASCII terminal connected to the CONTROL DTE port. Alternatively, you can manage IPmux-8/16 over Telnet, or via a network management station to one of the LAN ports or CONTROL ETH connector.

Starting Terminal Session for a First Time

➤ **To start a terminal session:**

1. Connect a terminal to the CONTROL connector of IPmux-8/16.
2. Turn on the control terminal PC and set its port parameters to 19.2 kbps, 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-8/16 up and proceed with management session.

Configuring the IP Management Parameters

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

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

- From the Host IP menu (**Configuration** > **General Configuration** > **Management Configuration** > **Host Configuration**), select an IP address and subnet mask of the IPmux-8/16 hosts.

➤ **To add a network manager:**

- From the Manager List menu (**Configuration** > **General Configuration** > **Management Configuration** > **Manager List**), and enter IP parameters for the network manager station.

Configuring TDM Interfaces at the Physical Level

The TDM interfaces (E1, T1, E3, T3, CT3) must be configured at the physical level first.

➤ **To configure TDM interfaces at the physical level:**

- From the Physical Layer Configuration menu (**Configuration** > **Physical Layer Configuration**> **Slot # 3/4** > **E1**, **T1**, **E3**, **T3**, or **CT3**, **Physical Layer Configuration**), configure the necessary parameters of the appropriate TDM interface.

Configuring Bundle Connections

The E1, T1 timeslots or unframed T1s of channelized T3 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 Time Slots Configuration menu (**Configuration** > **Time slots Configuration**), assign desired timeslots to a bundle.

➤ **To connect a bundle:**

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

Contents

Chapter 3. Operation

Chapter 4. Configuration

Chapter 5. Configuring for a Typical Application

Chapter 6. Troubleshooting and Diagnostics

Chapter 1
Introduction

1.1 Overview

IPmux-8 and IPmux-16 (referred to as IPmux-8/16) are TDM pseudowire access gateways. IPmux-8/16 modules enable TDM circuits to be emulated over Packet Switched Networks (PSN). The devices convert the data stream coming from the TDM ports into configurable-sized Ethernet frames that are transported over the Ethernet port and vice versa. IPmux-8/16 offers end-to-end synchronization for TDM applications and large buffers to compensate for the delay variation inserted by the network. The devices can be used to extend TDM-based services over IP/Ethernet backbones for both Metropolitan Area Network and corporate applications. IPmux-8/16 can be managed locally via an ASCII terminal or remotely via Telnet or RADview (RAD's SNMP-based network management application).

Versions

For IPmux-8, the following interfaces are available:

- E1 interface – One or two 4-port modules, balanced or unbalanced line with RJ-45 connector
- T1 interface – One or two 4-port modules, balanced line with RJ-45 connector
- Ethernet interface – One or two 1- or 4-port Ethernet modules

For IPmux-16, the following interfaces are available:

- E1 interface – One or two 4- or 8-port modules, balanced or unbalanced line with RJ-45 connector
- T1 interface – One or two 4- or 8-port modules, balanced line with RJ-45 connector
- E3 interface – One or two single-port modules, unbalanced line with BNC connector
- T3 interface – One or two single-port modules, unbalanced line with BNC connector
- Channelized T3 interface – One or two single-port modules, unbalanced line with BNC connector
- Ethernet interface – One or two 1- or 4-port Ethernet modules.

Applications

Three typical applications are illustrated below:

- *Figure 1-1* shows IPmux-8/16 extending E1/T1-based services over IP.
- *Figure 1-2* shows enterprise connectivity over campus or Metropolitan Area Networks.
- *Figure 1-3* shows IPmux devices managed by the RADview Network Management System.

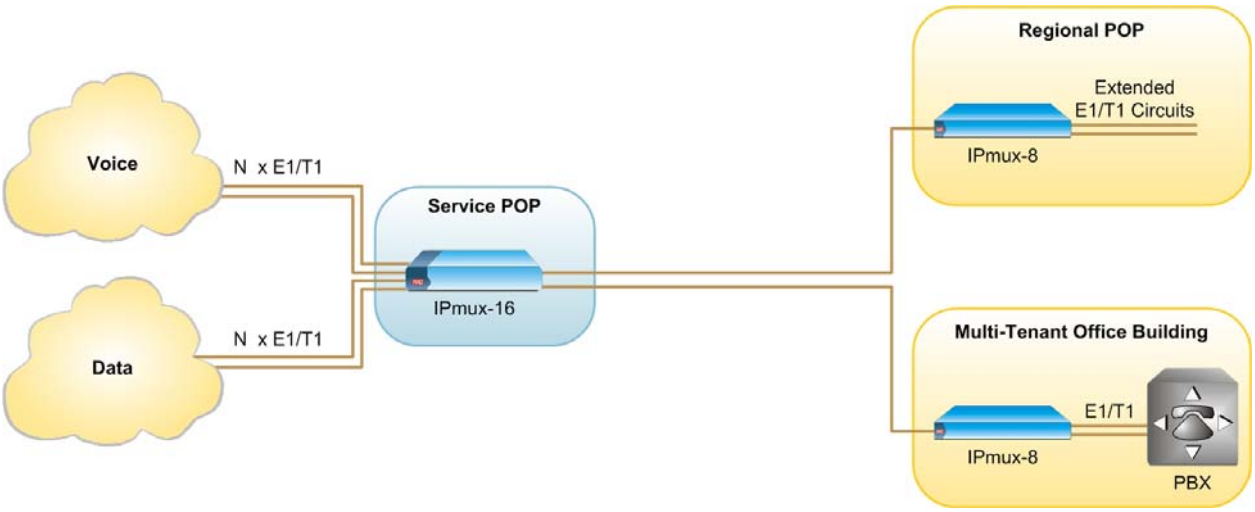


Figure 1-1. Extending E1/T1-Based Services over IP

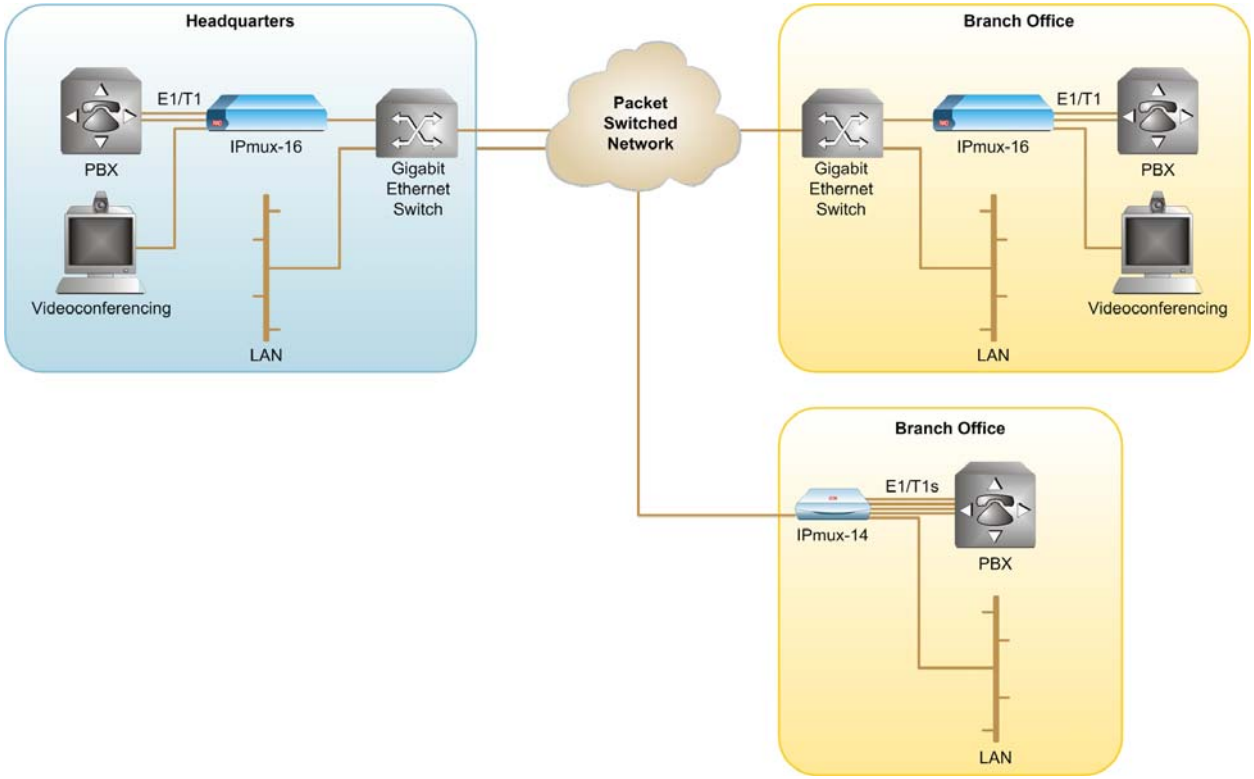


Figure 1-2. Enterprise Connectivity over Campus or Metro Area Networks

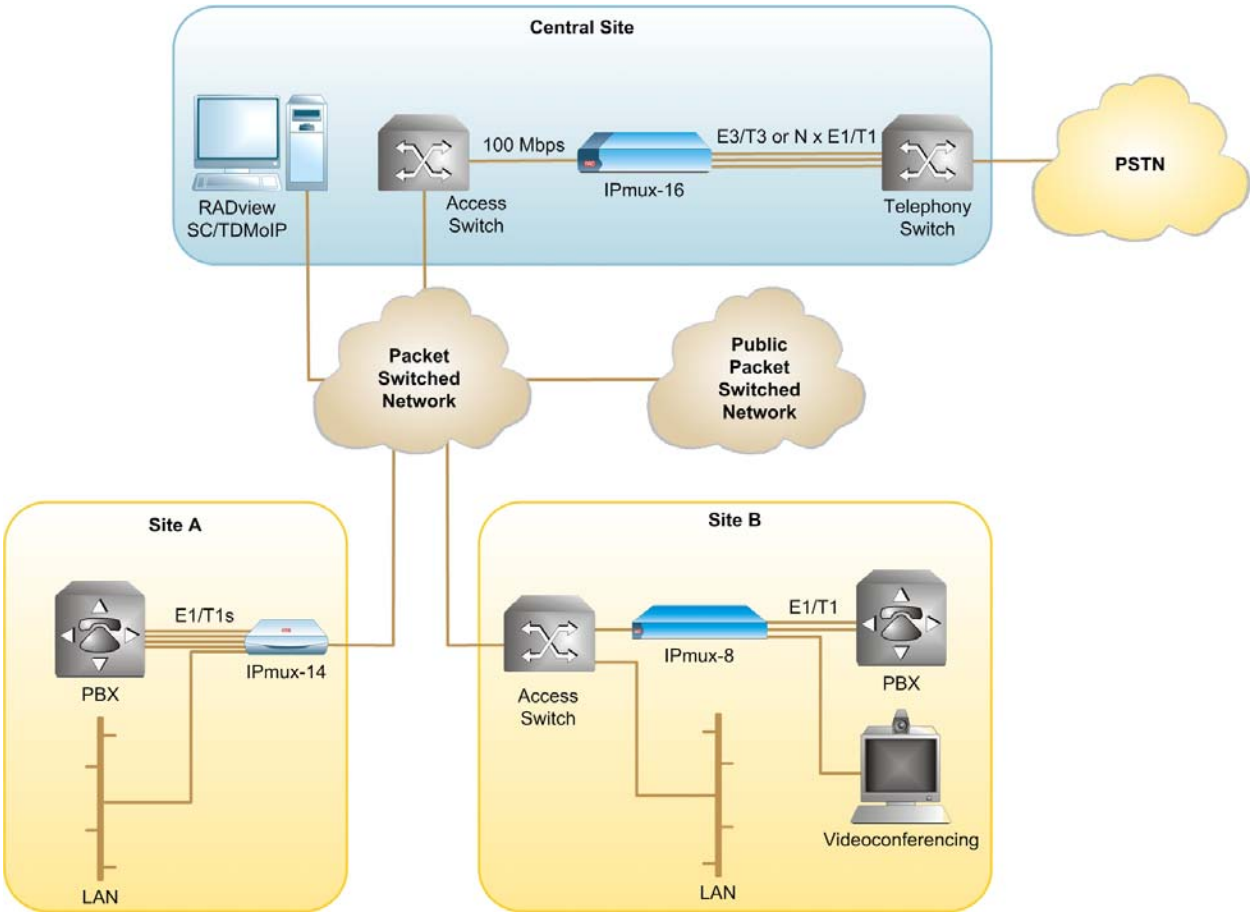


Figure 1-3. IPmux Devices Managed by RADview Network Management System

Features

E1/T1 frames or DS0 bundles are transported over the network based on IP addressing. E3/T3/CT3 ports and framers are available for IPmux-16.

Ethernet link redundancy to the network is supported when IPmux-8/16 is equipped with two Ethernet modules. The unit supports one or two 1- or 4-port Ethernet modules. The 4-port Ethernet modules include three user ports with L2 switch and rate limiter, and one 10/100BaseT or 10/100BaseFx uplink port. The 4-port Ethernet modules perform VLAN-aware or transparent bridging.

IPmux-8/16 supports three operation modes for E1/T1: unframed, fractional E1/T1, and fractional E1/T1 with CAS.

Multibundling can be performed for up to 31 bundles per E1 port and 24 bundles per T1 port, for transport over the network. Both mesh and star topologies are supported.

IPmux-8/16 allows an internal cross-connect of bundles between its E1 or T1 ports.

IPmux-8/16 supports VLAN tagging and priority labeling according to 802.1 p&Q. The Type of Service (ToS) of outgoing TDMoIP packets is user-configurable.

IPmux-8/16 maintains synchronization between TDM devices by deploying advanced clock distribution mechanisms. The clocking options are: internal, loopback, adaptive, and external (for IPmux-16).

IPmux-8/16 complies with the TDMoIP protocol.

Management

IPmux-8/16 can be managed via a local terminal, Telnet, or via RADview, RAD's Network Management system. IPmux-8/16 has a DB-9 port for the local terminal connection for monitoring and control. Software upload/download can be performed via the local terminal, using the XMODEM protocol.

E1 Modules

The E1 modules comply with G.703, G.704, and G.823 standards. E1 framers comply with G.704. The E1 modules support unframed, framed and multiframed operation with or without CRC-4. The E1 modules support long haul and short haul input signals and can be monitored for alarms and error statistics.

T1 Modules

The T1 modules comply with ANSI T1.403, G.703, and G.704 standards. T1 jitter performance is according to G.824 and TR-62411. The T1 modules support unframed, SF, ESF and Robbed Bit signaling. The T1 modules support 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.

E3 Modules

E3 modules (only for IPmux-16) comply with G.703 and G.823 standards. The E3 TDMoIP service is for full E3 and is fully transparent to E3 framing (framers in passthrough mode).

T3 Modules

T3 modules (only for IPmux-16) comply with ANSI T1.102 and Bellcore TR-NWT-000499 standards. The T3 TDMoIP service is for full T3 and is fully transparent to T3 framing (framers in passthrough mode).

CT3 Modules

Channelized T3 (CT3) modules (only for IPmux-16) comply with the following standards:

- Telcordia GR-253, GR-499
- ANSI T1.102, T1.404
- ITU-T G.703, G.755, G.824, G.151
- AT&T TR54014

The main purpose of CT3 modules are to convert the T3 TDM service signals into 28 unframed T1s and assign each of them to a TDMoIP bundle to be sent over Ethernet/IP/MPLS networks.

The CT3 module provides:

- Increased IPmux-16 T1 capacity - up to 56 T1 channels (28 × 2) on a single chassis – two CT3 modules in the same chassis
- Transmission of up to 28 bundles per CT3 card – each bundle containing an unframed T1 as per G.703
- Point-to-point and point-to-multipoint topologies
- Local cross connect between CT3 internal T1 channels
- External/Internal loop functions on CT3/internal T1 levels
- Detection of LOF (per ESF/SF framing) on the CT3 internal T1 channels (log file only).

IP

The data stream coming from the TDM ports is converted into IP packets and transferred over the Fast Ethernet port, and vice versa.

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

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

A destination IP address should be configured for each TDMoIP flow, i.e. E1, T1, E3, T3, CT3 or timeslot bundle (see *Multibundling*). IP ToS field support can be configured for IP Level Priority.

4-Port Ethernet Module

The 4-port Ethernet module of IPmux-8/16 includes four Fast Ethernet ports: one network port (10BaseT, 100BaseTx or 100BaseFx) and three user ports (10/100BaseT).

Network Ethernet Ports

The IPmux-8/16 Ethernet network ports operate in half or full duplex, providing autonegotiation and auto-crossover. The network ports support QoS, tagged frames (IEEE 802.1p), ToS (IPv4), RMON statistics, tagging/untagging per port or by IEEE 802.3q VLAN ID.

User Ethernet Ports

The IPmux-8/16 Ethernet user ports operate in half or full duplex, providing autonegotiation and auto-crossover. The network ports support QoS (determined by port), tagged frames (IEEE 802.1p), TOS (IPv4), RMON statistics, tagging/untagging per port or by IEEE 802.3q VLAN ID, double tagging per port, ingress rate limiting per port (128 kbps to 64 Mbps).

Transparent Bridging

Two 4-port Ethernet modules support up to two totally separated transparent bridges. The bridges performs automatic learning and aging, supporting up to 2000 MAC addresses per Ethernet module with VLAN 802.1p transparency.

VLAN-Based Bridging

VLAN-based bridging is performed in according to IEEE 802.1Q requirements. Up to 64 VLANs are supported per 4-port Ethernet module. At ingress the bridge supports tagged, priority-tagged and untagged frames.

1-Port Ethernet Module

The 1-port Ethernet module includes one full duplex Ethernet network port with autonegotiation support.

If autonegotiation is disabled, IPmux-8/16 can be configured to any of the following:

- 100BaseT: full duplex
- 10BaseT: full duplex

IPmux-8/16 supports VLAN ID and priority tagging (per 802.1p&Q).

A different VLAN can be configured for each TDMoIP flow so that operation over a pure Layer 2 network is supported (see *Multibundling*).

Ethernet redundancy backs up TDMoIP traffic if there is a failure in the Ethernet link.

The IP addresses for two Ethernet modules of IPmux-8/16 can belong to the same subnet. This allows you to connect two Ethernet cards in the same Ethernet network.

Note *You cannot have a manager on any host with an IP address that belongs to another host's subnet.*

Default Next Hop per Host

You can configure a default next hop for every Ethernet interface. Every bundle mapped to that Ethernet link uses this as its default next hop.

The Ethernet module has the following features:

- Reordering out-of-sequence packets arriving at IPmux-8/16 from the packet network – IP networks may send packets in incorrect order or duplicate IP packets; this creates a problem for TDMoIP traffic. The Ethernet card is able to reorder up to 32 packets, depending on the TDM Bytes/frame size and jitter buffer size. The formula, below, calculates the number of packets that can be reordered by the IPmux-8/16 as a function of TDM bytes/frame and jitter buffer size:

$$\text{Max Reordered Packets} = \frac{(\text{Jitter\_Buffer\_[ms]} - 1) \times (\text{Number\_of\_TS} \times 8)}{(47 \times \text{Number\_of\_TDM\_bytes\_per\_frame})/48}$$

Note *The Packet Reordering mechanism and the Duplicate Packets Handling mechanism operate only for the first bundle number in each E1/T1 port (e.g. for devices with E1 ports, bundles number 1, 32, 63, 94, etc.).*

- Total Transmitted Packet per Second (pps) – a previous IPmux-16 Ethernet module had a limitation on the total transmitted packet per second (pps) rate (see *Throughput Limitations and System Usage Control*). This limitation is not relevant for the current Ethernet card.
- Larger Ethernet frame size support (see *Throughput Limitations and System Usage Control*).
- Fiber optic Ethernet uplink – two ordering options for the Ethernet uplink interface are available, in addition to the regular electrical interface:
  - Electrical Ethernet uplink
  - Fiber optic single-mode Ethernet uplink
  - Fiber optic multi-mode Ethernet uplink.

Download (DL) Transparent

It is possible to determine whether the Channel Service Unit (CSU) Loop Code (upstream/downstream) is handled locally or transmitted to its parallel far-end channel via the packet-switched network. The CSU/DSU performs protective and diagnostic functions for the telecommunications line.

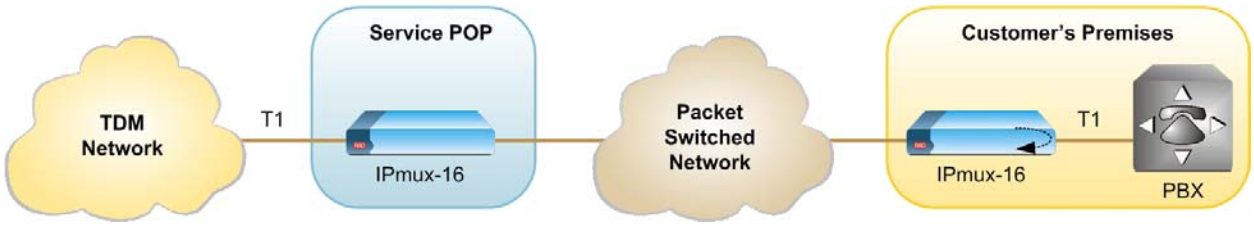


Figure 1-4. DL Transparent

Operation Modes for E1/T1

There are three operation modes for E1/T1:

- Unframed
- Fractional E1/T1
- Fractional E1/T1 with CAS

Multibundling

A bundle is a group of timeslots originating from a specific E1 or T1 channel. Up to 31 bundles per E1 channel and 24 bundles per T1 channel can be defined for transport over the network. Each bundle can contain 1 to 24/31 timeslots (T1/E1 respectively).

Note *It is recommended to configure up to 85 TDMoIP bundles for optimal agent operation. Up to 85 TDMoIP bundles can be handled before any degradation in management access is noticed.*

Two network topologies are supported:

- **Star (point-to-multipoint):** Multiple remote locations transport one bundle each to a central site that is capable of grooming the bundles into its E1 or T1 channel (see *Figure 1-7*).
- **Mesh:** Any-to-any connectivity is supported at the bundle (DS0) level (see *Figure 1-8*).

Internal Cross-connect

IPmux-8/16 allows for internal cross-connect of bundles between its E1/T1/CT3 ports.

QoS

QoS support:

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

You 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-8/16 traffic for delay-sensitive and secure applications. IPmux-8/16 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 you to work according to various RFC definitions (for example, RFC 2474, RFC 791). The user can also configure VLAN priority bits for Level 2 Priority.

Timing

IPmux-8/16 maintains synchronization between TDM devices by deploying advanced clock distribution mechanisms.

Available timing modes are:

- Loopback
- Adaptive
- Internal
- External (only for IPmux-16).

Standards

IPmux-8/16 follows the standards: G.703, G.704, G.706, G.823, ANSI T1.102, ANSI T1.403, Bellcore GR-499, TR-AT&T62411, G.824, IEEE 802.3, IEEE 802.3D, IEEE 802.1 p&Q.

Power

IPmux-8/16 can be ordered with dual redundant AC or DC power supplies.

IPmux-16 only

The following features are for IPmux-16 (not present in IPmux-8):

- External clock
- E3/T3/CT3 ports
- Out-of-band management via CONTROL ETH port.

1.2 Physical Description

IPmux-8 and IPmux-16 are compact, easily installable standalone units. Rack mounting kits are available.

Figure 1-5. IPmux-8 3D View

Figure 1-6. IPmux-16 3D View

The control port and indicator LEDs are located on the front panel of IPmux-8/16. For further details, see *Chapter 3*.

Fuses, power supplies, and interface connectors are located on the rear panel of IPmux-8/16. For further details, see *Chapter 2*.

The dry contact connector is located on the front panel of IPmux-8 and on the rear panel of IPmux-16.

1.3 Functional Description

IPmux-8/16 Ethernet modules connect the device to the network. Configuration and management are provided via the IPmux-8/16 local terminal, Telnet application, or SNMP such as RADview, RAD's network management system.

IPmux-8/16 modules support E1/T1 interfaces. E1/T1 bundles, composed of several timeslots (1–31 for E1, 1–24 for T1), can be defined. Each bundle can be connected to a different destination bundle anywhere on the network (see *Figure 1-7*). In addition, IPmux-16 units with channelized T3 TDM interfaces supports up to 28 bundles with one unframed T1 per bundle.

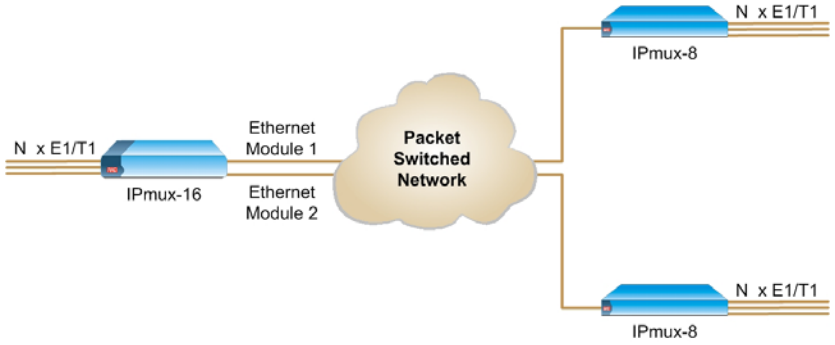


Figure 1-7. IPmux-8/16 Point-to-Point Application

Up to 85 sub-E1 or 85 sub-T1 remote bundles can be attached to one central IPmux-8/16. Multibundling enables concentrating many remote sites with few timeslots to the same TDM channel at the central site. A mesh topology application, in which the bundles at each site are defined to connect to several sites, is also supported (see *Figure 1-8*).

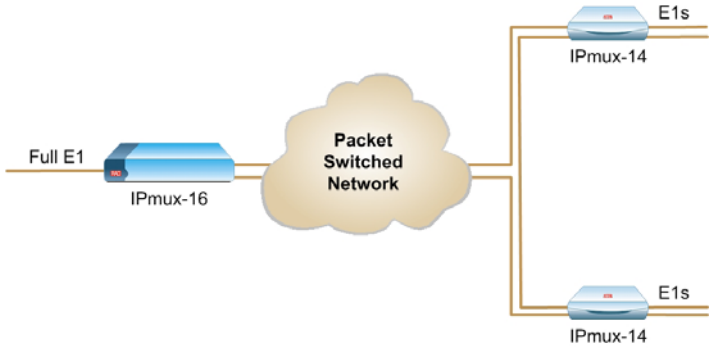


Figure 1-8. Grooming of Timeslots from Remote Sites into a Single E1/T1 Port at Central Site

Operation Modes

IPmux-8/16 operation modes for E1/T1 are:

- Unframed
- Fractional
- Fractional with CAS.

Note *For IPMux-16 with E3/T3 TDM interfaces, unframed is the only operation mode.*

Unframed

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

Framed

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 UDP/IP frames and transmitted.

This mode allows transmission of several selected time slots and not the whole E1/T1 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).

Testing

Diagnostic capabilities include local and remote loopback tests for rapid location of faults. Any of the ports can be looped locally toward the line, or toward the remote end (see *Chapter 6* for more information).

Timing Modes

The TDM Data Transmit (Tx) clock operates in several timing modes, to provide maximum flexibility for connecting the IPmux-8/16 TDM interface.

The available timing modes are:

- **Loopback clock** – the TDM Tx clock is derived from the receive (Rx) clock.
- **Adaptive clock** – the TDM 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 (toward the TDM device) decreases to avoid underflow.

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

- **Internal clock** – the Tx clock is received from an internal oscillator.
- **External clock** (IPmux-16 only) – the Tx clock is taken from the external clock input (ordering option). For CT3, there is an additional option to take the timing from an internal T1 line, as long as this T1 port is in adaptive mode. The other T1 lines can take their timing from this T1.

Notes

- *E3/T3 cannot use external clock as a clock source.*
- *The input signal **on the external clock port** is repeated and is available on the TD outputs in order to allow feeding other devices with the clock source signal.*
- *The output clock in the external clock port is not locked on the input clock. This is why RAD does not recommend using a concatenated cable to daisy chain the clock.*

Each of the clocks must be configured correctly on both the receive and transmit ends to ensure proper operation and prevent pattern slips.

The following paragraphs describe typical timing schemes and their correct timing mode settings in order to achieve end-to-end synchronization.

External Network Timing

E1/T1

When an external network is used to synchronize the E1/T1 devices, all the IPmux-8/16 units should be configured to work in loopback mode (see *Figure 1-9*).

This topology enables any-to-any connectivity; in *Figure 1-9* all three IPmux-8/16 units have direct E1/T1 connectivity. In this timing configuration both mesh and star bundle connection topologies are supported.

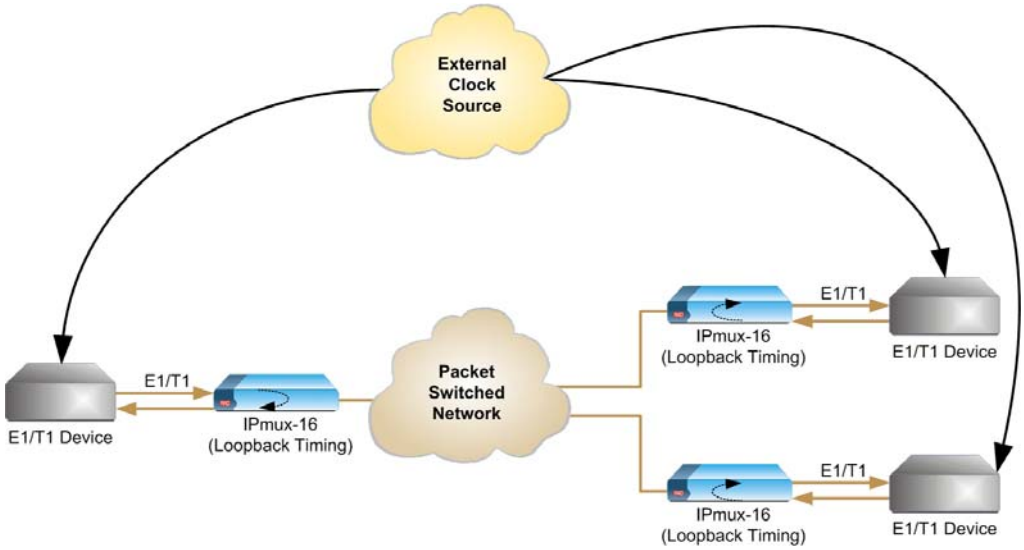


Figure 1-9. IPmux-8/16 in Loopback Timing Mode – E1/T1

External timing from the network can also be issued to IPmux-8/16 by external clock input; in this case the E1/T1 device will use LBT mode (see *Figure 1-10*).

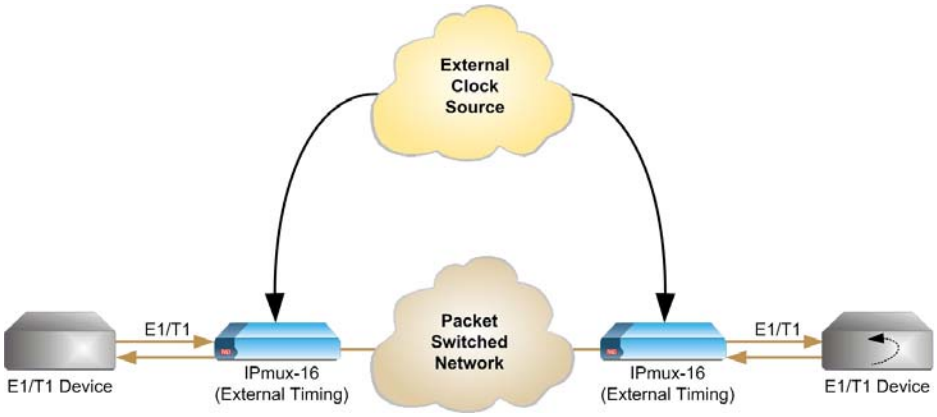


Figure 1-10. IPmux-8/16 in External Clock Mode – E1/T1

E3/T3

Note *Only IPmux-16 has E3/T3 ports.*

This topology enables point-to-point connectivity; in *Figure 1-11* both IPmux-16 units have direct E3/T3 connectivity. In this timing configuration both mesh and star bundle connection topologies are supported.

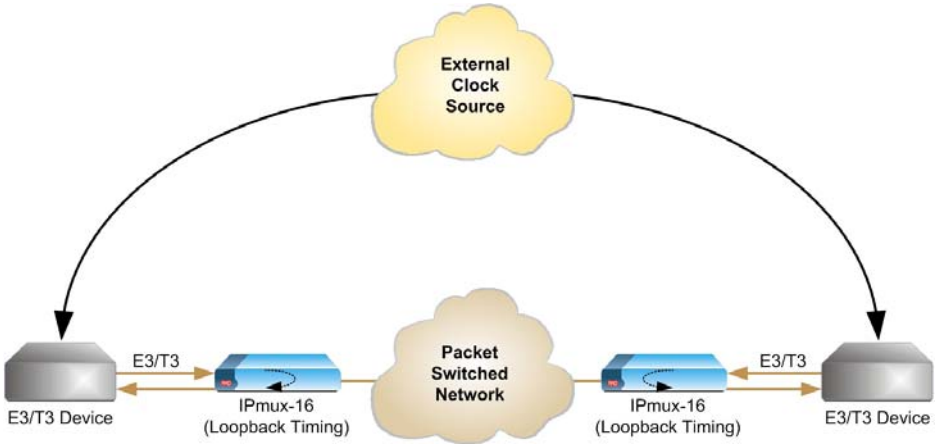


Figure 1-11. IPmux-16 in Loopback Timing Mode – E3/T3

Single Source Clock Network

Figure 1-12 illustrates an application when a common clock is not available on all the ends of the network:

- **E1/T1 Device Configuration:**
  One of the E1/T1 devices connected to IPmux-8/16 (or E3/T3/CT3 connected to IPmux-16) should work as the master clock while the other or others work in loopback timing.
- **IPmux-8/16 Configuration**:
  The IPmux-8/16 ports connected to the master clock device work in loopback timing, while the far-end IPmux-8/16 units work in adaptive mode.

Note *For E1/T1, when there are several bundles from different sources at the same E1/T1 port, the bundle that is used for adaptive clock regeneration for the port is the first bundle of every port. For example (E1): Bundle number 1 for port 1, bundle number 32 for port 2, bundle number 63 for port 3, bundle number 94 for port 4, etc. In this mode the regenerated clock is subject to network Packet Delay Variation and may not comply with jitter and wander specifications.*

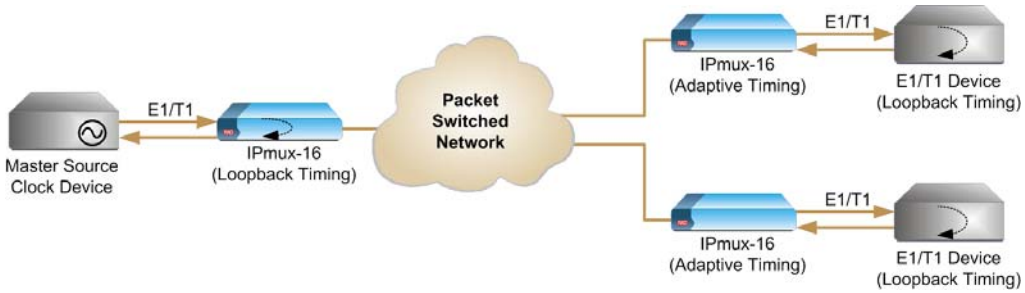


Figure 1-12. IPmux-8/16 in Adaptive Timing Mode – E1/T1

Figure 1-13. IPmux-16 in Adaptive Timing Mode – E3/T3

Bundle Redundancy

IPmux-8/16 features a bundle redundancy capability. This feature enables the user to backup the TDMoIP traffic in case of the bundle connection or TDM interface failure. This feature enables the user to set different paths for the primary bundle and for the secondary bundle (different IP networks, different links, different IPmux units, etc) and thus rely on two routes, which are not influenced by the same faulty IP/Ethernet conditions.

The redundancy type supported is 1:1 mode: only one bundle is actually transmitted towards the network while the secondary bundle is on standby.

This mode has a negligible effect on the throughput, but the recovery time of the system, in case switch/flip occurs, depends on the network elements involved in the application. In 1:1 mode IPmux-8/16 sends Keep Alive frames (called OAM) on the standby bundle in order to keep the path active (update tables entries, etc).

Note *For IPmux-16 units with an E3, T3 or CT3 interface bundle redundancy is available if the E3, T3 or CT3 interface module is installed in slot 3.*

Frame Format

The Ethernet frame sent by the IPmux-8/16 is a UDP datagram that transfers E1/T1 payload bytes over IP over Ethernet (UDP payload + CW + UDP header + IP header + Ethernet header).

The UDP payload size is equal to TDM bytes per frame (TDM bytes/frame configuration).

The illustration below specifies the structure of the different headers, special fields, and the payload in the Ethernet packet.

Figure 1-14. TDMoIP Frame Structure

Table 1-1. TDMoIP Frame Structure

	Field Length	Field	Notes
MAC Layer	7 bits	Preamble	
	1 bits	SFD	
	6 bytes	Destination MAC Address	
	6 bytes	Source MAC Address	
LLC Layer	2 bytes	Type	IEEE 802.1p&Q VLAN Tagging (additional 4 bytes if enabled)
IP Layer	1 byte	Vers/HLEN	
	1 byte	Service Type	
	2 bytes	Total Length	
	2 bytes	Identification	
	1 byte	Flags/Fragment Offset (most)	
	1 byte	Fragment Offset (least)	
	1 byte	Time to Live	
	1 byte	Protocol	
	2 bytes	Header Checksum	
	4 bytes	Source IP Address	
	4 bytes	Destination IP Address	
UDP Layer	2 bytes	UDP Source Port	The UDP source port field is used to transfer a destination bundle number. See *Note* below.
	2 bytes	UDP Destination Port	
	2 bytes	UDP Message Length	
	2 bytes	UDP Checksum	

Table 1-1. TDMoIP Frame Structure (Cont.)

	Field Length	Field	Notes
Control Word	4 bits	FORMID	Format Identifier: AAL1, AAL2, HDLC etc
	1 bit	R Bit	Indicates Local loss of Synchronization at the opposite TDM side
	1 bit	R Bit	Indicates that the opposite TDMoIP device is not receiving packets at the Ethernet port
	4 bits	RES	Reserved
	6 bits	LENGTH	TDMoIP packet length (CW and payload). Used when total packet length is less than 64 bytes. Otherwise is set to 0.
	16 bits	Sequence number	Used by the receiving IPmux to detect packet loss
Data Layer	...	Payload	
MAC Layer	4 bytes	CRC	

Note

The UDP Source Port value calculation depends on the selected TDMoIP version (1 or 2):

- *TDMoIP version 1:*
  - *During normal operation the UDP Source Port value equals* ***Destination Bundle Number + 1*** *(for example, for bundle 1 the UDP Source Port equals 2). The allowed range for the UDP Source Port values in the normal state is from 0 to 8191.*
  - *If a bundle is in the local fail state, the MSB of the UDP Source Port is set to 1 to indicate the local fail state to the remote equipment. In this case the UDP Source Port value equals* ***0x8000 + Destination Bundle Number + 1****. The UDP Source Port value in the local fail state is always greater than 32768.*
- *TDMoIP version 2: The UDP Source Port value equals* ***0x2000 + Destination Bundle Number****, it is always greater than 8192.*

VLAN Support

IPmux-8/16 can be configured with or without VLAN support. If VLAN is selected, then all the traffic originating from IPmux-8/16 must have 802.1 p&Q Ethernet frame format. IPmux-8/16 supports service levels of traffic separation to different VLANs. Every TDMoIP bundle has its own VLAN ID configuration.

VLAN, according to IEEE 802.1p&Q, adds four bytes to the MAC layer of the Ethernet frame. The contents of these bytes: MAC layer priority and VLAN ID, can be set by the user. In this mode, only VLAN format frames are sent and received by IPmux-8/16. The following figure describes the VLAN tag format.

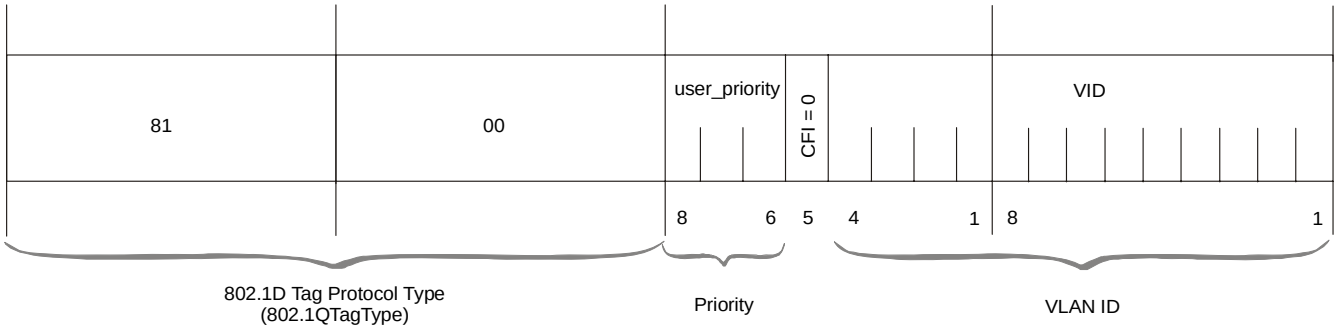


Figure 1-15. VLAN Tag Format

VLAN Groups

Every TDMoIP bundle (circuit) can be assigned a specific VLAN ID and VLAN Priority. In addition, IPmux supports a different VLAN ID for each Manager- so that only Managers that are included in the Manager List that transmit frames with the correct VLAN ID, will be processed by IPmux-8/16.

Ping

IPmux-8/16 supports ping (ICMP) from the device console to any other device on the network with a configured VLAN ID. It checks if the ping destination is one of the configured IP destinations; otherwise is uses the default configured VLAN ID.

Packet Delay Variation

TDMoIP packets are transmitted by IPmux-8/16 at a constant rate towards the PSN (Packet-Switched Network). Packet Delay Variation is the maximum deviation from the nominal time the packets are expected to arrive at the far end device. IPmux-8/16 has a jitter buffer that compensates for the deviation from the expected packet arrival time to ensure that the TDM traffic is sent to the TDM device at a constant rate.

The jitter buffer needs to be configured to compensate for the jitter level introduced by the PSN. If the PSN jitter level exceeds the configured jitter buffer size, underflow/overflow conditions occur, resulting in errors at the TDM side.

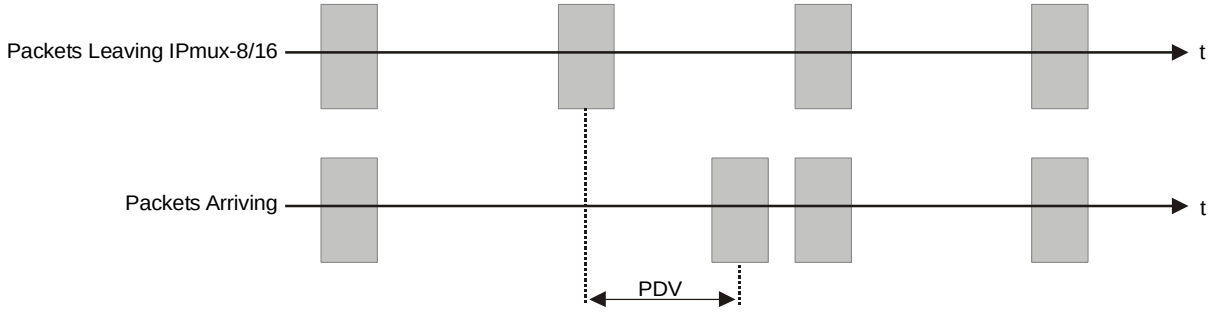


Figure 1-16. Packet Delay Variation

PDVT (Jitter) Buffer

IPmux-8/16 is equipped with a Packet DVT (Delay Variation Tolerance) buffer. The PDVT buffer or jitter buffer is filled by the incoming packets and emptied out to fill the TDM stream.

- A jitter buffer overrun occurs when it receives a burst of packets that exceeds the configured jitter buffer size + packetization delay. When an overrun is detected, IPmux-8/16 clears the jitter buffer, causing an underrun.
- A jitter buffer underrun occurs when no packets are received for more than the configured jitter buffer size, or immediately after an overrun.

When the first packet is received, or immediately after an underrun, the buffer is automatically filled with conditioning pattern up to the PDVT level in order to compensate for the underrun. Then, IPmux-8/16 processes the packet (packetization delay) and starts to empty out the jitter buffer to the TDM side. See *Figure 1-17* for the illustration of the PDVT buffer operation.

The PDVT (jitter) buffer is designed to compensate for the following network delay variation:

- E1: 32 msec
- T1: 24 msec
- E3/T3: 29 msec (IPmux-16 only)
- CT3: 42 msec (IPmux-16 only).

PDVT Buffer Effect on Delay

Packets arriving from the PSN side are stored in the jitter buffer before being transmitted to the TDM side, adding a delay to the TDM traffic. The delay time equals to the jitter buffer size configured by the user.

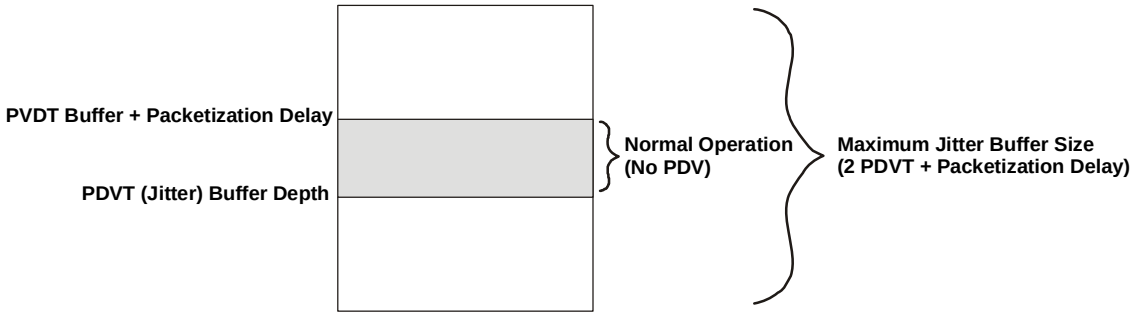


Figure 1-17. Jitter Buffer Operation

Packetization Delay

When IPmux-8/16 builds a frame, a packetization delay is introduced. The packetization delay is calculated according to the following formula:

$$\text{Packetization delay (ms)} = \frac{47 \times N \times 0.125}{TS}$$

Where:

$$N = \frac{\text{TDM bytes/frame}}{48}$$

TS = number of assigned timeslots (in unframed mode= 32 for E1, 24 for T1)

Note *For a bundle that contains a few timeslots (i.e. 1 to 3), the recommended number of TDM bytes/frame is 48 in order to prevent excessive packetization delay.*

Round Trip Delay

The voice path round-trip delay introduced by IPmux-8/16 is calculated as follows:

$$\text{Maximum Round Trip Delay } (\mu s) = 2 \times [(\frac{48 \times n}{NTS} \text{ x } 125\ \mu s) \times 2 + \text{PDVT buffer } (\mu s) + 1 \text{ msec}]$$

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

For framed E1/T1 NTS = number of assigned timeslots
For unframed:

E1: NTS = 32

T1: NTS = 24

E3: NTS = 537

T3: NTS = 699

Note

- $\frac{48 \times n}{NTS}$ *x 125 μs is packetization delay*
- *1 msec is end-to-end internal processing delay introduced by IPmux-8/16 (Rx – 0.5 msec, Tx – 0.5 msec)*
- *In real-life applications the PSN always introduce some delay that must be added to the RTD calculations. There is no network delay when IPmux-8/16 devices operate back-to-back.*

Ethernet

OAM

OAM is used to detect validity of the endpoint configuration and connection between them.

When IPmux-8/16 is powered up or a connection is opened/enabled, TDMoIP traffic is not sent immediately. First, a TDMoIP echo request packet is sent once every five seconds. This continues until a valid echo reply arrives. The remote IPmux receives the echo request packet, checks or answers it only if the destination bundle of the echo request message exists in the receiving end, and the connection is enabled. The remote IPmux sends a valid echo reply only if all parameters in the echo request match its local configuration. When a valid echo reply arrives, the transmitting echo request message stops, and TDMoIP flow begins at full rate. If there is a break in the connection, the initialization process begins again.

Ethernet Redundancy

With two Ethernet modules, IPmux-8/16 supports Ethernet redundancy to back up TDMoIP traffic if there is a failure in the Ethernet line. The system assigns the same IP and MAC addresses to each Ethernet interface, so that if a failure occurs, the data and management traffic will automatically switch to the second Ethernet module. The switching is transparent to the remote IPmux, and the switches and routers in the network. Ethernet redundancy provides a backup for the link and module.

Note *Enabling or disabling Ethernet redundancy can result in erasing all bundle configurations, depending on the CES card arrangement. Refer the table below for more exact information.*

Table 1-2. Ethernet Redundancy Modes

Slot 1	Slot 2	Slot 3	Slot 4	Switching from Ethernet Redundancy Mode	
				DIS→ENA	ENA→DIS
Ethernet	Ethernet	4/8 x E1/T1	---	Bundle configuration remains	Bundle configuration remains
Ethernet	Ethernet	---	4/8 x E1/T1	Bundle configuration remains	Bundle configuration erases
Ethernet	Ethernet	4/8 x E1/T1	4/8 x E1/T1	Bundle configuration erases	Bundle configuration erases
Ethernet	Ethernet	E3/T3 (IPmux-16 only)	---	Bundle configuration remains	Bundle configuration remains
Ethernet	Ethernet	---	E3/T3 (IPmux-16 only)	Bundle configuration remains	Bundle configuration erases

Note

- *8 ×E1/T1 CES card is available only for IPmux-16.*
- *Ethernet redundancy is not possible when two E3 or T3 modules are installed.*

Load Sharing

When IPmux-8/16 includes two Ethernet modules, the TDM data can be divided between them, so that there is a smaller load on each network link. The TDM data from slot 3 is mapped to the Ethernet module installed in slot 1, and the TDM data from slot 4 is mapped to slot 2.

Internal Switch Operation Modes

4-port Ethernet modules of IPmux-8/16 offer up to three user ports in addition to the network port. 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.

Note *When processing traffic IPmux-8/16 switch utilizes four queues for frame forwarding. This is why the switch combines VLAN priority into four groups 0–1, 2–3, 4–5, 6–7, preserving the initial hierarchy (frames with 0–1 priority are forwarded before frames with 2–3 priority).*

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 by a lower-rate device 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 1-3. Rate Limiter Options

Network Interface (Egress)	User Interface (Ingress)
256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 10 Mbps, 16 Mbps, 20 Mbps, 25 Mbps, 40 Mbps, 50 Mbps, 80 Mbps	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 1-4* lists all operation modes of the network and user ports. The modes are explained in greater detail in *Table 1-5*, *Table 1-6*, *Table 1-7*, *Table 1-8*, *Table 1-9*, *Table 1-10* and *Table 1-11*.

Table 1-4. 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 1-5. 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 1-6. 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 transparen*t 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 1-7. 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 1-8. 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 1-9. 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 1-10. 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 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 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 1-11. Mode G

Ingress	Egress
If a double-tagged frame enters the transparent port, it is switched to the double-tagged port	• If the double-tagged port is not a member of the first VID of the frame, the frame is discarded • If the double-tagged port is a member of the first VID of the frame, it removes the firs tag and transmits the frame tagged.
If a tagged frame enters the transparent port, it is switched to the double-tagged port	• If the double-tagged port is not a member of the frame VID, the frame is discarded • If the double-tagged port is a member of the frame VID, it removes the tag and transmits the frame untagged
If an untagged frame enters the transparent port, the frame is discarded	
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)

Note *When operating in the Mode G, the following rules apply:*
- *No VLANs can be created on the network port.*
- *Each user port has to be a member of its default VLAN ID, no other VLANs are valid.*
- *Both user ports can get the same default VLAN ID.*
- *In either case, no traffic is allowed between two user ports.*

Throughput Limitations and System Usage Control

Note *For IPmux-16 with CT3 modules only.*

Every Ethernet interface can handle a limited packet per second (pps) capacity. This limitation may be reached only when using a CT3 card. IPmux-16 deploys a System Usage Control mechanism that prevents configurations that will exceed the pps. This mechanism also monitors and displays current system performance optimization (percentage of budget in use). If the system usage is 80%, the system does not allow you to configure another bundle on this Ethernet card.

Ethernet Throughput

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

You can configure the TDM bytes/frame parameter in N × 48 bytes, where N is an integer from 1 to 30 (for E1/T1 or CT3) or 5 to 30 (for E3/T3).

If you configure TDM bytes/frame to a higher value, you will reduce the IP/Ethernet overhead segment of the total packet, and thus can significantly reduce the total Ethernet throughput.

On the other hand, packetization delay are increased; this contributes to a higher end-to-end delay. This effect can be small and negligible when full E1 (or many timeslots) is transferred but can be very significant when few E1/T1 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. The tables below show the throughput as a function of the TDM bytes/frame configuration for full E1 and full T1.

TDMoIP Calculator supplied on the TDMoIP technical documentation CD can be used for the following calculation:

- ETH/IP/MPLS bandwidth consumption,
- Packet per second rate
- Packetization delay,
- Maximum number of re-ordered packets
- End-to-end IPmux delay.

IPmux-16 with Two E3/T3 Cards

As the bandwidth for delivering two E3 or T3 over IP is more than 100 Mbps, two Ethernet modules are needed to support two E3 or T3 TDMoIP modules. Each of the Ethernet modules is used as an uplink to one of the E3/T3 ports. The Ethernet module at slot number 1 is used as the uplink to the E3/T3 module at slot number 3; the Ethernet card at slot number 2 is used as the uplink to the E3/T3 module at slot number 4.

End-to-End Alarm Generation

An end-to-end alarm generation mechanism exists in IPmux-8/16 to facilitate the following alarms:

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

Default Gateway Configuration

IPmux-8/16 supports a default gateway configuration. Normally, the default gateway should be on the subnet where the user wants to manage IPmux-8/16.

Management

IPmux-8/16 is designed for unattended operation. The IPmux-8/16 configuration (the complete collection of its operating parameters) is determined by a database stored in non-volatile memory. The database is automatically loaded when you power-up IPmux-8/16, thereby enabling IPmux-8/16 to automatically return to its last operating configuration.

The IPmux-8/16 management, as well as the other configuration, test, and monitoring activities (equipment status reading, alarm status and history, activation of test loops, reading of performance statistics, etc.) can be performed in three ways:

- **Inband Management**: Management traffic can run over the same network as the TDMoIP data. IPmux-8/16 can be managed via an Ethernet module in Slot 1 or Slot 2, or both.
- **Out-of-Band Management:** IPmux-16 can have a dedicated Ethernet port for management. This port is used when management is required to run over a separate network. It is obtained via the Control connector in the front panel.
  - **SNMP Management** – The SNMP management capability enables fully graphical, user-friendly management using the RADview network management stations offered by RAD, as well as management by other SNMP-based management systems.
  - **Telnet** – Remote management is also possible using the Telnet communication protocol, which uses TCP/IP communication, without SNMP service.
  - **Local Management**: IPmux-8/16 can be managed locally via the terminal, using the control DTE port. A “dumb” ASCII terminal connected to an RS-232 port of IPmux-8/16 (or a PC running a terminal emulation program), controlled by the program stored in IPmux-8/16, can be used as a supervision terminal. The terminal can also be connected through a modem link, to enable dial-in from a remote location. IPmux-8/16 supports both point-to-point and multidrop locations.

1.4 Technical Specifications

E1 Modules

Number of Ports	• IPmux-8: 4 per module • IPmux-16: 4 or 8 per module
Compliance	ITU-T Rec. G.703, G.706, G.732, G.823
Connector	Balanced: RJ-45 8 pin Unbalanced: TBNC 75Ω (an external adapter cable from TBNC to BNC is required)
Data Rate	2.048 Mbps
Line Code	HDB3
Line Impedance	Balanced: 120Ω; Unbalanced: 75Ω
Signal Levels	Receive: 0 to -32 dB with LTU 0 to -10 dB without LTU Transmit Balanced: ±3V ±10% Transmit Unbalanced: ±2.37V ±10%
Jitter Performance	ITU-T G.823 standard
External Adapter Cable	TBNC to BNC required for unbalanced interfaces
Compliance	G.704, G.706
Framing	Pass through, CRC4 MF, CAS MF
Signaling	CAS, CCS (transparent)

T1 Modules

Number of Ports	• IPmux-8: 4 per module • IPmux-16: 4 or 8 per module
Compliance	ANSI T1.403, ITU-T Rec. G.703
Connector	RJ-45, 8 pin
Data Rate	1.544 Mbps
Line Code	B8ZS, B7ZS, AMI
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 without CSU
Jitter Performance	AT&T TR-62411, G.824 standards
Compliance	ANSI T1.403

	Framing	Passthrough, SF, ESF
	Signaling	CAS (bit robbing), CCS (transparent)
E3 Module (IPmux-16)	*Number of Ports*	1 per module
	Compliance	G.703, G.823
	Connector	BNC
	Data Rate	34.368 Mbps
	Line Code	HDB3
	Line Impedance	Unbalanced 75Ω
	Jitter performance	According to G.823
	Framing	Unframed
T3 Module (IPmux-16)	*Number of Ports*	1 per module
	Compliance	ANSI T1.102
	Connector	BNC
	Data Rate	44.736 Mbps
	Line Code	B3ZS
	Line Impedance	Unbalanced 75Ω
	Jitter Performance	According to Bellcore TR-NWT-000499
	Framing	Unframed
CT3 Module (IPmux-16)	*Number of Ports*	1 per module
	Compliance	• Telcordia GR-253, GR-499 • ANSI T1.102, T1.404 • ITU-T G.703, G.755, G.824, G.151 • AT&T TR54014
	Connector	BNC coaxial
	Data Rate	44.736 MHz
	Line Code	AMI B3ZS
	Line Impedance	75Ω

	Jitter Performance	Jitter tolerance: GR-499 (CAT II), G.824, TR 54014 Jitter transfer: G.755, GR-499 (CAT II), TR 54014 Intrinsic jitter: G.755, GR-253, TR 54014 Output jitter: GR-499 input jitter attenuated to the levels of a T1.404 network interface for CI type I equipment
	Max. Average Reframe Time	To a DS3: less than 1.5 ms To a DS2: less than 7 ms
	Framing Formats	M23 and C-bit parity DS3
Ethernet Modules	*Number of Ports*	1-port Ethernet module: 1 per module (network) 4-port Ethernet module: 4 per module (1 network and 3 user ports), via SFP (up to 2 fiber optic ports per module)
	Compliance	IEEE 802.3, 802.3u, 802.1p&Q
	Maximum Frame Size	1536 bytes ***Note**: Maximum frame size of the management traffic (ICMP, SNMP etc) is 1532 bytes.*
	Connector	RJ-45, 8 pin
	Data Rate	10 Mbps or 100 Mbps, full or half-duplex
	Fiber Optic	Characteristics: see *Table 1-12, Table 1-13* Connector: LC
Terminal Control Port	*Interface*	RS-232 (V.24), DTE
	Baud Rate	9.6, 19.2, 38.4, 57.6, 115.2 kbps
	Connector	9-pin, D-type, male
Management Ethernet Port	*Compliance*	IEEE 802.3, 802.34
	Connector	RJ-45, 8-pin
	Data Rate	10 Mbps full/half-duplex
Alarm Relay	*Contacts*	30V 2A
	Connector	9-pin, D-type, female
General System Indicators	*PS1*	ON (green): PS1 OK ON (red): PS1 failed OFF: PS1 is absent
	PS2	ON (green): PS2 OK ON (red): PS2 failed OFF: PS2 is absent
	RDY	On: Normal operation OFF: During initialization phase

	ALM	ON (red): ON (yellow): OFF:	Major alarm Minor alarm No alarm
	RX	Blinking: OFF:	Receiving data Data is not received
	TX	Blinking: OFF:	Transmitting data Data is not transmitted
	LINK	ON: OFF:	Line is OK Line is connected
	COLL	Blinking: OFF:	Collisions occur Normal operation, no collisions
Ethernet Port Indicators	*LINK*	OFF: ON:	Line is not active Line is OK
	ACT	OFF: ON:	No activity A frame is transmitted or received on the line
	FDX	OFF: ON:	Half-duplex Full-duplex
	100M	OFF: ON:	10 MHz 100 MHz
E1/T1 Port Indicators	*SYNC*	ON: OFF: Blinks:	Port is synchronized (no alarm) Signal loss, LOF or AIS is detected (local alarm) RDI is detected (remote alarm)
		Note: *All LEDs are ON (green) after power-up.*	
Power	*IPmux-8*	100 to 230 VAC, 55W -40 to -57 VDC, 75W	
	IPmux-16	100 to 230 VAC, 75W -40 to -57 VDC, 75W	
Physical	***IPmux-8***		
	Height	44 mm (1.7 in)	
	Width	432 mm (17.0 in)	
	Depth	350 mm (13.8 in)	
	Weight	7 kg (15.4 lb)	
	IPmux-16		
	Height	66 mm (2.6 in)	
	Width	432 mm (17.0 in)	
	Depth	350 mm (13.8 in)	
	Weight	7.1 kg (15.8 lb)	

Environment

Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-20°C to 70°C (-4°F to 158°F)
Humidity	Up to 90%, non-condensing

Table 1-12. Fiber Optic Characteristics (1-Port Ethernet Module)

Type	Connector	Optical Power [dBm]		Receive Sensitivity [dBm]		Loss [dB/km]		Typical Range [km]	Typical Range [miles]
		Min	Max	Min	Max	Min	Max		
Multimode	LC	-19	-14	-32	-8	1	4	2	1.2
Single mode	LC	-15	-8	-28	-8	0.5	0.8	15	9.3

Table 1-13. Fiber Optic Characteristics (4-Port Ethernet Module)

Ordering Name, Interface, Connector	Wavelength, Fiber Type [nm], [µm]	Standard	Transmitter Type	Input Power [dBm]		Output Power [dBm]		Typical Max. Range	
				(min)	(max)	(min)	(max)	[km]	[miles]
SFP-1 100BaseFx, LC	1310 nm, 62.5/125 multimode	IEEE 802.3	LED	-30	-14	-20	-14	2	1.2
SFP-2 100BaseLX10, LC	1310 nm, 9/125 single mode	IEEE 802.3	Laser	-28	-8	-15	-8	15	9.3
SFP-3 Fast Ethernet, LC	1310 nm, 9/125 single mode	–	Laser (short haul)	-34	-10	-5	0	40	24.8
SFP-4 Fast Ethernet, LC	1550 nm, 9/125 single mode	–	Laser (long haul)	-34	-10	-5	0	80	49.7

Chapter 2

Installation and Setup

This chapter discusses:

- Site requirements and prerequisites
- Package contents
- Connecting interface and power cables
- AC/DC power supply replacement.

2.1 Introduction

IPmux-8/16 is delivered completely assembled for desktop installation.

The only mechanical installation procedure that may be necessary is optional installation in a 19-inch rack:

- IPmux-8 uses RM-ACE-202
- IPmux-16 uses RM-27.

After installing the unit, configure IPmux-8/16 using an ASCII terminal connected to the IPmux-8/16 control port. The IPmux-8/16 configuration procedures are described in *Chapter 3* of this manual.

If problems are encountered, refer to *Chapter 6* for test and diagnostics instructions.

Warning

No internal settings, adjustment, maintenance and repairs may be performed by either the operator or the user; such activities may be performed only by skilled service personnel who are aware of the hazards involved.
Always observe standard safety precautions during installation, operation, and maintenance of this product.

2.2 Site Requirements and Prerequisites

IPmux-8/16 is designed for installation as a desktop unit. The RM-ACE-202 or RM-27 rack mount kits, for installation of IPmux-8/16 in a 19-inch rack, are supplied with the units.

AC-powered IPmux-8/16 units should be installed within 1.5m (5 feet) of an easily-accessible grounded AC outlet capable of furnishing the required supply voltage, in the range of 100 to 230 VAC.

DC-powered IPmux-8/16 units require a -48 VDC power source, which must be adequately isolated from the mains supply.

Allow at least 90 cm (36 inches) of frontal clearance for operator access. Allow at least 10 cm (4 inches) clearance at the rear of the unit for cable connections. Make sure that the ventilation holes are not blocked.

The ambient operating temperature of IPmux-8/16 is 0° C to 50° C (32° F to 122°F), at a relative humidity of up to 90%, non-condensing.

2.3 Package Contents

The IPmux-8/16 package contains the following items:

- IPmux-8/16 unit
- CBL-RJ45/2BNC adapter cable for unbalanced E1 interface
- Power cord for each ordered power supply
- Matching SFP transceiver for 4-port Ethernet module (if ordered)
- CBL-DB9/DB9/NULL cross cable that connects the IPmux-8/16 control port and an ASCII terminal (DTE) for local management.
- RM-ACE-202 kit for IPmux-8 and RM-27 kit for IPmux-16, containing hardware for mounting on unit in a 19-inch rack.

2.4 Rear Panel Schematics and Module Combinations

Figure 2-1 and *Figure 2-2* illustrate construction of the IPmux-8 and IPmux-16 rear panels, respectively.

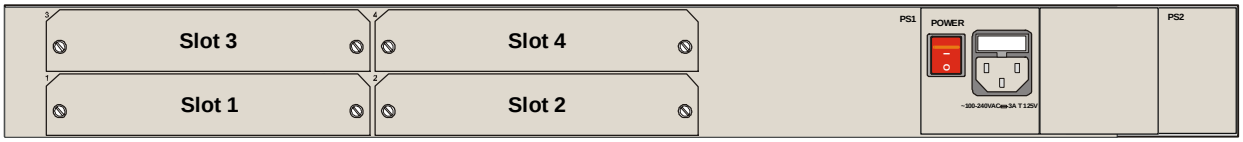


Figure 2-1. IPmux-8 Rear Panel Schematics

Figure 2-2. IPmux-16 Rear Panel Schematics

Table 2-1 lists the module combinations for IPmux-8/16.

Table 2-1. Module Combinations for IPmux-8/16

Slot 1	Slot 2	Slot 3	Slot 4	Comments
Ethernet module	Ethernet module	E1/T1	E3/T3/CT3	Load sharing
Ethernet module	Ethernet module	E3/T3/CT3	E1	Load sharing
Ethernet module	Ethernet module	E1/T1 or E3/T3/CT3	Empty	Redundancy
Ethernet module	Ethernet module	Empty	E1/T1 or E3/T3/CT3	Redundancy
Ethernet module	Ethernet module	E3/T3/CT3	E3/T3/CT3	Load sharing
Ethernet module	Ethernet module	E1/T1	E1/T1	Load sharing or Redundancy
Ethernet module	Empty	E3/T3/CT3	E1/T1	Not valid
Ethernet module	Empty	E3/T3/CT3	E3/T3/CT3	Not valid

Notes

- *When combining E1 and T1 modules, the T1 module must be inserted in slot 3.*
- *E3, T3 and CT3 modules always require an Ethernet module.*
- *E3/T3 bundle redundancy is available only when the E3 or T3 modules are installed in slot 3.*
- *IPmux-8 does not use E3, T3 and CT3 modules.*

2.5 Connecting to the TDM Equipment

IPmux-8/16 is connected to the TDM equipment via E1/T1 balanced RJ-45 ports or E3/T3/CT3 unbalanced BNC ports.

Connecting to the E1/T1 Devices

E1/T1 devices are connected to IPmux-8/16 via balanced RJ-45 ports designated E1/T1. Unbalanced E1 interface is provided via CBL-RJ45/2BNC adapter cable (see *Appendix A* for the connector pinouts and cable wiring diagram).

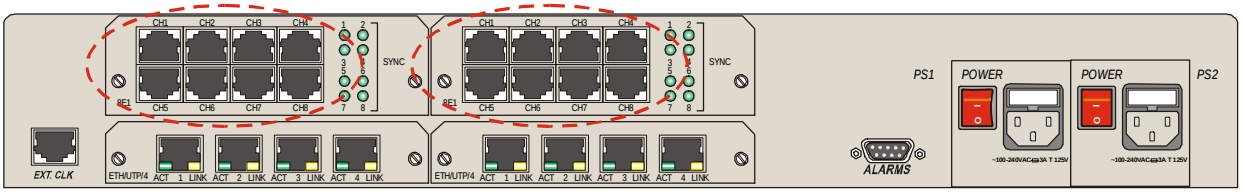


Figure 2-3. E1/T1 Connectors (8-Port Modules)

➤ **To connect to the E1/T1 devices with balanced interfaces:**

- Connect IPmux-8/16 to the E1/T1 devices using standard straight E1/T1 cables.

➤ **To connect to the E1 devices with unbalanced interfaces:**

1. Connect the RJ-45 connector of the CBL-RJ45/2BNC adapter cable to the IPmux-8/16 balanced RJ-45 ports.
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 to the E3, T3, CT3 Devices

E3, T3 and channelized CT3 devices are connected to IPmux-16 via unbalanced BNC ports designated E3, T3, CT3.

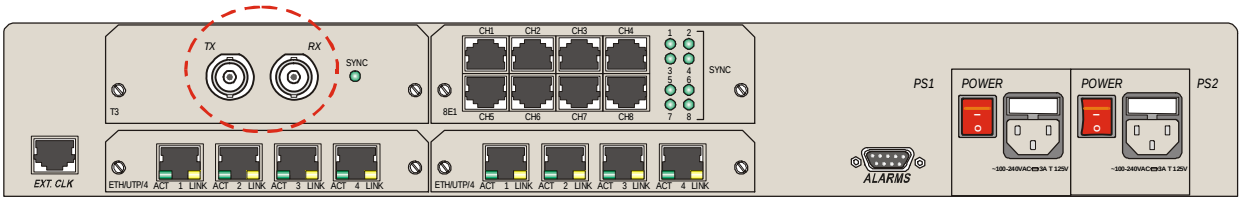


Figure 2-4. T3 Connectors

➤ **To connect to the E3, T3, CT3 devices:**

1. Connect the receive line of the 75Ω coaxial cable to the BNC connector labeled RX.
2. Connect the transmit line of the 75Ω coaxial cable to the BNC connector labeled TX.

2.6 Connecting to the Ethernet Equipment

IPmux-8/16 is connected to the Ethernet network equipment via the fiber optic LC connector (SFF-based for 1-port or SFP-based for 4-port Ethernet modules) or 8-pin RJ-45 electrical connector.
Connection to the Ethernet user equipment is made via LC fiber optic connector (available for port 2 only) or 8-pin RJ-45 electrical connectors on the 4-port Ethernet modules. Refer to *Appendix A* for the RJ-45 connector pinout.

Installing SFP Transceivers

The fiber optic interfaces of the 4-port Ethernet modules use SFP modules.

Warning

Third-party SFP optical transceivers must be agency-approved, complying with the local laser safety regulations for Class A laser equipment.

➤ **To install the SFP modules:**

1. Lock the wire latch of each SFP module by lifting it up until it clicks into place, as illustrated in *Figure 2-5*.

Note *Some SFP models have a plastic door instead of a wire latch.*

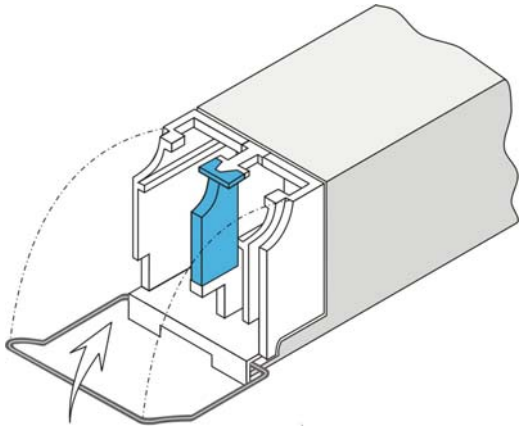


Figure 2-5. Locking the SFP Wire Latch

2. Carefully remove the dust covers from the SFP slots.
3. Insert the rear end of SFP into the socket, and push slowly backwards to mate the connectors until the SFP clicks into place. If you feel resistance before the connectors are fully mated, retract the SFP using the latch wire as a pulling handle, and then repeat the procedure.
4. Remove the protective rubber caps from the SFP modules.

➤ **To remove the SFP module:**

1. Disconnect the fiber optic cables from the SFP module.
2. Unlock the wire latch by lowering it downwards (as opposed to locking).
3. Hold the wire latch and pull the SFP module out of the user Ethernet port.

Connecting the Ethernet Network Equipment

Figure 2-6 illustrates a typical rear panel of IPmux-16 with fiber optic LC connector (4-port Ethernet module). *Figure 2-7* illustrates a typical rear panel of IPmux-8 with electrical RJ-45 network connector (1-port Ethernet module).

➤ **To connect to the Ethernet network equipment with fiber optic interface:**

- Connect IPmux-8/16 to the Ethernet network equipment using a standard fiber optic cable terminated with an LC connector.

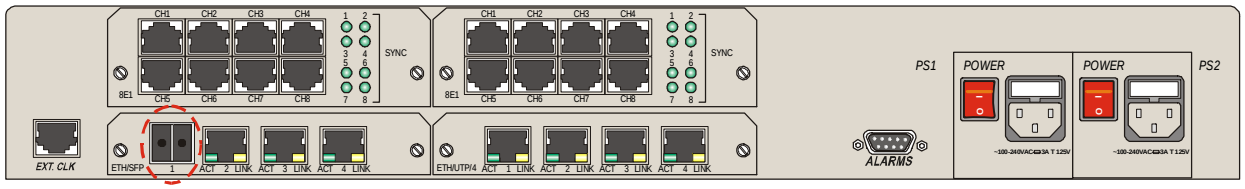


Figure 2-6. Fiber Optic Network Connector (4-Port Ethernet Module)

➤ **To connect to the Ethernet network equipment with a copper interface:**

- Connect IPmux-8/16 to the Ethernet network equipment using a standard straight UTP cable terminated with an RJ-45 connector.

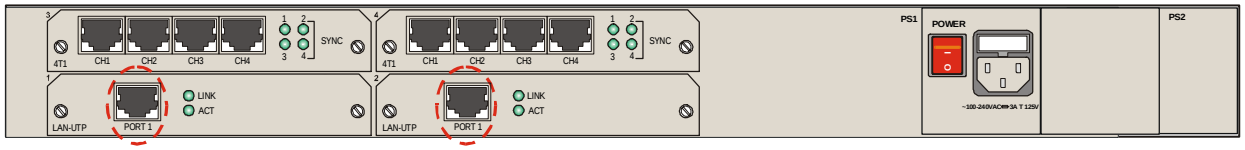


Figure 2-7. Electrical Connector (1-Port Ethernet Modules)

2.7 Connecting to the External Clock Source

IPmux-16 is connected to the external clock source via a balanced RJ-45 connector designated EXT. CLK. Refer to *Appendix A* for the connector pinout.

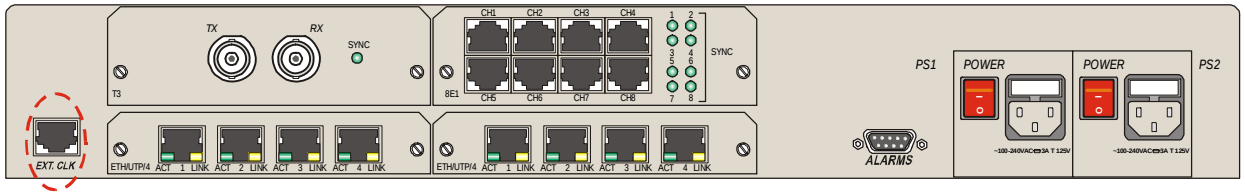


Figure 2-8. EXT. CLK Connector

➤ **To connect to the external clock source:**

- Connect IPmux-16 to the external E1 or T1 clock source using an appropriate cable.

2.8 Connecting to the Management Stations

IPmux-16 can be connected to a local ASCII terminal via CONTROL DTE port or to remote network management station via a dedicated CONTROL ETH port. IPmux-8 does not include a dedicated Ethernet management port.

Connecting to the ASCII Terminal

IPmux-8/16 is connected to an ASCII terminal via a 9-pin D-type male connector designated CONTROL DTE. A CBL-DB9/DB9/NULL cross cable is supplied with the unit for the ASCII terminal connection. *Appendix A* lists the control connector pinout and the cross cable wiring.

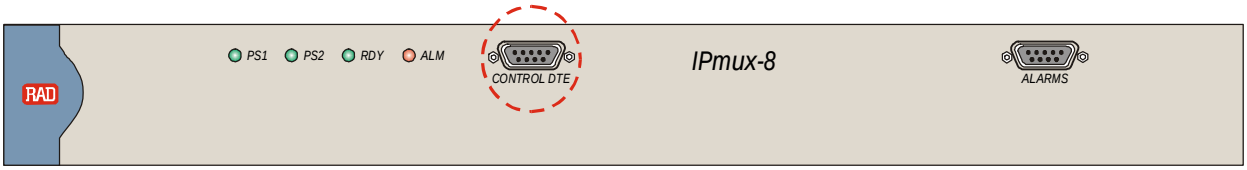


Figure 2-9. CONTROL DTE Connector (IPmux-8)

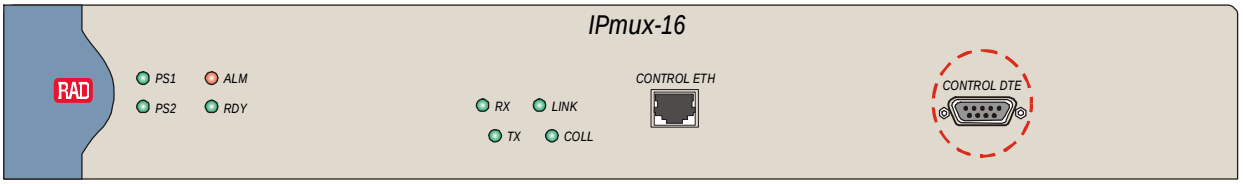


Figure 2-10. CONTROL DTE Connector (IPmux-16)

➤ **To connect to an ASCII terminal:**

1. Connect one 9-pin D-type connector of CBL-DB9/DB9/NULL cable to the CONTROL DTE connector.
2. Connect the other connector of the CBL-DB9/DB9/NULL cable to an ASCII terminal.

Connecting to the Network Management Station

IPmux-16 is connected to an NMS via an 8-pin RJ-45 connector designated CONTROL ETH. Refer to *Appendix A* for the connector pinout.

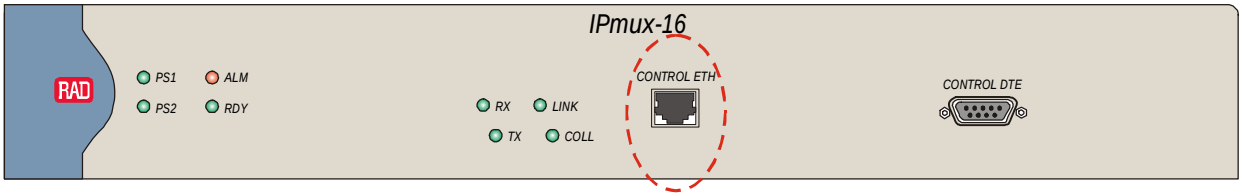


Figure 2-11. CONTROL ETH Connector

➤ **To connect to an NMS:**

- Connect IPmux-16 to a hub or switch using a straight cable.

  or

- Connect IPmux-16 to a network interface card using a cross cable.

Connecting to the External Alarm Device

IPmux-8/16 is connected to an external alarm device via a 9-pin D-type female connector designated ALARMS. Refer to *Appendix A* for the connector pinout.

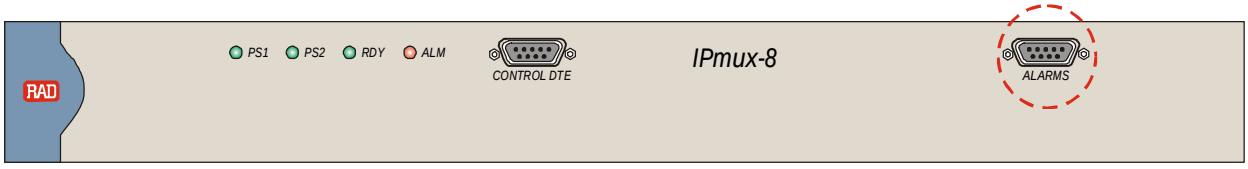


Figure 2-12. ALARMS Connector (IPmux-8)

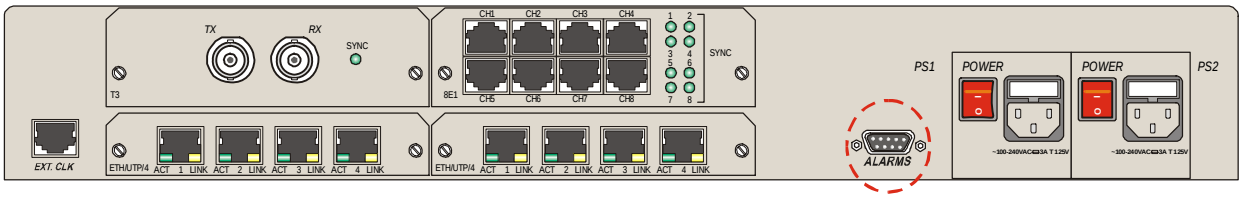


Figure 2-13. ALARMS Connector (IPmux-16)

➤ **To connect to an external alarm source:**

1. Prepare a cable in accordance with the alarm connector pinout given in *Appendix A*.
2. Connect IPmux-8/16 to an external alarm device, such as a buzzer, using prepared cable.

2.9 Connecting IPmux-8/16 to Power

To connect power to IPmux-8/16, refer to the appropriate section below, depending on your version of the unit (AC or DC).

Interrupting the protective grounding conductor (inside or outside the instrument) or disconnecting the protective earth terminal can make this instrument dangerous. Intentional interruption is prohibited.

Warning

Before switching ON this instrument and before connecting any other cable, the protective earth terminals of this instrument (either AC or DC version) must be connected to the protective ground conductor of the power cord.

Make sure that only fuses with the required rated current and specified type, 2 A T 250V as marked on the IPmux-8/16 rear panel, are used for replacement.

Whenever it is likely that the protection offered by fuses has been impaired, the instrument must be made inoperative and be secured to prevent any operation.

Note

Refer also to the sections describing connections of AC and DC mains at the beginning of the manual.

Connecting AC Power

AC power is supplied to IPmux-8/16 through the 1.5m (5 ft) standard power cable terminated by a standard 3-prong plug. The cable is supplied with the unit according to the number of ordered power supplies.

➤ **To connect AC power:**

1. Verify that the AC outlet is grounded properly. Ensure that the supply voltage is in the range 100 VAC to 240 VAC.
2. Check that the POWER switch on the rear panel is set to OFF.
3. Connect the power cable to the rear panel connector first and then to the AC mains outlet.

Connecting DC Power

➤ **To connect DC power:**

- Refer to the DC power supply connection supplement for instructions how to wire the DC adapters. The DC supplement is provided on the technical documentation CD supplied with the unit.

Replacing AC or DC Power Supplies

IPmux-8/16 can contain one or two power supply units (AC or DC). They are located in two slots, PS1 and PS2, in the rear panel. The following instructions refer to the power supply installation in any unit. These instructions are also valid for power supply replacement in any unit.

➤ **To install/replace the power supplies:**

1. Turn off the power switch/switches (red, lit) of the power supply (PS1, PS2) on the rear panel (see *Figure 2-14*).

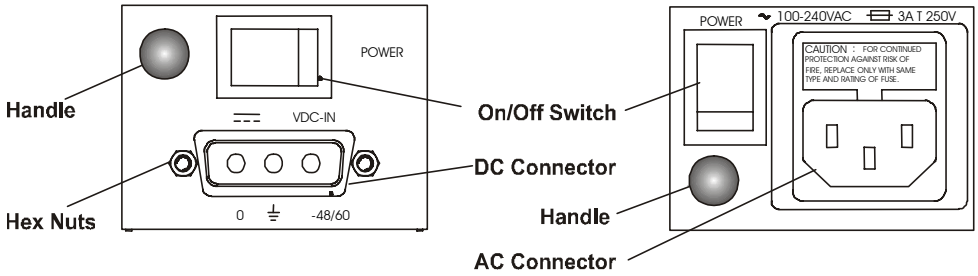


Figure 2-14. Power Supply (DC and AC) Rear Panel

2. Disconnect IPmux-8/16 from mains.
3. AC power supply: Pull out the cable safety lock and disconnect the power cable.

   DC power supply: Remove the cable screws connected to the hex nuts on the rear panel.

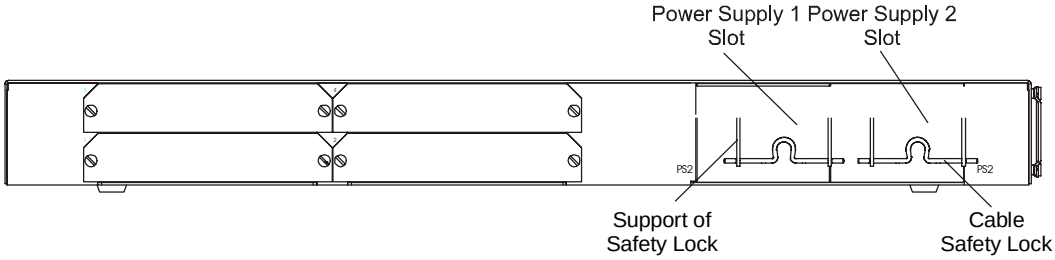


Figure 2-15. IPmux-8/16 Rear Panel – PS Replacement

4. Pull the black knob in the power supply panel and remove the replaceable power supply unit (see *Figure 2-15*).
5. Remove the new power supply from the package.
6. Slide the new power supply in its slot, and push the black knob until the unit is firmly in place.
7. Connect the power cable connector to the power supply.

8. Connect IPmux-8/16 to the mains.
9. Turn the power supply switch on. The switch red cover lights up.
10. Turn the power supply switch off.
11. AC power supply: Insert the cable safety lock.

    DC power supply: Lock the DC connector by inserting the two locking cable screws into the hex nuts on the power supply panel.
12. Verify the power supply is secured in its slot.

Note *If IPmux-8/16 has a single AC power supply unit, install the safety lock support first at the proper power supply slot. The safety lock support consists of one banded part attached to the protection panel with screws. In this case, the cable safety lock is already installed in the support.*

Chapter 3

Operation

This chapter:

- Provides a detailed description of the front panel controls and indicators
- Explains power-on and power-off procedures
- Provides instructions for using a terminal connected to the IPmux-8/16 control port
- Describes how to navigate menus
- Illustrates management menus.

For a detailed explanation of parameters of the menus, see *Chapter 4*.

3.1 Turning IPmux-8/16 On

IPmux-16 power switches are located on the back panel of the unit.

IPmux-8 does not have a power switch. The unit turns on automatically upon connection to the mains.

➤ **To turn on IPmux-8:**

- Connect the power cord to the mains.

  The PWR indicator ligzhts up and remains lit as long as IPmux-8/16 receives power.

➤ **To turn on IPmux-16:**

- Set the PS1 and/or PS2 power supply switch(es), located on the rear panel, to ON.

3.2 Front Panel Controls, Connectors, and Indicators

IPmux-8

The IPmux-8 LEDs are located on the left side of the front panel. Interface modules installed in IPmux-8 have their own LED indicators (see *Figure 3-1* and *Figure 3-2*).

Figure 3-1. IPmux-8 Front Panel

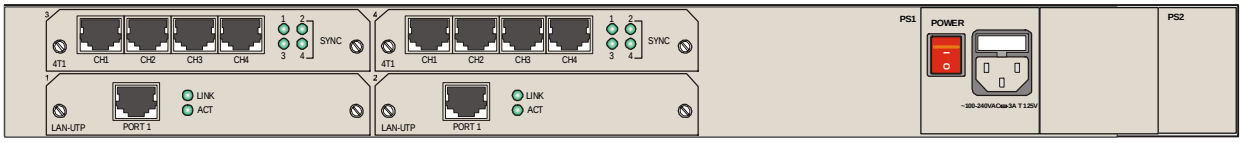


Figure 3-2. IPmux-8 Rear Panel (2 × 4-Port T1 Modules, 2 × 1-Port Ethernet Modules)

Table 3-1 lists the functions of the IPmux-8 system indicators.

Table 3-1. IPmux-8 System Indicators

Module	Name	Type	Function
System	RDY	LED (green)	ON: Device is OK OFF: Self-test in progress Blinking: Malfunction detected
System	PS1/PS2	LED (green)	ON: Unit powered OFF: Unit not powered
	ALM	LED (red)	ON: Alarm is stored in the log file OFF: No alarm is stored in the log file
Ethernet	LINK	LED (yellow)	ON: LAN is connected OFF: LAN is disconnected
	ACT	LED (green)	ON: Frame being transferred on line OFF: No activity
E1/T1	SYNC	LED (green)	ON: Port synchronized (no alarm) OFF: Unframed – Signal loss or AIS detected Framed – Signal loss, loss of frame or AIS detected Blinking: RDI detected (remote alarm)
Rear panel	PS1/PS2	Switch	Turns IPmux-8/16 power on and off

IPmux-16

The IPmux-16 LEDs are located on the left side of the front panel. Interface modules installed in IPmux-16 have their own LED indicators (see *Figure 3-3* and *Figure 3-4*).

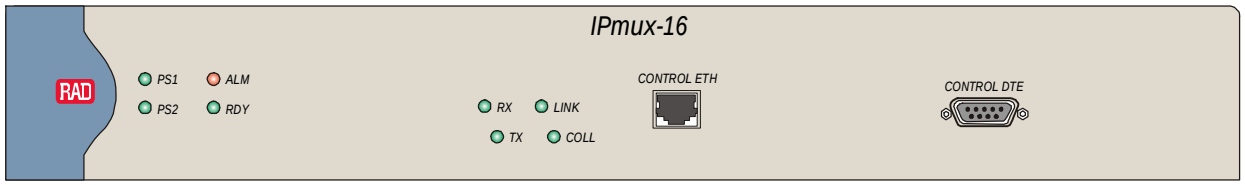


Figure 3-3. IPmux-16 Front Panel

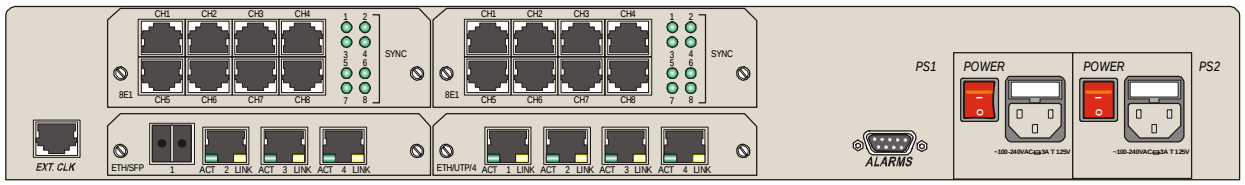


Figure 3-4. IPmux-16 Rear Panel Switch (2 × 8-Port E1 Modules, 2 × 4-Port Ethernet Modules)

Table 3-2 lists the functions of the IPmux-16 system indicators.

Table 3-2. IPmux-16 Front Panel Indicators and Switches

Module	Name	Type	Function
System	RDY	LED (green)	ON: Device is OK OFF: Self-test in progress Blinking: Malfunction detected
	PS1/PS2	LED (green)	ON: Unit powered OFF: Unit not powered
	ALM	LED (red)	ON: Alarm is stored in the log file OFF: No alarm is stored in the log file
Ethernet (MNG)	LINK	LED (yellow)	ON: LAN is connected OFF: LAN is disconnected
	COLL	LED (yellow)	ON: Collision is detected on the Ethernet interface (half duplex mode only) OFF: No collision is detected on the Ethernet interface
	TX	LED (yellow)	ON: Data is being transmitted on the Ethernet interface OFF: No data is being transmitted on the Ethernet interface
	RX	LED (yellow)	ON: Data is being received on the Ethernet interface OFF: No data is being received on the Ethernet interface

Table 3-3. IPmux-16 Interface/Rear Panel Indicators and Switches

Module	Name	Type	Function
Ethernet (user)	LINK	LED (yellow)	ON: LAN is connected OFF: LAN is disconnected
	ACT	LED (green)	ON: Frame being transferred on line OFF: No activity
E1/T1	SYNC	LED (green)	ON: Port synchronized (no alarm) OFF: Unframed – Signal loss or AIS detected Framed – Signal loss, loss of frame or AIS detected Blinking: RDI detected (remote alarm)
E3/T3	SYNC		ON: Port synchronized (signal detected) OFF: Signal loss or AIS detected
CT3	SYNC		ON: Port synchronized (signal detected) OFF: Signal loss or AIS detected
Rear panel	PS1/PS2	Switch	Turns IPmux-16 power on and off

3.3 Default Settings

Table 3-4 lists the default settings of the IPmux-8/16 configuration parameters.

Table 3-4. Default Settings

Type	Parameter	Default Value
SYSTEM	Telnet Access	Enable
	SNMP Access	Enable
Authentication/Community	Authentication failure trap	Off
	Trap	public
	Read	public
	Write	public
Host Configuration	Host Index	OOB Management Host
Manager List	Manager IP Address	0.0.0.0
	Host Index	Ethernet 1 Host
Default Gateway	Gateway IP	0.0.0.0
ASCII Terminal Configuration	Display Mode	Color
	Baud Rate	19200
	15 min. Timeout	On
	Hard flow ctrl (RTS/CTS)	Off

Table 3-4. Default Settings (Cont.)

Type	Parameter	Default Value
PHYSICAL LAYER CONFIGURATION		
E1	Channel Status	Enable
	Transmit Clock Source	Loopback
	Loopback State	Disable
	Rx Sensitivity	-10 dB
	Line Type	CRC4 Enabled
	UpLink fail Alarm Behavior	Cond.
	Idle Code	7E
	Signaling Mode	CAS enable
	Cond. Data pattern	7F
	Cond. CAS (ABCD) Pattern	01
T1	Channel Status	Enable
	Transmit Clock Source	Loopback
	Line Type	T1-ESF
	Line Code	B8ZS
	Line Mode	DSU
	Line Length(feet)/Tx Gain	0-133/ -7.5 dB
	UpLink fail Alarm Behavior	Cond.
	Restore Time	1 second
	Idle Code	7E
	Signaling Mode	CAS enable
	Leased Line	Disable
	Cond. Data pattern	7F
	Cond. CAS (AB/ABCD) Pattern	01
	Cond. CAS first 2.5sec Pattern	FF
	Loopback State	Disable
	Loopback Location	Local System
	Activate Loop Pattern	10000
	Deactivate Loop Pattern	100
E3, T3	Channel Status	Enable
	Transmit Clock Source	Loopback
	Loopback State	Disable

Table 3-4. Default Settings (Cont.)

Type	Parameter	Default Value
PHYSICAL LAYER CONFIGURATION (Cont.)		
Channelized T3 (External)	Channel Status	Enable
	Line Type	C_Bit
	Transmit Clock Source	Loopback
	Loopback State	Disable
Channelized T3 (T1)	Channel Status	Enable
	Line Type	T1-ESF
	Restore Time	1 second
	Loopback State	Disable
	Transmit Clock Source	Loopback
OOB Management Channel	Default Type	10baseT Full Duplex
IP SUPPORT	IP ToS	0

3.4 Configuration Alternatives

After installation, there are no special operating procedures for IPmux-8/16. Once it is powered up, the unit operates automatically. The unit operational status can be monitored constantly.

If required, IPmux-8/16 can be reconfigured. IPmux-8/16 can be managed using different ports and applications:

- Local management via an ASCII terminal connected to RS-232 port. Usually, preliminary configuration of the system parameters is performed via ASCII terminal. Once the IPmux-8/16 host IP parameters are set, it is possible to access it via Telnet or RADview for further configuration.
- Remote management from a network management station connected to CONTROL ETH port. Remote management is performed using Telnet or RADview, RAD's SNMP-based network management system.

The following functions are supported by the IPmux-8/16 management software:

- Viewing system information
- Modifying configuration and mode of operation, including setting system default values
- Monitoring IPmux-8/16 performance
- Initiating diagnostic tests
- Uploading and downloading software, configuration and user files.

Configuring IPmux-8/16 via Terminal

IPmux-8/16 includes a V.24/RS-232 asynchronous DTE port, designated CONTROL and terminated in a 9-pin D-type female connector. The control port continuously monitors the incoming data stream and immediately responds to any input string received through this port.

The IPmux-8/16 control port can be configured to communicate at the following rates: 9.6, 19.2, 38.4, 57.6 or 115.2 kbps.

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

1. Make sure all IPmux-8/16 cables and connectors are properly connected.
2. Connect IPmux-8/16 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 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 6* for instructions.

Login

To prevent unauthorized modification of the operating parameters, IPmux-8/16 supports two access levels: .

- **Superuser** can perform all the activities supported by the IPmux-8/16 management facility.
- **User** cannot perform any configuration changes, they are allowed to monitor the IPmux-8/16 operation only.

Note *It is recommended to change default passwords to prevent unauthorized access to the unit.*

➤ **To enter as a superuser:**

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

This allows you to configure all the parameters of IPmux-8/16, and to change the passwords.

➤ **To enter as a user:**

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

This does not allow you to make configuration changes.

Choosing Options

➤ **To choose an option:**

1. Type the number corresponding to the option, and press **<Enter>**.
2. Press **<Spacebar>** to toggle between the available values.
3. Press **<Enter>** when the required value is displayed.

Saving Changes

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

- Type **S** to save the changes that were made to the IPmux-8/16 configuration.

Overview of Menu Operations

Use these menu trees as a reference aid while performing configuration and control functions. *Chapter 4* illustrates menus and explains parameters.

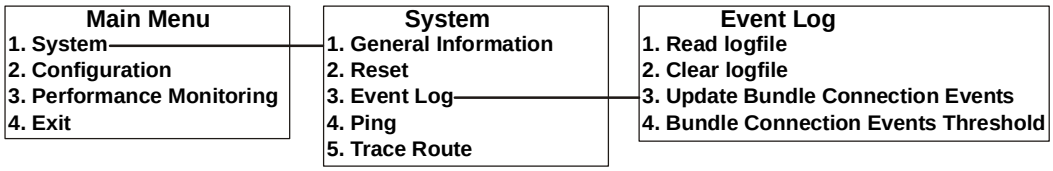


Figure 3-5. Main Menu > System > Event Log

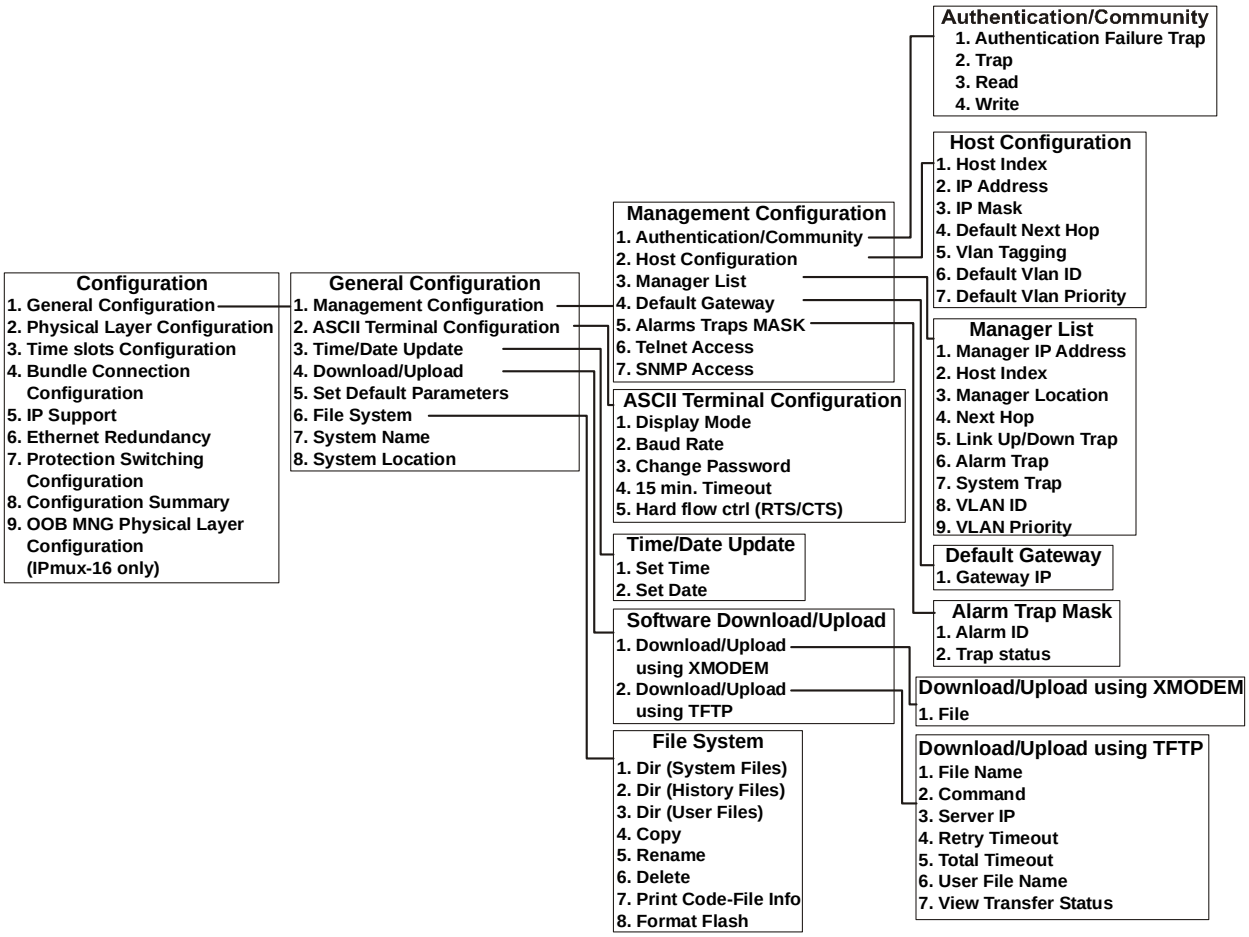


Figure 3-6. Configuration > General Configuration

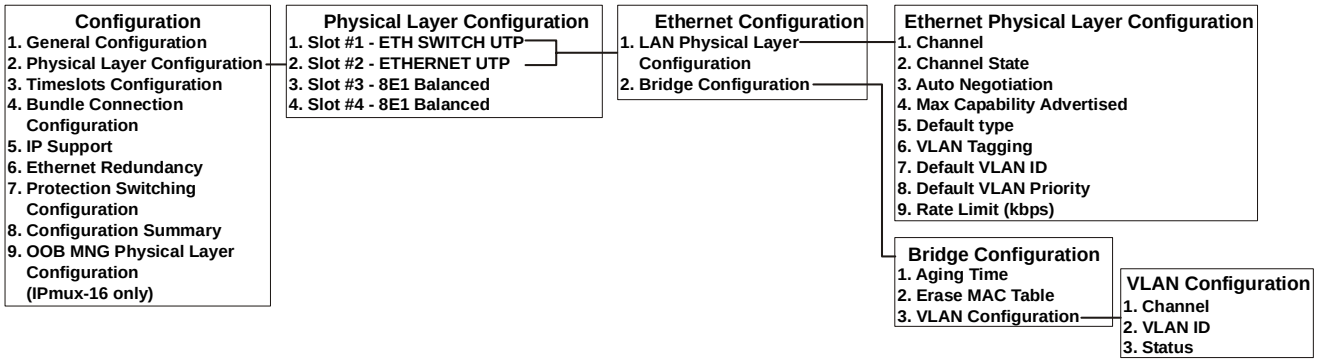


Figure 3-7. Configuration > Physical Layer Configuration (Ethernet Modules)

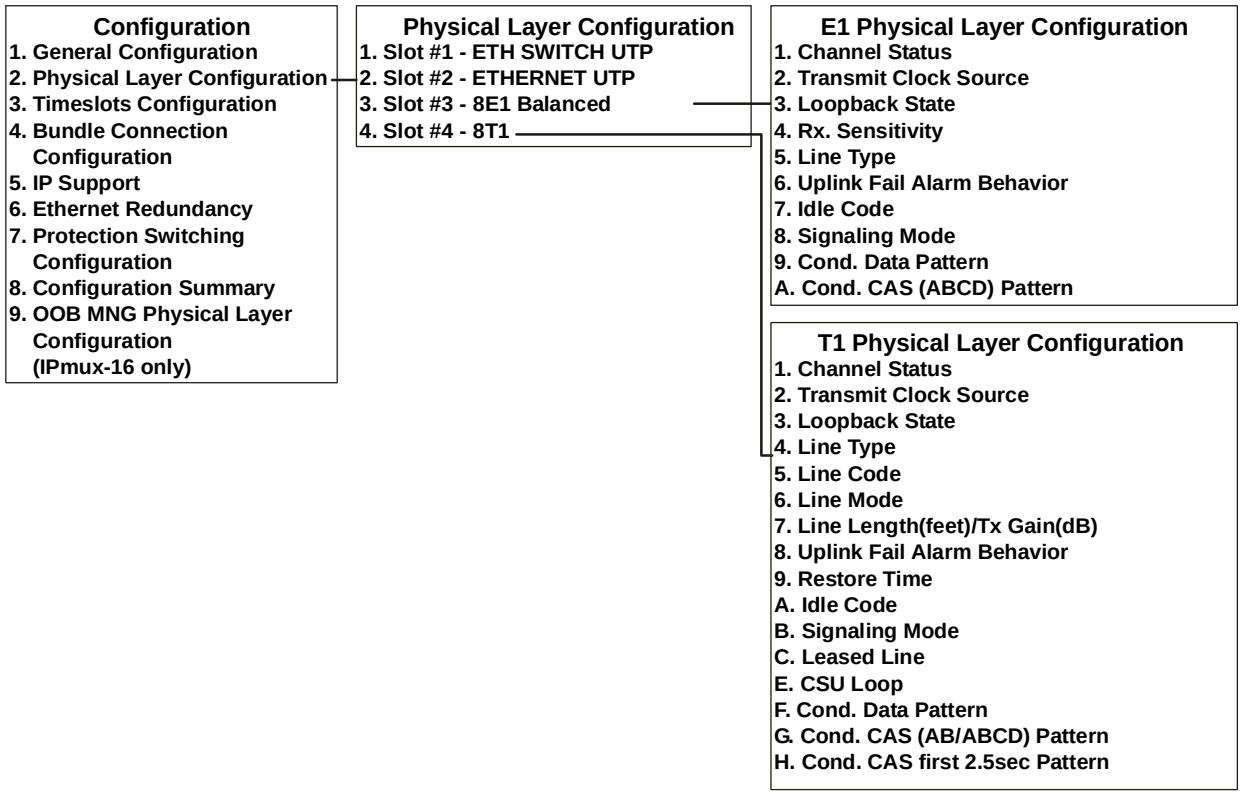


Figure 3-8. Configuration > Physical Layer Configuration (E1 and T1 Modules)

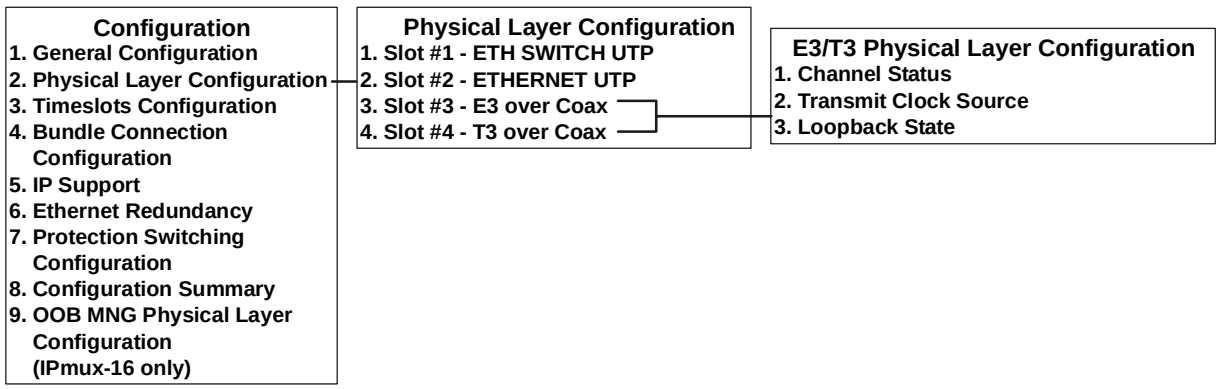


Figure 3-9. Configuration > Physical Layer Configuration (E3 and T3 Modules)

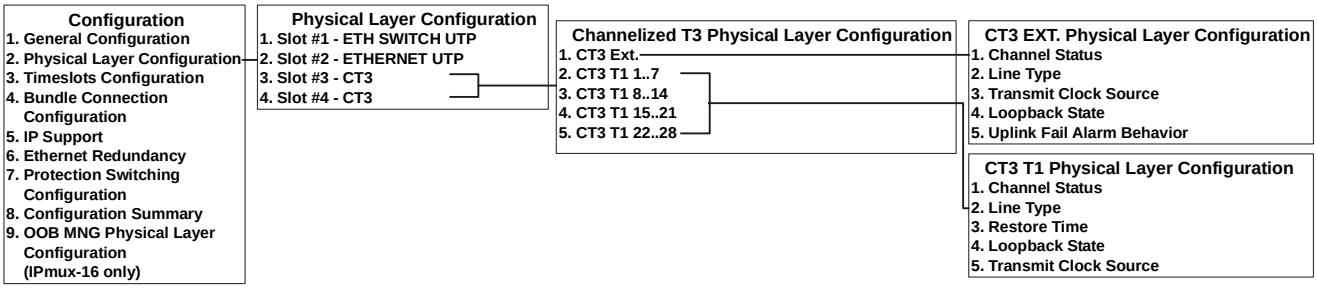


Figure 3-10. Configuration > Physical Layer Configuration (Channelized T3 Modules)

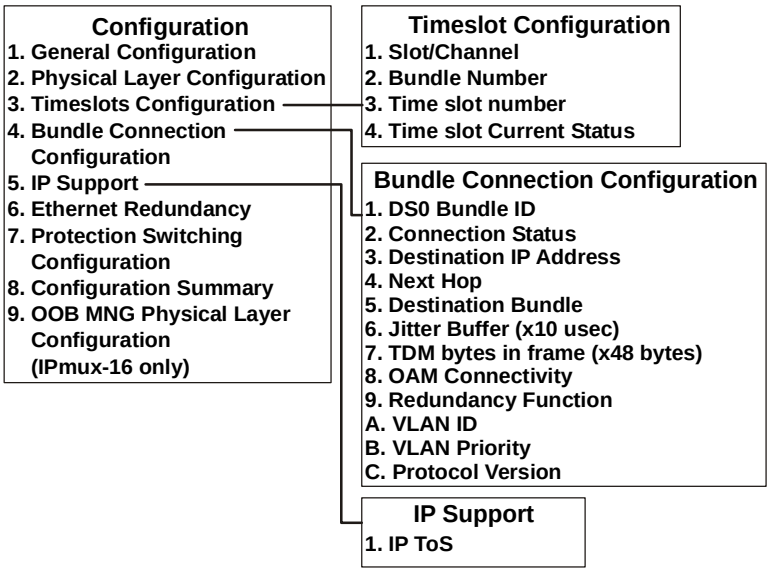


Figure 3-11. Configuration > Timeslot Configuration, Bundle Connection Configuration, IP Support

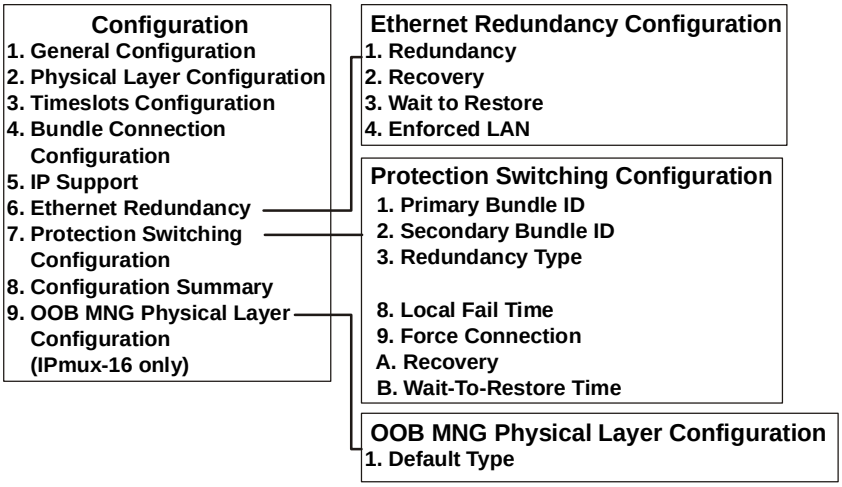


Figure 3-12. Configuration > Ethernet Redundancy, Protection Switching Configuration

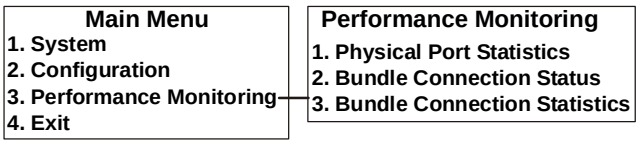


Figure 3-13. Main Menu > Performance Monitoring

3.5 Turning IPmux-8/16 Off

➤ **To power off IPmux-8:**

- Remove the power cord from the power source.

➤ **To power off IPmux-16:**

- Set the PS1 and/or PS2 power supply switch(es) to OFF.

Chapter 4

Configuration

This chapter illustrates the configuration IPmux-8/16 screens and explains their parameters.

Menu trees of the IPmux-8/16 management software are shown in *Chapter 3*.

4.1 Configuring IPmux-8/16 for Management

The IPmux-8/16 management software allows you to perform the following:

- Defining IP management parameters
- Defining ASCII terminal parameters
- Configuring out-of-band management port.

Configuring IP Parameters

IPmux-8/16 can be managed by a network management station, which is located on the LAN connected to one of its 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, and define at least one network manager.

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-8/16.

Path: Main > Configuration > General Configuration > Management Configuration > Authentication/Community.

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

1. Follow the path above to display the Authentication/Community menu (*Figure 4-1*).
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-8/16 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).

```
                    AUTHENTICATION/COMMUNITY


1. Authentication Failure Trap                    Off

2. Trap                                           public

3. Read                                           public

4. Write                                          public

ESC. Exit

Select item from the menu:  _
```

Figure 4-1. Authentication/Community Menu

Configuring Host IP Parameters

IPmux-8/16 hosts must be assigned an IP address and IP mask to allow communication between the local and remote IPmux units. Valid IP addresses are also needed for the inband and out-of-band management of the unit. IPmux-8/16 supports separate hosts for out-of-band management (OOB Management Host) and two Ethernet module hosts (Ethernet 1 Host and Ethernet 2 Host). The out-of-band management host IP address should be on a different subnet than the Ethernet 1 and Ethernet 2 host IP addresses.

Note *IPmux-8 does not support out-of-band management host.*

Path: Main > Configuration > General Configuration > Management Configuration > Host Configuration.

➤ **To configure host IP parameters:**

1. Follow the path above to display the Host Configuration menu (*Figure 4-2*).
2. From the Host Configuration menu, configure the following:
   - Host Index (Host identification index)
     - OOB Management Host (Host for out-of-band management traffic via CONTROL ETH port)
     - Ethernet 1 Host IP (Network port host of the Ethernet module installed in slot 1. This host serves for both TDMoIP traffic and inband management)
     - Ethernet 2 Host (Network port host of the Ethernet module installed in slot 2. This host serves for both TDMoIP traffic and inband management)
   - IP Address
   - IP Mask

- Default Next Hop (IP address to which traffic from this host is sent to enable reaching the destination IP. This parameter is required whenever the destination IP address of the opposite TDMoIP device does not reside on the same subnet as the source IP address (i.e. Host IP address). The default gateway address is needed to acquire the MAC address of the access router, which is used under the Dest MAC address of the TDMoIP frame.)
  - When the host is LAN1 or LAN2 the next hop IP address is used for the TDMoIP traffic if no next hop is defined under bundle connection configuration (see *Figure 4-15*).
  - When the host is out-of-band management host (relevant for IPmux-16 only), the default next hop is used by the managers defined under OOB manager list (see *Figure 4-3*), if no next hop is defined for the network managers.
- VLAN Tagging
  - Yes (VLAN tags are added by the host to outgoing traffic)
  - No (VLAN tags are not added by the host to outgoing traffic)
- Default VLAN ID (VLAN tag to be added by the host to outgoing traffic): 1–4095
- Default VLAN Priority (Priority to be assigned by the host to outgoing traffic): 0–7

Note *Default next hop, default VLAN ID and default VLAN priority values are used for the management and TDMoIP traffic if no VLANs or next hop addresses were configured in the Manager List and Bundle Connection Configuration menus.*

```
                          HOST CONFIGURATION

1. Host Index               OOB Management Host
2. IP Address               192.168.217.12
3. IP Mask                  255. 255. 255. 0
4. Default Next Hop         192.168.217.1
5. Vlan Tagging             No
6. Default Vlan ID          00
7. Default Vlan Priority    0
ESC. Exit                   N. Next
Select item from the menu:_
```

Figure 4-2. Host Configuration Menu

➤ **To delete a host:**

1. From the Host Configuration menu, select a host to be deleted.
2. Type **D**.

   The following confirmation message is displayed: **Configuration will be deleted! Are you sure? (Y/N)**.

3. Type **Y** to confirm.

   A second confirmation message is displayed: **`Bundle connections, Default GW and Managers IP will be deleted (Y/N)`**.

4. Type **Y** to confirm.

   The host is deleted.

Deletion of host ID automatically deletes the following parameters: host IP, default gateway, all managers and all bundles connected to the host.

Defining Network Managers

Define network managers, which access IPmux-8/16 via its Ethernet ports. The management access can be ether out-of-band (via CONTROL ETH port) or inband via LAN ports of the Ethernet modules. Each manager must be assigned to a specific host (out-of-band, Ethernet 1 or Ethernet 2). Up to eight network managers can be added. Also, you can enable or disable manager stations to receive certain traps sent out by IPmux-8/16 in case of malfunction.

Path: Main > Configuration > General Configuration > Management Configuration > Manager List.

➤ **To define a network manager:**

1. Follow the path above to access the Manager List menu (*Figure 4-3*).
2. From the Manager List menu, configure the following:
   - Manager IP Address (IP address of the management station)
   - Host index (index of the host, which the management station is assigned to)
     - OOB Management Host (host for out-of-band management traffic via CONTROL ETH port)
     - Ethernet 1 Host (Host of the network port of the Ethernet module installed in slot 1. This host serves for the TDMoIP traffic and inband management)
     - Ethernet 2 Host (Host of the network port of the Ethernet module installed in slot 2. This host serves for the TDMoIP traffic and inband management)
   - Manager Location (Relevant only for 4-port Ethernet modules. Specifies which internal switch ports are allowed to handle management traffic coming from the current manager station)
     - Network Port Only (only network port is allowed to handle the management traffic)
     - User Port1 Only (Only user port 1 is allowed to handle the management traffic)
     - User Port2 Only (Only user port 2 is allowed to handle the management traffic)

- User Port3 Only (Only user port 3 is allowed to handle the management traffic)
- All User Ports (All user ports are allowed to handle the management traffic)
- All Ports (All ports are allowed to handle the management traffic)

- Next Hop (IP address to which traffic from the host is sent to enable reaching the management station IP. This is usually the address of an IP router port. You need to specify the next hop IP address only if the destination IP address is not within the IP subnet of the current host port.)

Note *If the manager next hop is not configured, the unit uses the default next hop configured from Host Configuration menu (Figure 4-2). If the default next hop is also not defined, the unit uses the default gateway IP address.*

- Link Up/Down Trap (sending a Link Up/Down trap to the manager station if a physical failure occurs on the Ethernet or TDM link)
  - Yes (Link Up/Down trap is sent)
  - No (Link Up/Down trap is not sent)
- Alarm Trap (Sending Alarm trap to the manager station if an unmasked alarm is registered in the IPmux-8/16 log file. This trap informs the network manager of both entry and exit from an alarm state.)
  - Yes (Alarm trap is sent)
  - No (Alarm trap is not sent)
- System Trap (Sending System trap to the manager station if the IPmux-8/16 power supply or fan failure occurs)
  - Yes (Alarm trap is sent)
  - No (Alarm trap is not sent)
- VLAN ID (VLAN tag to be added by the host to the management traffic sent to the current network manager): 0–4095
- VLAN Priority (Priority to be assigned by the host to the management traffic sent to the current network manager): 0–7.

Note
- *The VLAN ID and VLAN Priority parameters are not displayed if VAN tagging is disabled in the Host Configuration menu.*
- *If no VLANs and next hop are defined for the management traffic, IPmux-8/16 uses their default values set in the Host Configuration menu.*

3. From the From the Manager List menu, type **N** to add another network manager, **D** to delete the current one or **P** to ping it.

```
                              MANAGER LIST

1. Manager IP Address  192.114.35.1

2. Host Index                OOB Management Host

3. Manager Location          Network Port Only

4. Next Hop

5. Link Up/Down Trap         On

6. Alarm Trap                Off

7. System Trap               Off

8. VLAN ID                   0

9. VLAN Priority             00

ESC. Exit              S. Save     D. Delete           P. Ping      N. Next

After Save: ESC. Exit

Select item from the menu:  _
```

Figure 4-3. Manager List Menu

Configuring Default Gateway

Defines default gateway for the management traffic. This is a "master" default gateway, which is used by default as the next hop IP address to reach any IP address residing outside of the IPmux-8/16 subnets, if no other next hop is configured.

Path: Main > Configuration > General Configuration > Management Configuration > Default Gateway.

➤ **To define the default gateway:**

1. Follow the path above to access the Default Gateway menu (*Figure 4-4*).
2. From the Default Gateway menu, select **Gateway IP**, and enter the IP address of the device, which serves as a default gateway.

```
                              DEFAULT GATEWAY


1. Gateway IP     0.0.0.0
ESC. Exit

Select item from the menu.
```

Figure 4-4. Default Gateway Menu

Controlling Telnet Access

You can enable or disable access to the IPmux-8/16 management system via Telnet. By disabling Telnet, you prevent unauthorized access to the system when security of the IPmux-8/16 IP address has been compromised. When Telnet access is disabled, IPmux-8/16 closes the TCP port, allowing management via an ASCII terminal only. In addition, you can allow Telnet only for the network management stations defined via the Managers List menu (*Figure 4-3*).

Note *If no network managers are defined, Telnet access is allowed for all users.*

Path: Main > Configuration > General Configuration > Management Configuration.

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

1. Follow the path above to display the Management Configuration menu.
2. From the Management Configuration menu, select **Telnet Access** and select **Disable** to disable access via Telnet, **Enable** to enable the Telnet access, or **Managers** to allow Telnet access for the defined network managers only.

Controlling SNMP Access

You can enable or disable access to the IPmux-8/16 management system via SNMP. When SNMP access is disabled, IPmux-8/16 closes the UDP port (161), allowing management via an ASCII terminal or a Telnet host. In addition, you can allow SNMP access only for the network management stations defined via the Managers List menu (*Figure 4-3*).

Notes
- *If no network managers are defined, SNMP access is disabled for all users.*
- *SNMP access configuration is available only in terminal and Telnet management sessions.*
- *No SNMP traps are sent, when the SNMP access is disabled.*

Path: Main > Configuration > General Configuration > Management Configuration.

➤ **To enable or disable SNMP access:**

1. Follow the path above to display the Management Configuration menu.
2. From the Management Configuration menu, select **SNMP Access** and select **Disable** to disable access via SNMP, **Enable** to enable the SNMP access, or **Managers** to allow SNMP access for the defined network managers only.

Configuring the Terminal Control Port

IPmux-8/16 embedded software enables you to configure the terminal control port parameters, which include specifying display mode, terminal baud rate, password for terminal control session, hardware flow control and security timeout.

Path: Main > Configuration > General Configuration > ASCII Terminal Configuration.

➤ **To configure the terminal control port:**

1. Follow the path above to access the ASCII Terminal Configuration menu (*Figure 4-5*).
2. From the ASCII Terminal Configuration menu, configure the following:
   - Display Mode (ASCII terminal display mode)
     - Color
     - MonoChrome 3 color
     - MonoChrome 2 color
   - Baud Rate (in bps)
     - 9600
     - 19200
     - 38400
     - 57600
     - 115200

Note *If you change the baud rate of the IPmux-8/16 control port, make sure to change the rate of the ASCII terminal to match the new setting.*

   - Change password (assigning a new password to an existing user)
   - Hard Flow Ctrl (hardware flow control)
     - On (Hardware flow control is enabled)
     - Off (Hardware flow control is disabled)
   - Security Timeout T (A time interval after which IPmux-8/16 automatically exits to the password entry screen if no input from the user is detected for 15 minutes)
     - On (Security timeout is enabled)
     - Off (Security timeout is disabled)

```
                        ASCII Terminal Configuration

1. Display Mode       Color

2. Baud Rate [bps]    19200

3. Change Password

4. Hard flow ctrl (RTS/CTS)  Off

5. 15 Min. Timeout    On
ESC. Exit
            +-------------------------------------------------+
            |Notice: Change the Baud Rate of the ASCII Terminal|
            |after changing and saving of new Baud Rate data!  |
            +-------------------------------------------------+

Select item from the menu:_
```

Figure 4-5. ASCII Terminal Configuration Menu

Configuring Out-of-Band Management Port

IPmux-16 supports 10BaseT port for out-of-band management, which has to be configured at the physical layer.

Path: Main > Configuration > OOB MNG Physical Layer Configuration.

➤ **To configure out-of-band management port:**

1. Follow the path above to access the OOB Physical Layer Configuration menu.
2. From the OOB Physical Layer Configuration menu, select **Default Type** and choose default type of the out-of-band management port (10BaseT full duplex or 10BaseT half duplex).

4.2 Configuring IPmux-8/16 for Operation

The recommended configuration procedure for IPmux-8/16 operation includes the following stages:

- Configuring Ethernet and TDM interfaces at the physical level
- Creating bundles by allocating timeslots to them timeslots
- Directing the bundles defined above to remote IPmux unit.

Configuring IPmux-8/16 at the Physical Level

The TDM (E1, T1, E3, T3, channelized T3) and Ethernet interfaces of IPmux-8/16 must be configured at the physical level.

Configuring Ethernet Interfaces

IPmux-8/16 supports 1- and 4-port Ethernet modules. This section illustrates configuration procedure for a 4-port Ethernet module with 4-port Ethernet switch. For a 1-port Ethernet module only the following parameters are user-configurable:

- Autonegotiation
- Maximum capability advertised
- Default type.

Path: Main > Configuration > Physical Layer Configuration > Slot # 1/2 > LAN Physical Layer Configuration.

➤ **To configure Ethernet interfaces:**

1. Follow the path above to display the LAN Physical Layer Configuration menu.
2. From the LAN Physical Layer Configuration, configure the following:
   - Channel
     - Port 1 (Network port)
     - Port 2 (User port 1)
     - Port 3 (User port 2)
     - Port 4 (User port 3)
   - Channel state
     - Enable (Current Ethernet interface is enabled)
     - Disable (Current Ethernet interface is disabled)
   - Autonegotiation:
     - 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 degrades the connection to a half-duplex mode. In order to avoid this, autonegotiation must be disabled and the ports must be configured manually. Half-duplex degradation occurs also when autonegotiation is enabled at one port and disabled at the opposite port.*

- VLAN Tagging (Operation mode for the corresponding port of internal switch):
  - Tag (Tagged)
  - Untag (Untagged)
  - Transparent
  - Double Tag (Double Tagged)

  When one of the user ports is in the Double Tagged mode, the rest of the user ports can be configured to operate as Transparent (towards network only) or Double Tagged.
- Default VLAN ID (VLAN associated with untagged frames arriving at the port): 1–4095
- Default VLAN Priority: 0–7

Note *For the 4-port Ethernet modules VLAN priority is mapped to one of the following queues:*

Default VLAN Priority	***Priority Queue***
0, 1	*0 (lowest priority)*
2, 3	*1*
4, 5	*2*
*6, 7**	*3 (highest priority)*

** – If the user Ethernet traffic is configured to receive the highest priority (6 or 7), it may interfere with TDM traffic, which has high priority by default.*

If VLAN Tagging mode of a port is set to Tag and no rate limiting is defined for the port, its priority is defined according to the VLAN priority of incoming traffic (P-bit setting). If the incoming user traffic has high priority, it also may interfere with TDM traffic, which has high priority by default.

- Rate limit:
  - Network port: Disable, 256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 10 Mbps, 16 Mbps, 20 Mbps, 25 Mbps, 40 Mbps, 50 Mbps, 80 Mbps
  - User port: Disable, 256 kbps, 512 kbps, 1 Mbps, 2 Mbps, 4 Mbps, 8 Mbps, 16 Mbps, 32 Mbps, 64 Mbps

```
                    LAN Physical Layer Configuration



1. Channel                            Network
2. Channel State                      Enable
3. Auto Negotiation                   Enable
4. Max Capability Advertised          100baseT Full Duplex
5. Default Type                       100baseT Full Duplex
6. VLAN Tagging                       Transparent
7. Default VLAN ID                    1
8. Default VLAN Priority              0
9. Rate Limit(Kbps)                   128 kbps

ESC. Exit                               N. Next
               Current Slot/Channel is  1 /Network



Select item from the menu.
```

Figure 4-6. LAN Physical Layer Configuration Menu

Configuring Ethernet Bridge

4-port Ethernet modules contain internal bridge where with three ports is used as the user ports, and the fourth is used as an Ethernet network port.

Path: Main > Configuration > Physical Layer Configuration > Slot # 1/2 > Bridge Configuration.

➤ **To configure Ethernet bridge:**

1. Follow the path above to display the Bridge Configuration menu (*Figure 4-7*).
2. From the Bridge Configuration menu, do the following:
   - 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.
   - Select **Erase MAC table**, if you intend to delete all learned addresses from the MAC table.

```
                          Bridge Configuration

1. Aging time               >
2. Erase MAC table
3. VLAN Configuration       >
ESC. Exit
                Current Slot  2


Select item from the menu.
```

Figure 4-7. Bridge Configuration Menu

Defining VLANs

Bridge ports of the 4-port Ethernet modules can be defined as members of existing VLANs.

Path: Main > Configuration > Physical Layer Configuration > Slot # 1/2 > Bridge Configuration > VLAN Configuration.

➤ **To define bridge ports as VLAN members:**

1. Follow the path above to access the VLAN Configuration menu (*Figure 4-8*).
2. From the VLAN Configuration menu, configure the following:
   - Channel
     - Network-Eth1
     - User1-Eth2
     - User2-Eth3
   - VLAN ID (Specifies VLAN, which the current bridge port will be a member of): 1–4095
   - Status
     - Enable (Adds the current port as a VLAN member)
     - Disable (Disables VLAN membership of the current port)

```
                          VLAN Configuration

1. Channel                  Network
2. VLAN ID                  0
3. Status                   Disable
>
ESC. Exit
                Current Slot  2


Select item from the menu.
```

Figure 4-8. VLAN Configuration Menu

Configuring E1 Interface

IPmux-8/16 supports up to 8 or 16 E1 links. Each E1 interface must be configured individually.

Path: Main > Configuration > Physical Layer Configuration > Slot # 3/4 > Channel #1–4 or Channel #1–8.

➤ **To configure E1 interface:**

1. Follow the path above to access the E1 Physical Layer Configuration menu (*Figure 4-9*).
2. From the E1 Physical Layer Configuration menu, configure the following:
   - Channel 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)
   - Loopback State (Controls activation of diagnostic loopbacks, see *Diagnostic Loopbacks* in Chapter 6 for detailed loopback function explanation)
     - Internal (Internal loopback is activated)
     - External (External loopback is activated)
     - Disable (All loopbacks are deactivated)
   - Rx sensitivity (Maximum attenuation of the receive signal that can be compensated for by the interface receive path)
     - -10 dB
     - -32 dB
   - Line Type (E1 framing mode)
     - Unframed (Framing is not used)
     - CRC4 Enable (G.704 framing, CRC-4 function enabled)
     - Framed G.704 CRC4 (G.704 framing, CRC-4 function disabled)

Note *The following parameters are masked when the line type is set to unframed:*

- *UpLink Fail Alarm Behavior*
- *Idle Code*
- *Signaling Mode*
- *Cond. Data Pattern*
- *Cond. CAS (ABCD) Pattern*.

- Uplink fail Alarm Behavior (Notification sent to the E1 side if Ethernet link fails)
  - Cond (Conditioning code notification. The code pattern is selected via Cond. Data Pattern parameter.)
  - AIS (alarm indication signal)
- Idle Code (Code transmitted to fill unused timeslots in the E1 frames): 00 to ff.
- Signaling Mode
  - CAS Enable (CAS is enabled)
  - CAS Disable (CAS is disabled)
- Cond. Data Pattern (Conditioning pattern transferred in timeslots toward the IP path when loss of signal, loss of frame or AIS is detected at the E1 line. Conditioning data pattern is also applied to timeslots toward the E1 line when packet receive buffer overrun, underrun or packet loss occurs. In unframed mode, AIS is transmitted.): 00–FF

Note *When CAS is disabled, the Cond CAS Pattern parameter is masked.*

- Cond. CAS (ABCD) Pattern (Conditioning pattern transferred in CAS toward the IP path when loss of signal, loss of frame or AIS is detected at the E1 line. Conditioning data pattern is also applied to CAS sent toward the E1 line when packet receive buffer overrun, underrun or packet loss occurs.): 1–F.

```
                    E1 PHYSICAL LAYER CONFIGURATION

1. Channel Status                          Enable
2. Transmit Clock Source                   Loopback
3. Loopback State                          Disable
4. Rx. Sensitivity                         -10dB
5. Line Type                               CRC4 enable
6. UpLink Fail Alarm Behavior              Cond.
7. Idle Code                               7E
8. Signaling Mode                          CAS enable
9. Cond. Data Pattern                      FF
A. Cond. CAS (ABCD) Pattern                01

  ESC. Exit
               Current Slot/Channel is 4 /1


 Select item from the menu.
```

Figure 4-9. E1 Physical Layer Configuration Menu

Configuring T1 Interface

IPmux-8/16 supports up to 8 or 16 T1 links. Each T1 interface must be configured individually.

Path: Main > Configuration > Physical Layer Configuration > Slot # 3/4 > Channel #1–4 or Channel #1–8.

➤ **To configure T1 interface:**

1. Follow the path above to access the T1 Physical Layer Configuration menu (*Figure 4-10*).
2. From the T1 Physical Layer Configuration menu, configure the following:
   - Channel Status
     - Enable (T1 link is enabled)
     - Disable (T1 link is disabled)
   - Transmit Clock Source
     - Adaptive (Adaptive clock regeneration)
     - Loopback (T1 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)
   - Loopback Configuration (Controls activation of diagnostic loopbacks, see *Diagnostic Loopbacks* in Chapter 6 for detailed loopback function explanation)
   - Line Type (T1 framing mode)
     - Unframed (Framing is not used)
     - T1-D4 (12 frames per multiframe)
     - T1-ESF (24 frames per multiframe)

Note *The following parameters are masked when the line type is set to unframed:*

- *UpLink Fail Alarm Behavior*
- *Restore Time*
- *Idle Code*
- *Signaling Mode*
- *Cond. Data Pattern*
- *Cond. CAS (AB/ABCD) Pattern*
- *Cond. CAS First 2.5 sec Pattern*.

   - Line Code (Line code and zero suppression method used by the port)
     - B7ZS
     - B8ZS
     - AMI

- Line Mode
  - DSU (DSU interface)
  - CSU (CSU interface)
- Line length (DSU mode only, length of a cable in feet between the IPmux-8/16 T1 port connector and the T1 access point):
  - 0–133
  - 133–266
  - 266–399
  - 399–533
  - 533–655
- Tx Gain (CSU mode only, Tx gain level relative to T1 output transmit level)
  - 0 dB – no attenuation
  - 7.5 dB – attenuation of 7.5 dB relative to the nominal transmit level
  - 15 dB – attenuation of 15 dB relative to the nominal transmit level
  - 22.5 dB – attenuation of 22.5 dB relative to the nominal transmit level
- Uplink fail Alarm Behavior (Notification sent to the T1 side if Ethernet link fails)
  - Cond (Conditioning code notification. The code pattern is selected via Cond. Data Pattern parameter.)
  - AIS (alarm indication signal)
- Restore Time (time required for the T1 port to return to normal operation after sync loss):
  - 1 second
  - 10 seconds
- Idle Code (Code transmitted to fill unused timeslots in the T1 frames): 00 to ff.
- Signaling Mode
  - CAS Enable (CAS is enabled)
  - CAS Disable (CAS is disabled)
- Cond. Data Pattern (Conditioning pattern transferred in timeslots toward the IP path when loss of signal, loss of frame or AIS is detected at the T1 line. Conditioning data pattern is also applied to timeslots toward the T1 line when packet receive buffer overrun or underrun occurs. In unframed mode, AIS is transmitted.)
  - 00–FF

Note *The following parameters are masked when CAS is disabled*

- *Cond. CAS (AB/ABCD) Pattern*
- *Cond. CAS First 2.5 sec Pattern*.

- Cond. CAS (AB/ABCD) Pattern (2- or 4-bit code applied to AB (D4) or ABCD (ESF) bits when a fault condition occurs. The ABCD conditioning pattern transferred in CAS toward the IP path when loss of signal, loss of frame or AIS is detected at the T1 line. Conditioning data pattern is also applied to CAS sent toward the T1 line when packet receive buffer overrun or underrun occurs.): 1–F.
- Cond. CAS First 2.5 sec. Pattern (2-or 4-bit code applied (during the first 2.5 seconds) to AB (D4) or ABCD (ESF) bits (relevant in CAS mode only) when fault conditions occur. After the first 2.5 seconds the code specified in 'Cond. CAS (AB/ABCD) pattern' is applied. AB/ABCD conditioning pattern is sent toward the IP path when loss of signal, loss of frame or AIS detected at the T1 line. Conditioning pattern can be sent applied toward the T1 line when packet receive buffer overrun or underrun occurs. When configured to FF, this parameter is ignored.)
  - 0–F (ESF).
  - 0–3 (D4)
  - FF.

```
                    T1 PHYSICAL LAYER CONFIGURATION

1. Channel Status                          Enable
2. Transmit Clock Source                   Loopback
3. Loopback Configuration                  >
4. Line Type                               T1-ESF
5. Line Code                               B8ZS
6. Line Mode                               DSU
7. Line Length(feet)/Tx Gain(dB)           0-133
8. UpLink Fail Alarm Behavior              Cond.
9. Restore Time                            1 second
A. Idle Code                               7E
B. Signaling Mode                          CAS enable
C. Leased Line                             Disable
E. Cond. Data Pattern                      FF
F. Cond. CAS (AB/ABCD) Pattern             01
G. Cond. CAS first 2.5sec pattern(FF=NULL)  FF

  ESC. Exit
               Current Slot/Channel is 4 /1

 Select item from the menu.
```

Figure 4-10. T1 Physical Layer Configuration Menu

Configuring E3 or T3 Interface

IPmux-16 supports up to two E3 or T3 links. Each E3 or T3 interface must be configured individually.

Path: Main > Configuration > Physical Layer Configuration > Slot # 3/4.

➤ **To configure E3 or T3 interface:**

1. Follow the path above to access the E3/T3 Physical Layer Configuration menu (*Figure 4-11*).
2. From the E3/T3 Physical Layer Configuration menu, configure the following:
   - Channel Status
     - Enable (E3/T3 link is enabled)
     - Disable (E3/T3 link is disabled)
   - Transmit Clock Source
     - Adaptive (Adaptive clock regeneration)
     - Loopback (E3/T3 recovered Rx clock is used as the Tx clock)
     - Internal (Tx clock is received from an internal oscillator)
   - Loopback State (Controls activation of diagnostic loopbacks, see *Diagnostic Loopbacks* in Chapter 6 for detailed loopback function explanation)
     - Internal (Internal loopback is activated)
     - External (External loopback is activated)
     - Disable (All loopbacks are deactivated)

```
                    E3/T3 PHYSICAL LAYER CONFIGURATION

1. Channel Status                              Enable

2. Transmit Clock Source                       Loopback

3. Loopback State                              Disable


ESC. Exit
                Current Slot  3


Select item from the menu.
```

Figure 4-11. E3/T3 Physical Layer Configuration Menu

Configuring Channelized T3 Interface

IPmux-16 supports up to two channelized T3 links. Each channelized T3 interface consists of external T3 layer and 28 unframed T1 channels. The external T3 and each T1 channel have to be configured individually.

Configuring External Channelized T3 Interface

Path: Main > Configuration > Physical Layer Configuration > Slot # 3/4 > CT3 EXT.

➤ **To configure external channelized T3:**

1. Follow the path above to access the CT3 Ext. Layer Configuration menu (*Figure 4-12*).
2. From the CT3 Ext. Layer Configuration menu, configure the following:
   - Channel Status
     - Enable (CT3 link is enabled)
     - Disable (CT3 link is disabled)
   - Line Type (T3 framing mode)
     - C_BIT (C_bit Parity)
     - M13 (M13 framing)
   - Transmit Clock Source
     - Loopback (IPmux-8/16 is locked on the T3 clock generated by the adjacent TDM device)
     - Internal (IPmux-8/16 generates the T3 clock towards the adjacent TDM device)

Note *The T3 clock is not propagated over the IP/Ethernet/MPLS to the remote IPmux-16 but it is terminated by IPmux-16 at each end. Therefore the T3 clock should be only synchronized between the T3 device and IPmux-16.*

   - Loopback State (Controls activation of diagnostic loopbacks, see *Diagnostic Loopbacks* in Chapter 6 for detailed loopback function explanation)
     - Internal (Internal loopback is activated)
     - External (External loopback is activated)
     - Disable (All loopbacks are deactivated)
   - Uplink fail Alarm Behavior (Notification sent to the T1s if Ethernet link fails)
     - Cond (Conditioning code notification. The code pattern is selected via Cond. Data Pattern parameter.)
     - AIS (alarm indication signal).

```
                    CT3 EXT. LAYER CONFIGURATION

1. Channel Status                          Enable

2. Line Type                               C_BIT

3. Transmit Clock Source                   Loopback

4. Loopback State                          Disable

5. UpLink Fail Alarm Behavior              Cond.


ESC. Exit
                Current Slot  3


Select item from the menu.
```

Figure 4-12. CT3 External Layer Configuration Menu

Configuring Individual T1 in Channelized T3

Path: Main > Configuration > Physical Layer Configuration > Slot # 3/4 > CT3 T1 1–28 > T1 1–28.

➤ **To configure individual T1 in channelized T3:**

1. Follow the path above to access the CT3 T1 1–28. Layer Configuration menu (*Figure 4-12*).
2. From the CT3 Ext. Layer Configuration menu, configure the following:
   - Channel Status
     - Enable (T1 link is enabled)
     - Disable (T1 link is disabled)
   - Line Type (T1 framing mode)
     - Unframed (Framing is not used)
     - T1-D4 (12 frames per multiframe)
     - T1-ESF (24 frames per multiframe)

Note *IPmux-16 transmits internal T1s as unframed streams. However, the unit detects alarms related to the internal T1 framing. This is why it is important to select the correct T1 line type, which is also required for transmitting the Far End TDM Fail alarm in TDMoIP V2.*

   - Restore Time (time required for the T1 port to return to normal operation after sync loss):
     - 1 second
     - 10 seconds

- Loopback State (Controls activation of diagnostic loopbacks, see *Diagnostic Loopbacks* in Chapter 6 for detailed loopback function explanation)
  - Internal (Internal loopback is activated)
  - External (External loopback is activated)
  - Disable (All loopbacks are deactivated)
- Transmit Clock Source
  - Adaptive (The internal T1 clock is regenerated from the IP/Ethernet/MPLS network)
  - Loopback (The internal T1 clock is locked on the internal T1 clock arriving from the T3 device)
  - Internal (The internal T1 clock is generated by IPmux-16)
  - External (The internal T1 CLK is locked on the external clock port input signal)
  - Port (The T1 clock is regenerated from the IP/ETH/MPLS network. This option is used to configure more than one internal T1 to adaptive clock. When the Port clock source is selected, IPmux-16 displays additional option – Internal T1 Source.)
- Internal T1 Source (To enable the adaptive clock for the current T1 port, enter the number of the internal T1, which is already configured to the adaptive clock source.)

Notes

- *Adaptive mode can be configured for a single internal T1, the rest of the adaptive ports must be set as Port mode.*
- *Although configuration requires indicating the internalT1 number, which is set to adaptive clock, every internal T1 set to the port mode uses its own independent adaptive clock.*
- *It is important to maintain T1 clock integrity end-to-end.*

```
                    CT3 T1 PHYSICAL LAYER CONFIGURATION

1. Channel Status                              Enable

2. Line Type                                   UNFRAMED

3. Restore Time                                1 second

4. Loopback State                              Disable

5. Transmit Clock Source                       Loopback
ESC. Exit
                Current Slot/Channel is  3/T1-1

Select item from the menu.
```

Figure 4-13. CT3 T1 Physical Layer Configuration Menu

Configuring Bundle Connections

E1 and T1 timeslots can be organized into bundles. IPmux-8/16 supports up to 31 (E1) or 24 (T1) bundles per link. The bundles can be connected to any bundle of the TDMoIP device that operates opposite IPmux-8/16. Timeslot configuration is not available for E3, T3, and channelized T3 TDM links.

Note *It is recommended to configure up to 85 bundles per unit.*

Assigning Timeslots to Bundles

Path: Main > Configuration > Time Slots Configuration.

➤ **To assign timeslots to bundles:**

1. Follow the path above to display the Time Slots Configuration menu (see *Figure 4-14*).
2. From the Time Slots Configuration menu, configure the following:
   - Slot/Channel (Specifies IPmux-8/16 slot where the TDM module is installed and the number of the E1/T1 link which is currently being configured)
     - 3, 4 for the slot
     - 1–4 or 1–8 for the link
   - Bundle Number (Number of bundle which is currently being configured)
   - Time slot number (Number of timeslot to be assigned to or freed from the current bundle)
     - 1–31 for E1 or 1–24 for T1

Note

- *No timeslots can be added or removed from an active bundle. The bundle must be disabled first (see Figure 4-15).*
- *Timeslot 0 is reserved for framing information and cannot be assigned to a bundle. Likewise, when CAS is enabled, timeslot 16 is reserved for signaling information.*
- *A list of timeslots assigned to the current bundle and available timeslots for the current E1/T1 link are displayed at the bottom of the Time Slots Configuration menu.*
- *It is possible to create a secondary (redundant) bundle on a current E1/T1 channel by assigning to it timeslots which have already been assigned to the primary (active) bundle. These timeslots are listed as FREE TIME SLOTS FOR REDUNDANCY (see Configuring Bundle Redundancy for a Single Unit without TDM Protection below).*
- *If the port is configured to the unframed mode, it is not possible to assign individual timeslots to a bundle. Full data link at 1544 kbps (T1) or 2048 kbps (E1) is automatically assigned to a bundle in the unframed mode.*

   - Time Slot Current Status
     - Set (Timeslot is assigned to the current bundle)
     - Free (Timeslot is removed from the current bundle)

```
                        TIME SLOTS CONFIGURATION
1. Slot/Channel                                 4/1
2. Bundle Number                                193
3. Time slot number                             1-31
4. Time slot Current Status                     Empty!
ESC. Exit

ACTIVE TIME SLOTS IN THIS BUNDLE:

FREE TIME SLOTS: 11,12,13,14,15,16,17,18,19,20,21,22,23,24, 25,
                 26,27,28,29,30,31

FREE TIME SLOTS FOR REDUNDANCY: 1,2,3,4,5,6,7,8,9,10

Select item from the menu.
```

Figure 4-14. Time Slots Configuration Menu

Connecting Bundles

When the timeslots were assigned to a bundle, it must be connected to a bundle of the remote TDMoIP device. For channelized T3 interface each bundle contains full T1 link, up to 28 bundles can be opened per CT3 module.

Path: Main > Configuration > Bundle Connection Configuration.

➤ **To connect bundles:**

1. Follow the path above to access the Bundle Connection Configuration menu (*Figure 4-15*).
2. From the Bundle Connection Configuration menu, configure the following:
   - DS0 Bundle ID (Selects bundle whose connection you intend to configure)
     - 496 (E1), 384 (T1)

       For CT3 interface, refer to *Table 4-1* to select bundle IDs for the internal T1s.

Table 4-1. Bundle IDs for Internal T1s in Channelized T3 Interface

Internal T1	Bundle ID
1	1
2	9
3	17
4	25
5	33
6	41
7	49

Table 4-1. Bundle IDs for Internal T1s in Channelized T3 Interface (Cont.)

Internal T1	Bundle ID
8	57
9	65
10	73
11	81
12	89
13	97
14	105
15	113
16	121
17	129
18	137
19	145
20	153
21	161
22	169
23	177
24	185
25	193
26	201
27	209
28	217

When an additional CT3 module is installed in slot 4, bundle ID range for its internal T1s starts with ID 249 and incremented by 8 for each additional bundle. For example, 249, 257, 265, ..., 457, 465

- Connection Status
  - Enable (connection is enabled)
  - Disable (no frames are sent on this connection)

Note *Disable Connection Status before changing the following parameters:*
- *Destination IP Address*
- *Next Hop*
- *Destination Bundle.*

- 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 next hop IP address is used. If the default hop IP address is not defined, IPmux-8/16 uses the default gateway IP address.)
  - 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 in × 10 microseconds)
  - E1: 50–3200 (0.5 msec to 32 msec)
  - T1: 50–2400 (0.5 msec to 24 msec)
  - E3: 300–2900 (3 msec to 29 msec)
  - T3: 300–2900 (3 msec to 29 msec)
  - CT3: 50–4200 (0.5 msec to 42 msec)
- TDM Bytes in Frame (x48 bytes) (UDP payload length – this parameter controls Ethernet throughput): 1–30
- OAM Connectivity
  - Enable (The device starts transmitting at full rate after it detects an active, properly configured unit on the other side of the line.)
  - Disable (OAM connectivity is disabled)
- Redundancy Function (Determines the bundle redundancy functionality):
  - Disable (The bundle is not part of protected switching configuration)
  - Primary (The bundle is set as the main bundle. At startup it is selected by IPmux-8/16 as the active bundle.)
  - Secondary (The bundle is set as the backup bundle. At startup it is selected by IPmux-8/16 as the offline bundle.)
- VLAN ID: 1–4095
- VLAN priority: 0–7

Note *VLAN parameters are available only if the VLAN tagging is enabled for the current module in the Host Configuration menu (Figure 4-2).*

- Protocol Version (TDMoIP format):
  - V1 (Old format)
  - V2 (New format, as per ietf-pwe3-tdmoip)

Note *TDMoIP format configuration is not available for E3 and T3 interfaces.*

The Bundle Connection Configuration menu also contains several additional information parameters:

- System Usage – Percentage of the Ethernet uplink that is being currently used. This information is provided for each Ethernet uplink.

Note *For channelized T3 interfaces, when the system usage reaches 100%, the unit does allow adding another bundle on the current Ethernet uplink.*

- Bundle Throughput – Bandwidth used by the current bundle
- Total Throughput – Bandwidth used by all bundles

```
                    BUNDLE CONNECTION CONFIGURATION
1. DS0 Bundle ID                              194
2. Connection Status                          Enable
3. Destination IP Address                     0.0.0.0
4. Next Hop                                   0.0.0.0
5. Destination Bundle                         249
6. Jitter Buffer (x10 usec)                   300
7. TDM bytes in frame (x48 bytes)             Empty!
8. OAM Connectivity                           Disable
9. Redundancy Function                        None
A. VLAN ID                                    10
B. VLAN Priority                              00
C. Protocol Version                           V2

  ESC. Exit                                N. Next

SYSTEM USAGE         BUNDLE THROUGHPUT[BPS]       TOTAL THROUGHPUT[BPS]

LAN 1: Not Applicable            0.0              46600
LAN 2: 12.00%                    46600            497321


Select item from the menu.
```

Figure 4-15. Bundle Connection Configuration Menu

Configuring Internal Cross Connect

IPmux-8/16 allows connect bundles from the same unit internally.

➤ **To connect bundles internally:**

1. Define two bundles (for example 1 and 2).
2. Set the host IP address as destination IP address for both bundles.
3. For bundle 1, set bundle 2 as destination bundle.

   IPmux-8/16 automatically sets bundle 1 as destination bundle for bundle 2.

Note *No configuration parameters can be changed for cross-connected bundles. To reconfigure parameters, delete the bundles and define them anew.*

Configuring the Protection Switching (Bundle Redundancy)

IPmux-8/16 supports 1:1 bundle redundancy, which allows backing up TDMoIP traffic in case of a bundle connection or TDM interface failure.

Path: Main > Configuration > Protection Switching Configuration.

Note *E3/T3 bundle redundancy is available only when the E3 or T3 modules are installed in slot 3.*

➤ **To configure the protection switching:**

1. Follow the path above to access the Protection Switching Configuration menu (*Figure 4-16*).
2. From the Protection Switching Configuration menu, configure the following:
   - Primary Bundle ID (Sets the primary (active) bundle)

Note *Make sure that this bundle is also set as a primary bundle in the Bundle Connection Configuration menu.*

   - Secondary Bundle ID (Sets the secondary (redundant) bundle)

Note *Make sure that this bundle is also set as a secondary bundle in the Bundle Connection Configuration menu.*

   - TDM Fail Time (Determines the time period during which detection of a LOS, LOF, or AIS alarm triggers a flip. This parameter is relevant only if the primary and secondary bundles originate from different TDM ports.)
   - Local Fail Time (Defines a period of time, during which a continuous Local Fail alarm causes a flip)
   - Forced Connection (Forces a specific bundle to be an active bundle regardless of the current redundancy status. No flips occur if the Forced Connection is enabled.)
   - Recovery (Determines whether after performing a redundancy flip, IPmux-8/16 tries to recover to the primary bundle. The recovery flip occurs only if the primary bundle is functioning. When set to No, flipping between the bundles occurs only when the currently active bundle fails. The recovery cannot be performed if the secondary bundle resides in the second IPmux-8/16)
   - Wait-To-Restore Time (Defines a period of time that IPmux-8/16 has to wait before trying to recover to the primary bundle. This option is relevant only when recovery is enabled.)

```
                    PROTECTION SWITCHING CONFIGURATION
1. Primary Bundle ID (0=None)                    0
2. Secondary Bundle ID (0=None)                  0
3. Redundancy Type                               1:1
4. TDM Fail Time                                 Disable

8. Local Fail Time (msec)                        1 sec
9. Forced Connection                             Disable
A. Recovery                                      Yes
B. Wait-To-Restore Time                          0 sec

ESC. Exit                                 N. Next

Select item from the menu.
Use <ESC>-key or keys <1> to <9> and <A> to <B>
```

Figure 4-16. Protection Switching Configuration Menu

Protection Switching Configuration Guidelines

This section provides examples for configuring bundle redundancy.

Configuring Bundle Redundancy for a Single Unit without TDM Protection

Figure 4-17 illustrates a bundle redundancy application (without TDM protection).

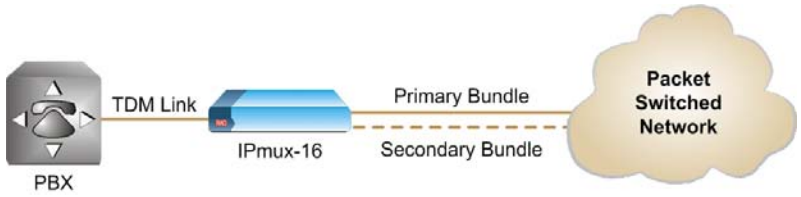


Figure 4-17. Bundle Redundancy without TDM Protection

➤ **To configure bundle redundancy (without TDM protection):**

1. Define host IP and mask IP addresses for Ethernet module 1 and 2.
2. Configure the TDM ports at the physical layer.
3. Assign timeslots to the bundles:
   - Framed mode:
     1. Select a number for a bundle to be configured as a primary bundle.
     2. Assign timeslots to the primary bundle.
     3. Save the changes.
     4. Select a number for a bundle to be configured as a secondary bundle. The bundle must be within the allowed bundle range for the port.

5. Assign to it the same timeslots, which have already been assigned to the primary bundle. These timeslots are listed as Free Time Slots for Redundancy at the bottom of the Time Slots Configuration menu (see *Figure 4-14*).
6. Save the changes.

- Unframed mode: since in the unframed mode all channels timeslots are automatically allocated to the bundle, there is no need to configure a second bundle for redundancy. Any bundle within the allowed bundle range for the port can be activated as the secondary bundle from the Bundle Connection Configuration menu.

4. Connect the configured bundles to the destination bundles.

Note *Bundles defined as redundant to each other are saved with the Connection Status disabled. Their connections are enabled automatically after setting the protected switching configuration.*

- Enable OAM Connectivity.
- Set the desired redundancy type (primary or secondary) for each bundle.

5. Configure the desired protected switching parameters for each bundle.
   - Disable TDM Fail Time.

Configuring Bundle Redundancy for a Single Unit with TDM Protection

Figure 4-18 illustrates a bundle redundancy application (with TDM protection).

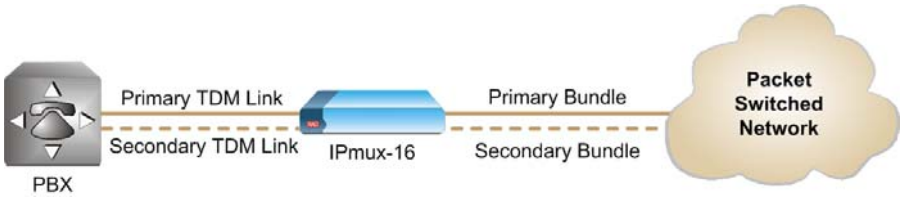


Figure 4-18. Bundle Redundancy with TDM Protection

➤ **To configure bundle redundancy (with TDM protection):**

1. Define host IP and mask IP addresses for Ethernet module 1 and 2.
2. Configure the physical parameters of the desired TDM ports, which are redundant to each other.
3. Define the bundles by assigning timeslots of each TDM port to the appropriate bundle number.
4. Connect the configured bundles to the destination bundles.

Note *Bundles defined as redundant to each other are saved with the Connection Status disabled. Their connections are enabled automatically after setting the protected switching configuration.*

- Enable OAM Connectivity.
- Set the desired redundancy type (primary or secondary) for each bundle.

5. Configure the desired protected switching parameters for each bundle.

Configuring Bundle Redundancy for Two Units (with or without TDM Protection)

Figure 4-19 illustrates a two-unit bundle redundancy application (with or without TDM protection).

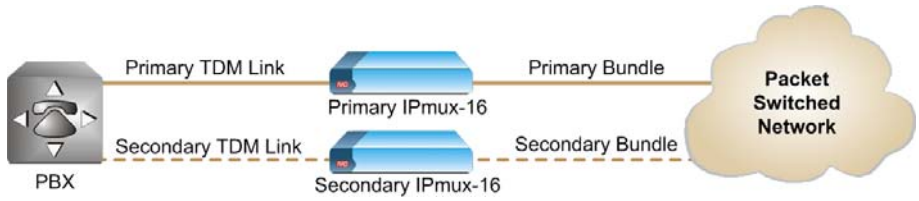


Figure 4-19. Bundle Redundancy for Two Units

➤ **To configure the primary IPmux-8/16:**

1. Define host IP and mask IP addresses for Ethernet module 1.
2. Configure the desired TDM port at the physical layer.
3. Assign timeslots to the primary bundle.
4. Connect the configured bundle to the destination bundle.

Note *Bundle defined as redundant is saved with the Connection Status disabled. Its connection is enabled automatically after setting the protected switching configuration.*

- Enable OAM Connectivity.
- Define redundancy type as Primary.

5. Configure the desired protected switching parameters for the bundle.
   - Set the secondary bundle ID to 0 (None).

➤ **To configure the secondary IPmux-8/16:**

1. Define host IP and mask IP addresses for Ethernet module 1.
2. Configure the desired TDM port at the physical layer.
3. Assign timeslots to the secondary bundle.
4. Connect the configured bundle to the destination bundle.

Note *Bundle defined as redundant is saved with the Connection Status disabled. Its connection is enabled automatically after setting the protected switching configuration.*

- Enable OAM Connectivity.
- Define redundancy type as secondary.

5. Configure the desired protected switching parameters for the bundle.
   - Set the primary bundle ID to 0 (None).

Configuring IP ToS Support

IPmux-8/16 supports enabling or disabling IP ToS support for all network and out-of-band Ethernet ports. This setting applies to all TDMoIP packets transmitted by IPmux-8/16.

You can configure the WHOLE ToS byte field, since different vendors may use different bits to tag packets for traffic prioritization. You can also configure VLAN priority bits for level-2 priority.

Path: Main > Configuration > IP Support.

➤ **To configure IP support:**

1. Follow the path above to access the IP Support menu.
2. From the IP Support menu, select **IP ToS** and set the IP ToS field in the IP frames: 0–255.

Configuring Ethernet Redundancy

When IPmux-8/16 is equipped with two Ethernet modules, it supports fully automatic switching between the Ethernet links in case of the uplink failure.

Path: Main > Configuration > Redundancy Configuration.

➤ **To configure Ethernet redundancy:**

1. Follow the path above to access the Redundancy Configuration menu (*Figure 4-20*).
2. From the Redundancy Configuration menu, select the following:
   - Redundancy (Controls redundancy operation)
     - Enable (Ethernet redundancy is enabled, IPmux-8/16 switches to the secondary link, if the primary link fails)
     - Disable (Ethernet redundancy is disabled)
   - Recovery (Controls recovery operation)
     - Yes (IPmux-8/16 restores the primary link after the Wait to Restore time is elapsed)
     - No (No recovery is performed)
   - Default LAN (Defines the primary Ethernet interface from which the redundancy mechanism starts, and to which it restores)
     - Ethernet 1 (Network interface of Ethernet module installed in slot 1)
     - Ethernet 2 (Network interface of Ethernet module installed in slot 2)
   - Wait to Restore (Defines time period after which IPmux-8/16 attempts to switch to the primary link)
     - 30 Sec.
     - 60 Sec.
   - Enforced LAN (Enforces selected Ethernet interface to remain active, even if a failure occurs)
     - Ethernet 1 (Network interface of Ethernet module installed in slot 1)
     - Ethernet 2 (Network interface of Ethernet module installed in slot 2)
   - Active LAN (Read-only field displaying the currently active link)
   - Last Flip Caused by (Read-only field displaying the cause to the last link flip)

```
                    REDUNDANCY CONFIGURATION

1. Redundancy                              Disable

2. Recovery                                No

3. Default LAN                             Ethernet 1

4. Wait to Restore                         30 sec.

5. Enforced LAN                            No Enforcement


  ESC. Exit
Active LAN: Redundancy Not Configured
Last flip caused by: No flip occurred

Select item from the menu.
```

Figure 4-20. Redundancy Configuration Menu

4.3 Additional Tasks

This section describes additional operations supported by the IPmux-8/16 management software:

- Displaying the IPmux-8/16 general information
- Displaying the bundle configuration summary
- Setting date and time of the IPmux-8/16 internal real-time clock
- Managing files stored in the flash memory
- Assigning name to the device and defining its location
- Transferring software and configuration files
- Resetting the unit.

Displaying the IPmux-8/16 General Information

The IPmux-8/16 General Information screen displays information on current boot, application and backup software versions, as well as the hardware revision of the unit. It also lists all available network and user interfaces of the units along with their software and hardware versions. Power supplies and fan units installed in the chassis are also listed.

Path: Main > System > General Information.

➤ **To display the IPmux-8/16 inventory:**

1. From the Main menu, select **System**.
2. From the System menu, select **General Information**.

   The General Information screen appears (see *Figure 4-21*).

```
Software Versions                                  Hardware Version Inventory No.
 Boot:        2.5 2-8-2004 11:18                     0.2-G/1.1-A      247512
 Application: 6.00D1 6-17-2004 14:21
 Backup:      4.00 11-26-2003 11:26

 Modules    Description        Version                              Inventory No.
 Network    ETH SWITCH UTP     HW:0.0 SW: boot:                        35771824
 Network    ETHERNET UTP       HW:6.0 SW:1.3                           248535
 User       STS1               HW:0.0                                  35743253
 User       8E1 Balanced       HW:3.0                                  141090

 Optional                      Version                                 Status
 Clock unit                    HW:0.0 T1 dsx-1                          O.K.


 Peripherals devices           Present                                 Status
 Power supply1                 Present                                  O.K.
 Power supply2                 Not present                              N/A
 Fan1                          Present                                  O.K.
 Fan2                          Present                                  O.K.

       Press ESC to exit.
```

Figure 4-21. General Information Screen

Displaying Configuration Summary

IPmux-8/16 allows you to display configuration summary for all defined bundles.

Path: Main > Configuration > Configuration Summary.

➤ **To define bundle configuration summary:**

- Follow the path above to display the bundle configuration summary.

  Configuration summary display includes the following information:
  - Bundle – Number of defined bundle
  - Dst – Number of the destination bundle
  - Dst IP.Next Hop – Destination IP address
  - TDM/Jitter – TDM bytes in frame and jitter buffer depth values
  - Assigned TS – Timeslots assigned to the bundle
  - Usage – Uplink bandwidth used by the bundle.

Setting Date and Time

You can set the time for the IPmux-8/16 internal real-time clock.

Path: Main > Configuration > General Configuration > Time/Date Update.

➤ **To set date and time:**

1. Follow the path above to display the Time/Date Update menu (*Figure 4-22*).
2. From the Date/Time Update 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.

```
                              TIME/DATE UPDATE

1. Set Time (hh:mm:ss)       08:17:15

2. Set Date (yyyy-mm-dd)     2004-07-07


ESC. Exit
Select item from the menu:_
```

Figure 4-22. Time/Date Update Menu

Managing File System

IPmux-8/16 contains on-board 16-MB flash memory chip, which stores system and user files. The management software allows viewing the contents of the IPmux-8/16 flash, copying, renaming and deleting user files, and formatting the flash memory.

Path: Main > Configuration > General Configuration > File System.

➤ **To manage the file system:**

1. Follow the path above to access the File System menu (*Figure 4-23*).
2. From the File System menu, do the following:
   - Select **Dir (System Files)** to display all system files stored in the IPmux-8/16 flash.
   - Select **Dir (History Files)** to display all history files stored in the IPmux-8/16 flash.
   - Select **Dir (User Files)** to display all user files stored in the IPmux-8/16 flash.
   - Select **Copy** to copy one of the user files.
     - Enter the name of the file that you intend to copy.
     - Enter a name for the copy of the file.
   - Select **Rename** to rename a user file.
     - Enter the name of the file that you intend to rename.
     - Enter a new name for the file.
   - Select **Delete** to delete a user file.
     - Enter the name of the file that you intend to rename.
     - IPmux-8/16 displays the following confirmation message:
       `Delete XX.LOG ??? (Y/N)`
     - Type **Y** to confirm.
   - Select **Print Code-File Info** to print the file contents.
   - Select **Format Flash** to erase all flash memory contents.

- IPmux-8/16 displays the following confirmation message:
  All file-system will be erased and system will be reset. CONTINUE??? (Y/N)
- Type **Y** to confirm.

```
                    FILE SYSTEM
1. Dir (System Files)
2. Dir (History Files)
3. Dir (User Files)
4. Copy
5. Rename
6. Delete
7. Print Code-File Info
8. Format Flash
ESC. Exit
```

Figure 4-23. File System Menu

Entering Device Information

The IPmux-8/16 management software allows you to assign a name to the unit and specify its location to distinguish it from the other devices installed in your system.

Path: Main > Configuration > General Configuration.

➤ **To enter device information:**

1. Follow the path above to display the General Configuration menu.
2. From the General Configuration menu, select **System Name**, and enter a desired name for the IPmux-8/16 unit.
3. Select **System Location**, and enter the desired name for the current IPmux-8/16 location.

Transferring Files

This section presents procedures for downloading and uploading application, configuration, boot, LAN codes and user files. The files are transferred via XMODEM or TFTP.

Transferring Files via XMODEM

Path: Main > Configuration > General Configuration > Download/Upload > Download/Upload using XMODEM.

➤ **To transfer files using XMODEM:**

1. Follow the path above to display the Download/Upload Using XMODEM menu (see *Figure 4-24*).

2. From the Download/Upload Using XMODEM menu, select File and choose the type of the file which you intend to transfer:
   - Application code
   - Boot code
   - Configuration file
   - User file
   - LAN code.
3. Type **D** to download file to IPmux-8/16 or type **U** to upload file from IPmux-8/16.
4. Send the file to IPmux-8/16 or upload file from the unit using the XMODEM tool of your terminal application.

```
                    DOWNLOAD/UPLOAD using XMODEM

1. File                              Application code
  ESC. Exit        D. Download       U. Upload

Select item from the menu.
```

Figure 4-24. Download/Upload Using XMODEM Menu

Transferring Files via TFTP

Path: Main > Configuration > General Configuration > Download/Upload > Download/Upload using TFTP.

1. Follow the path above to access the Download/Upload using TFTP menu.
2. From the Download/Upload using TFTP menu, configure the following:
   - File name (Name of the file that you intend to transfer)
   - Command (Operation type)
     - Software download
     - Configuration download
     - Configuration upload
     - LAN program file
     - User file download
     - User file upload

Note *It is not possible to download Boot code via TFTP.*

   - Server IP (IP address of the TFTP server)
   - Retry Timeout (Interval between connection retries in seconds).
   - Total Timeout (TFTP connection timeout in seconds)
   - User File Name (Name of the user file to be transferred)
   - View Transfer Status (Current status of the TFTP transfer)

3. Save the changes.

   IPmux-8/16 starts file transfer using TFTP.

```
                    DOWNLOAD/UPLOAD using TFTP

1. File Name                                  FileName.cmp

2. Command                                    No operation

3. Server IP                                  0.0.0.0

4. Retry Timeout                              15

5. Total Timeout                              60

6. User File Name                             XXXXXXXX.YYY

7. View Transfer Status

  ESC. Exit

Select item from the menu.
```

Figure 4-25. Download/Upload Using TFTP Menu

Resetting IPmux-8/16

IPmux-8/16 supports two types of reset:

- Reset to the default settings
- Overall reset of the device.

Resetting IPmux-8/16 to the Defaults

You can reset IPmux-8/16 to its default settings.

Path: Main > Configuration > General Configuration > Set Default Parameters.

➤ **To reset IPmux-8/16 to the default settings:**

1. From the General Configuration menu, select **Set Default Parameters**.

   IPmux-8/16 displays the following message: **`Configuration will be overwritten and system will RESET. Continue ? (Y/N)`**

2. Type **Y** to confirm the reset.

   IPmux-8/16 resets all parameters to their default values and reboots itself.

Notes

- *Setting default parameters from an ASCII terminal erases all the configurations and optionally asks if you want to erase host IP and default gateway values.*
- *Setting default parameters from Telnet or NMS does not erase host IP and default gateway values.*

Resetting IPmux-8/16

You can perform the overall reset of IPmux-8/16.

Path: Main > System > Reset.

➤ **To reset IPmux-8/16:**

1. From the System menu, select **Reset**.

   The following confirmation message appears: **ARE YOU SURE YOU WANT A TOTAL RESET ??? (Y/N)**

2. Type **Y** to confirm the reset.

Chapter 5

Configuring for a Typical Application

This chapter provides detailed instructions for setting up a typical application using IPmux-11 and IPmux-16.

5.1 Overview

Application

The section provides detailed instructions for configuring two IPmux-11 units opposite an IPmux-16 unit, in a point-to-multipoint application including configuration via a supervisory terminal (see *Figure 5-1*).

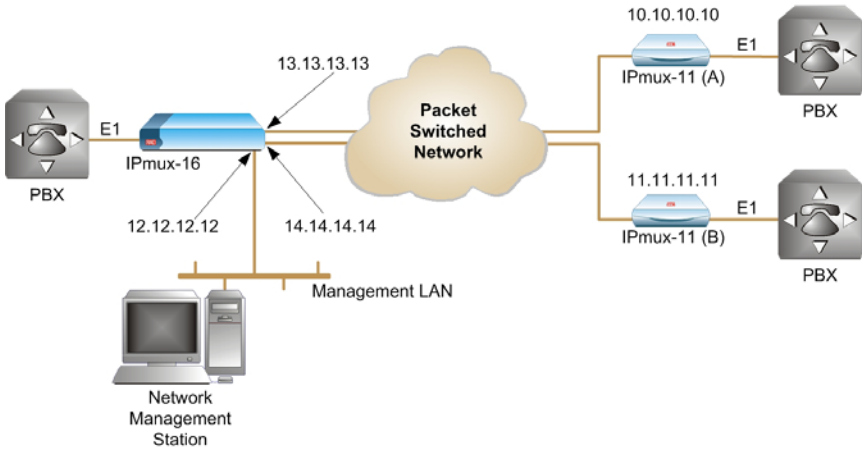


Figure 5-1. Two IPmux-11 Units Operating opposite IPmux-16

Guidelines for Configuring IPmux Units

Certain guidelines are relevant to this application. In general, there are four basic configuration steps (described below) that need to be followed when deploying any IPmux unit.

1. IP Configuration – Setting the device host IP address and the manager IP address.

Note *For IPmux-16 it is necessary to define three IP addresses:*

- *For out-of-band management traffic (optional)*
- *For TDMoIP traffic via Ethernet port 1*
- *For TDMoIP traffic via Ethernet port 2.*

- The IP network can consist of either switches or routers. The minimum requirement is 10 Mbps full duplex.
- An IPmux should be configured with a default gateway/next hop addresses if a routed network is used.
- The manager IP address will be used to manage the agent by the network management station.

2. Physical layer configuration – Setting the TDM parameters (line type, clocking, etc.) according to the application requirements and topology.
   - TDM traffic will be sent between the central IPmux-16 and the two remote IPmux-11 units (A and B) over the IP network.
   - The TDM traffic can be either generated by a BER tester connected to the IPmux units or by a PBX. A remote local loop can be used on the remote IPmux units in order to avoid the need for an additional BER tester.
3. Creating bundles – Allocating timeslots to bundle/s
4. Connecting bundles – Directing the bundles, defined above, to remote IPmux units.

Configuration Summary Table

Table 5-1. Configuration Summary

Device	E1 Parameters	IP Parameters	Bundle Creation	Bundle Connection
IPmux-11 (A)	• Transmit clock source: adaptive • Line type: Framed G.704 CRC-4 disabled • CAS: disabled	Host IP address: 10.10.10.10	Bundle No. 1 Timeslots in bundle: 1–10	IPmux-16 Ethernet port 1
IPmux-11 (B)	• Transmit clock source: adaptive • Line type: Framed G.704 CRC-4 disabled • CAS: disabled	Host IP address: 11.11.11.11	Bundle No. 1 Timeslots in bundle: 1–10	IPmux-16 Ethernet port 2
IPmux-16	• Transmit clock source: loopback • Line type: CRC-4 disabled (framed) • CAS: disabled	• Out-of-band host IP address: 12.12.12.12 • Ethernet port 1 host IP: 13.13.13.13 • Ethernet port 2 host IP: 14.14.14.14	Bundle No. 1, Timeslots in bundle: 1–10	IPmux-11 (A)
			Bundle No. 2, Timeslots in bundle: 11–20	IPmux-11 (B)

The initial configuration of the IPmux-11 and the IPmux-16 needs to be done via an ASCII terminal connected to the IPmux terminal control port. However, after performing the initial configuration (host IP address, default gateway and a manager list), you can manage the units using any of the following options:

- Manage IPmux-11 or IPmux-16 from any IP host using the Telnet protocol. After establishing a Telnet session with the IPmux unit, the Telnet protocol offers the same functionality as the supervisory terminal, enabling remote access over IP networks.
- Manage IPmux-11 or IPmux-16 by means of SNMP-based network management stations, e.g., the RADview TDMoIP Service Center network management station offered by RAD.

5.2 Configuring IPmux-11 Units

This section explains how to configure IPmux-11 units. The configuration procedure is similar for both units, except for defining different destination bundles.

Configuring the IP Parameters

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

1. Display the Host IP menu (**Configuration** > **System** > **Host IP**), and configure the IP address and mask of the host.
2. Save the changes.

➤ **To configure the manager list:**

1. Display the Manager List menu (**Configuration** > **System** > **Management** > **Manager list**), and enter IP parameters for the network manager station.
2. Save the changes.

Configuring E1 Parameters at the Physical Layer

➤ **To configure E1 parameters at the physical layer:**

1. Display the TDM (E1) Configuration menu (**Configuration** > **Physical layer** > **TDM (E1) configuration**), and configure the following parameters:
   - Transmit clock source – Adaptive
   - Line type – Framed G.704.
2. Leave all other parameters with their default values.
3. Save the changes.

Configuring Bundles

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

1. Display the Connection menu (**Configuration** > **Connection**), and assign a number to a bundle.
2. Display the DS0 Bundle Configuration menu (**Configuration** > **Connection** > **DS0 bundle configuration**), and assign timeslots 1 to 10 to the current bundle.

➤ **To connect IPmux-11 bundles:**

1. Display the Bundle Connection Configuration menu (**Configuration** > **Connection** > **Bundle connection configuration**) and configure the following parameters:
   - Destination IP Address – IP address of the IPmux-16 Ethernet 1/2 host, 13.13.13.13 for IPmux-11 (A) and 14.14.14.14 for IPmux-11 (B)
   - Next Hop – IP address of the next hop router (if the destination IP address is not in the same subnet as this IPmux)
   - Destination Bundle – **1** for IPmux-11 (A) and **2** for IPmux-11 (B).
2. Leave all other parameters with their default values.
3. Save the changes.

5.3 Configuring IPmux-16

Configuring the IP Parameters

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

1. Display the Host IP menu (**Configuration** > **General Configuration** > **Management Configuration** > **Host Configuration**), and assign the following IP addresses to the hosts:
   - 12.12.12.12 for out-of-band management host
   - 13.13.13.13 for Ethernet 1 host
   - 14.14.14.14 for Ethernet 2 host.
2. Save the changes.

➤ **To configure the manager list:**

1. Display the Manager List menu (**Configuration** > **General Configuration** > **Management Configuration** > **Manager List**), and enter IP parameters for the network manager station.
2. Save the changes.

Configuring E1 Parameters at the Physical Layer

➤ **To configure E1 parameters at the physical layer:**

1. Display the TDM (E1) Configuration menu (**Configuration** > **Physical Layer Configuration**> **Slot # 3/4** > **Channel 1–4/1–8** > **E1 Physical Layer Configuration**), and configure the following parameters:
   - Transmit Clock Source – Loopback
   - Line Type – CRC4 disable
   - Signaling Mode – CAS disable.
2. Leave all other parameters with their default values.
3. Save the changes.

Configuring Bundles

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

1. Display the Time Slots Configuration menu (**Configuration** > **Time slots Configuration**), and select the following:
   - Slot/Channel – slot and E1 channel contain the timeslots to be assigned to a bundle
   - Bundle number – 1
   - Time slot Number – 1–10
   - Time slot Current Status – SET.
2. Save the changes.
3. Press <Esc> to return to Configuration menu.
4. Display the Time Slots Configuration menu again and select the following:
   - Slot/Channel – slot and E1 channel contain the timeslots to be assigned to a bundle
   - Bundle number – 2
   - Time slot Number – 11–20
   - Time slot Current Status – SET.
5. Save the changes.

➤ **To connect IPmux-16 bundles:**

1. Display the Bundle Connection Configuration menu (**Configuration** > **Bundle connection configuration**) and configure the following parameters:
   - DS0 Bundle ID – **1** for a bundle to be routed to IPmux-11 (A)
   - Destination IP Address – IP addresses of the IPmux-11 (A) host
   - Next Hop – IP address of the next hop router (if the destination IP address is not in the same subnet as this IPmux).
   - Destination Bundle – **1**.
2. Leave all other parameters with their default values.
3. Save the changes.
4. Display the Bundle Connection Configuration menu again and configure the following parameters:
   - DS0 Bundle ID – **2** for a bundle to be routed to IPmux-11 (B)
   - Destination IP Address – IP addresses of the IPmux-11 (B) host
   - Next Hop – IP address of the next hop router (if the destination IP address is not in the same subnet as this IPmux).
   - Destination Bundle – **1**.
5. Save the changes.

5.4 Checking the Application

Once you have finished configuring all the IPmux units, there are several levels on which to check the application:

- The IPmux Statistics screens
- The TDM equipment statistics and functionality.

Step 1 – Using IPmux Statistics

➤ **To check the application using the IPmux Statistics screens:**

1. Select the Performance Monitoring menu in IPmux-16.
2. Select the Bundle Connection Status menu and verify that the connectivity status is OK, and that you don't have any sequence errors, underflows or overflows rising. Verify this for both bundle 1 and bundle 2.
3. If the connectivity status is not OK (either local or remote failure):
   - Check that all cables and physical connections on the IP side are OK.
   - Check that the bundle connection configuration was properly made (enable the OAM mechanism in order to validate the connection sanity).
   - Check that the IP addresses and default gateways are configured correctly.

4. If you have sequence errors and underflows:
   - Check under LAN Statistics that your Ethernet connection is full duplex. If it is detected as half duplex, this could indicate that a problem exists in the autonegotiation mechanism between IPmux and the switch/router. In this case, disable autonegotiation for both devices, set default type for IPmux to full duplex, and either 10 Mbps or 100 Mbps, according to the switch/router capability.
   - Check under LAN Statistics that only the correct frames and correct octets are received and transmitted. If other counters are rising, check the physical connection of the IP side (cables, switch/router port, etc.).
5. If you have underflows or overflows at set intervals of time:
   - Check that all IPmux units are configured to the correct clock modes.
   - Check that the TDM device is configured to the correct clock mode.
6. If you have underflows or overflows at non-set intervals of time:
   - Try to gradually increase the jitter buffer size.
   - Check that there are no E1alarms (such as LOS or LOF), through the IPmux E1/T1 Statistics. If problems do exist on the E1/T1 level, check both physical connections (cables and E1 ports) and E1/T1 parameter configuration compatibility between the TDM equipment and the IPmux units (such as CRC and CAS Enable/Disable).
   - Check that the bundle connection configuration was made correctly.

Step 2 – Using TDM Equipment Statistics and Functionality

After you have verified all the issues in step 1, check the following:

- Check that there are no alarms or BER on the TDM equipment.

If you are using a PBX check voice quality. If an echo exists, verify that you haven't configured the jitter buffer size to be too large (remember that the initial configuration should be 3 ms, unless it is required to be larger).

Chapter 6

Troubleshooting and Diagnostics

This chapter discusses:

- Error detection by LEDs or alarms
- Diagnostic tests
- Troubleshooting
- Technical support information.

6.1 Monitoring IPmux-8/16 Performance

IPmux-8/16 provides powerful performance monitoring and statistics collection tools, which consist of the following:

- Physical port statistics – Status of the physical layer parameters for the Ethernet, E1, T1, E3, T3, and channelized T3 interfaces.
- Bundle connection statistics – TDMoIP bundle/s connection status at the Ethernet/IP network level.

Monitoring Physical Port Performance

IPmux-8/16 collects statistic data for all unit interfaces (LAN and TDM) at the physical layer.

Displaying Ethernet Statistics

IPmux-8/16 allows viewing current status of the network LAN port, as well as statistic data on the received and transmitted frames.

Path: Main > Performance Monitoring > Physical Port Statistics > Slot # 1/2.

➤ **To display Ethernet statistics:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Physical Port Statistics**.
3. From the Physical Layer Statistics menu, select **Slot # 1** or **Slot # 2**.

   Physical Port Statistics screen for the first LAN port of the selected module is displayed (see *Figure 6-1* and *Figure 6-2*). *Table 6-1* and *Table 6-2* explain the Ethernet statistic parameters provided by IPmux-8/16.

4. From the Physical Port Statistics menu, select **Port** and enter the number of the LAN port, which statistics you intend to display (1 for 1-port Ethernet modules, 1–4 for 4-port Ethernet modules).
5. Type **R** to reset the Ethernet counters.

```
                          PHYSICAL PORT STATISTICS
ETHERNET UTP
 Mac Address                          00-20-D2-20-98-24
 Mode                                 full duplex
 Rate(Mbps)                           100
 Status                               Connected
 Active Link                          Redundancy Not Configured

 Frames received from the user
 Correct frames:                       287709257
 Correct Octets:                      2424794390
 Alignment Err:                              0
 FCS Errors:                                 0

 Frames transmitted to the user
 Correct frames:                       289609257
 Correct Octets:                      2616784790
 Sngl Collision:                             0
 Mlty Collision:                             0
 Deferred transm:                            0
 Late Collision:                             0
 Carrier Sense:                              0
--------------------------------------------------------------------------------
 Slot -  1         1.Port -  1
 ESC. Exit        R. Reset Counters
```

Figure 6-1. Physical Port Statistics (1-Port Ethernet Module)

```
                          PHYSICAL PORT STATISTICS
ETH SWITCH UTP
 Mac Address                          00-20-D2-21-D5-B0
 Mode                                 half duplex
 Rate(Mbps)                           10
 Status                               Not connected
 Active LAN                           Redundancy Not Configured

 Frames received from the user
 Total frames:                               0
 Total Octets:                               0
 Oversize frames:                            0
 Fragments:                                  0

 Frames transmitted to the user
 Jabber:                                     0
 Dropped frames:                             0
 CRC errors:                                 0
 Correct frames:                             0
 Correct Octets:                             0
 Collision:                                  0
--------------------------------------------------------------------------------
 Slot -  1         1.Port -  1
 ESC. Exit        R. Reset Counters
```

Figure 6-2. Physical Port Statistics (4-Port Ethernet Module)

Table 6-1. Ethernet Statistic Parameters (1-Port Ethernet Module)

Parameter	Description
MAC Address	MAC address of the local port.
Mode	Port mode is set either manually or via the autonegotiation mode (under LAN configuration screen). ***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/forced manually. Half-duplex degradation will occur also when autonegotiation is enabled at one port and disabled at the opposite port.*
Rate (Mbps)	Port rate is set either manually or via the auto negotiation mode.
Status	Link status: Connected – Normal operation. Not connected – Ethernet link loss
Frames Received from the User	
Correct Frames	The number of frames successfully received. When a valid connection is established the number should increase steadily.
Correct Octets	The number of octets successfully received. When a valid connection is established the number should increase steadily.
Alignment Errors	The number of frames received that are not an integral number of octets in length (RFC 1643). All frames should end on an 8-bit boundary, but physical problems on the network could cause the number of bits to deviate from the multiple of eight.
FCS Errors	Counts the number of frames received that do not pass the FCS check (RFC 1643). An FCS check is a mathematical way to ensure that all the frame bits are correct without the system having to examine each bit and compare it against the original.
Frames Transmitted to the User	
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.
Single Collision	Collisions occur only in half duplex mode (RFC 1643). Counts the successfully transmitted frames for which transmission is inhibited by exactly one collision (see Collision above).
Multi Collision	Multi Collisions occur only in half duplex mode (RFC 1643). Counts the successfully transmitted frames for which transmission is inhibited by more than one collision (multi-collision).
Deferred Transmission	Occur only in half-duplex mode (RFC 1643). Counts the number of frames for which the first transmission attempt (carrier sense) is delayed because the medium is busy. This is normal behavior when trying to transmit high traffic rate in a half-duplex environment. The higher the traffic rate is, the higher the chances of collisions and deferred transmissions.
Late Collision	Occur only in Half-duplex mode (RFC 1643). In order to allow collision detection to work properly, the period in which collisions are detected is restricted (512 bit-times). For 10BaseT Ethernet (10 Mbps), it is 51.2 msec (microseconds), and for Fast Ethernet (100 Mbps), 5.12 msec. For Ethernet stations, collisions can be detected up to 51.2 microsec after the beginning of the transmission, or in other words: up to the 512th bit of the frame. When a station detects a collision after it has sent the 512th bit of its frame, this is counted as a late collision.
Carrier Sense	The counter increments when a packet collides because carrier sense is disabled.

Table 6-2. Ethernet Statistic Parameters (4-Port Ethernet Module)

Parameter	Description
MAC Address	MAC address of the current port
Mode	Port mode is set either manually or via the autonegotiation process. ***Note**: When autonegotiation protocols do not support each other, this degrades connection to a half-duplex mode.* *In order to avoid this, autonegotiation should be disabled and the ports should be configured/forced manually. Half-duplex degradation will occur also when autonegotiation is enabled at one port and disabled at the opposite port.*
Rate (Mbps)	Port rate is set either manually or via the autonegotiation mode
Status	Link status: Connected – Normal operation. Not connected – Ethernet link loss
Active LAN	Displays a currently active LAN port, if Ethernet redundancy is enabled
Frames received from the user	
Total Frames	The number of frames successfully received. When a valid connection is established the number should increase steadily.
Total Octets	The number of octets successfully received. When a valid connection is established the number should increase steadily.
Oversize Frames	Number of received frames which meet the following conditions: • Frame data length equals or is greater than 1518/1536 bytes • Frame has valid CRC
Fragments	Number of received frames which meet the following conditions: • Frame data length is less than 64 bytes • Frame has invalid CRC • Collision event has not been detected • Late collision event has not been detected
Frames transmitted to the user	
Jabber	Number of received frames which meet the following conditions: • Frame data length is greater than 1518/1536 bytes • Frame has invalid CRC
Dropped	Number of received dropped packets
CRC Errors	Number of received frames which meet the following conditions: • Frame data length is between 64 and 1518/1536 bytes • Frame has invalid CRC • Collision event has not been detected • Late collision event has not been detected
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.
Collision	Number of received frames with collision event detected

Displaying E1/T1 Statistics

E1/T1 statistics refer to the physical status of the E1/T1 traffic reaching the IPmux 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.

Path: > Performance Monitoring > Physical Port Statistics > Slot # 3/4.

➤ **To view the E1/T1 connection statistics:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Physical Port Statistics**.
3. From the Physical Layer Statistics menu, select **Slot # 3** or **Slot # 4**.
4. Select E1 or T1 channel (**1**–**4** or **1**–**8**).

   Physical Port Statistics screen for the first E1 or T1 port of the selected module is displayed (see *Figure 6-3*). *Table 6-3* explains the E1/T1 statistic parameters provided by IPmux-8/16.
5. From the Physical Port Statistics menu, select **Interval** and enter the number of the 15-minute, which statistics you intend to display (**1**–**96**), or type **N** or **P** to browse the stored interval statistics.

   Interval time indication is presented as follows:
   - Time Since – Time (in seconds) elapsed since the beginning of the currently active interval.
   - Start Time – Time and date of the beginning of the stored interval.

Note *The current active interval is always marked as interval 0, the previous interval is marked as 1 and so on. Whenever a new interval is started, the counters are reset to zero. The E1/T1 counters cannot be reset manually.*

```
                          PHYSICAL PORT STATISTICS
8E1 Balanced
 LOS:                    |                    900
 LOF (Red):              |                      0
                         |
 LCV:                    |                      0
                         |
 RAI (Yellow):           |                      0
 AIS:                    |                      0
 FEBE:                   |                      0
                         |
 BES:                    |                      0
 DM:                     |                      0
 ES:                     |                     10
 SES:                    |                      0
 UAS:                    |                    900
                         |
 LOMF:                   |                      0
                         |
--------------------------------------------------------------------------------
Start Time: 2002-03-21 22:15:00                  Valid Intervals        96
    Slot/Channel             4/1        1. Interval Num         6
 ESC. Exit        P. Prev Inv        N. Next Inv
```

Figure 6-3. Physical Port Statistics (E1 Port)

Table 6-3. E1/T1 Statistic Parameters

Alarm	Description	Recommendation
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 can also be noticeable when the SYNC LED is off (Green indicates proper synchronization).	Check the physical layer (connectors, cables, etc.)

Table 6-3. E1/T1 Statistic Parameters (Cont.)

Alarm	Description	Recommendation
LOF (Red)	A Loss of Frame indicates that the IPmux 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 can also be noticeable when the SYNC LED is off. When the IPmux enters a Red alarm condition, it sends an Yf bit (Yellow alarm or RAI) towards the adjacent E1/T1 device.	Check all framing related parameters (CRC-4, CAS enabled/disabled, ESF/D4 (for T1), etc.), and physical connections.
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.	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 (loses synch). RAI 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 can also be noticeable when the SYNC LED is flashing.	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. When receiving AIS, the SYNC LED turns off.	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 counter will increase by one for each second during which the FEBE indication is received.	Check physical link integrity.

Table 6-3. E1/T1 Statistic Parameters (Cont.)

Alarm	Description	Recommendation
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).	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).	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.	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.	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.	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 TS16 MSB in frame 0 for two consecutive multi frames. Available only for E1 Multi-Frame mode (CAS).	Check physical link integrity, signaling method (CAS enable only), and framing-related parameters.

Table 6-3. E1/T1 Statistic Parameters (Cont.)

Alarm	Description	Recommendation
Inband Loop	T1 interface only. Displays the current status of the inband loopback. **External** – Loopback Location (Configuration > T1 Physical Layer Configuration > T1 Loopback Configuration) is set to Local System and IPmux-8/16 detected a loopback activation code sent from the adjacent TDM device. **Internal** – Loopback Location (Configuration > T1 Physical Layer Configuration > T1 Loopback Configuration) is set to Remote System and IPmux-8/16 detected a loopback activation code sent from the adjacent TDM device. This indication appears in the remote IPmux-8/16. **Disable** – No inband loopbacks are currently active.	
LLB Loop	T1 interface only. Displays the current status of the inband loopback activated via F-bit. **On** – Leased Line (Configuration > T1 Physical Layer Configuration) is set to Disable and IPmux-8/16 detected a loopback activation code sent from the adjacent TDM device on the F-bit. **Off** – Leased Line (Configuration > T1 Physical Layer Configuration) is set to Enable or IPmux-8/16 does not detect a loopback activation code sent from the adjacent TDM device on the F-bit.	
Transmitting Loop Code	T1 interface only. **On** – The local IPmux-8/16 has received indication from the remote unit configured to the Transparent mode (Configuration > T1 Physical Layer Configuration > T1 Loopback Configuration > Loopback Location) that the remote TDM device is transmitting an inband loopback code.	

Displaying E3/T3 Statistics

E3/T3 statistics refer to the physical status of the E3/T3 traffic reaching the IPmux from the adjacent E3/T3 device.

Path: > Performance Monitoring > Physical Port Statistics > Slot # 3/4.

➤ **To view the E3/T3 connection statistics:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Physical Port Statistics**.
3. From the Physical Layer Statistics menu, select **Slot # 3** or **Slot # 4**.

   Physical Port Statistics screen for E3 or T3 port is displayed (see *Figure 6-4*). *Table 6-4* explains the E3/T3 statistic parameters provided by IPmux-8/16.
4. From the Physical Port Statistics menu, select **Interval** and enter the number of the 15-minute, which statistics you intend to display (**1**–**96**), or type **N** or **P** to browse the stored interval statistics.

Interval time indication is presented as follows:

- Time Since – Time (in seconds) elapsed since the beginning of the currently active interval.
- Start Time – Time and date of the beginning of the stored interval.

Note *The current active interval is always marked as interval 0, the previous interval is marked as 1 and so on. Whenever a new interval is started, the counters are reset to zero. The E3/T3 counters cannot be reset manually.*

```
                          PHYSICAL PORT STATISTICS
E3 over COAX
 LOS:                     |                          0
                          |
                          |
                          |
                          |
 AIS:                     |                          0
                          |
                          |
                          |
                          |
 ES:                      |                          0
 SES:                     |                          0
 UAS:                     |                          0
                          |
                          |
                          |
-------------------------------------------------------------------------------
Start Time: 2002-03-21 22:15:00                Valid Intervals        96
    Slot/Channel             3/1        1. Interval Num         6
 ESC. Exit        P. Prev Inv        N. Next Inv
```

Figure 6-4. Physical Port Statistics (E3 Port)

Table 6-4. E3/T3 Statistic Parameters

Alarm	Description
LOS	The LOS defect is declared upon observing 175 +/- 75 contiguous pulse positions with no pulses of either positive or negative polarity. The LOS defect is terminated upon observing an average pulse density of at least 33% over a period of 175 +/- 75 contiguous pulse positions starting with the receipt of a pulse.
AIS	The AIS is framed with "stuck stuffing." This implies that it has a valid M-subframe alignments bits, M-frame alignment bits, and P bits. The information bits are set to a 1010 sequence, starting with a one (1) after each M-subframe alignment bit, M-frame alignment bit, X bit, P bit, and C bit. The C bits are all set to zero giving what is called "stuck stuffing." The X bits are set to one. The E3/T3 AIS defect is declared after E3/T3 AIS is present in contiguous M-frames for a time equal to or greater than T, where 0.2 ms ≤ T ≤ 100 ms. The E3/T3 AIS defect is terminated after AIS is absent in contiguous M-frames for a time equal to or greater than T. The E3/T3 binary content of the AIS is nominally a continuous stream of ones. When receiving AIS, the SYNC LED turns off.
ES	Number of Errored Seconds in the current interval. Any second containing the following error events: • Line Errored Seconds (LES) • P-bit Errored Seconds (PES) • C-bit Errored Seconds (CES).
SES	Number of Line Severely Errored Seconds in the current interval. A Any second containing the following errored events is counted as severely errored seconds: • P-bit Severely Errored Seconds (PSES) • C-bit Severely Errored Seconds (CSES) • Severely Errored Framing Seconds (SEFS).
UAS	Number of Unavailable Seconds in the current interval. The line becomes unavailable if 10 consecutive SESs appear. The 10 SESs are included in the UAS time. The link becomes available if 10 consecutive seconds pass with no SESs. The 10 seconds with no SESs are excluded from the UAS.

Displaying Channelized T3 Statistics

Channelized T3 statistics refer to the physical status of the CT3 traffic reaching the IPmux from the adjacent device.

Path: > Performance Monitoring > Physical Port Statistics > Slot # 3/4.

➤ **To view the channelized T3 statistics:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Physical Port Statistics**.
3. From the Physical Layer Statistics menu, select **Slot # 3** or **Slot # 4**.

   Physical Port Statistics screen for channelized T3 port is displayed (see *Figure 6-5*). *Table 6-5* explains the channelized T3 statistic parameters provided by IPmux-8/16.

4. From the Physical Port Statistics menu, select **Interval** and enter the number of the 15-minute, which statistics you intend to display (1–96), or type **N** or **P** to browse the stored interval statistics.

   Interval time indication is presented as follows:

   - Time Since – Time (in seconds) elapsed since the beginning of the currently active interval.
   - Start Time – Time and date of the beginning of the stored interval.

Note *The current active interval is always marked as interval 0, the previous interval is marked as 1 and so on. Whenever a new interval is started, the counters are reset to zero. The CT3 counters cannot be reset manually.*

```
                          PHYSICAL PORT STATISTICS
CT3
 LOS:                    |                           0
 LOF                     |                           0
                         |
                         |
 RAI                     |                           0
 AIS:                    |
                         |
 LES                     |                           0
 PES                     |                           0
 PSES                    |                           0
 CES                     |                           0
 CSES:                   |                           0
 SEFS:                   |                           0
 UAS:                    |                           0
                         |
                         |
--------------------------------------------------------------------------------
Start Time: 2002-03-21 22:15:00                 Valid Intervals        96
    Slot/Channel             3/1        1. Interval Num         6
 ESC. Exit        P. Prev Inv        N. Next Inv
```

Figure 6-5. Physical Port Statistics (CT3 Port)

Table 6-5. CT3 Statistic Parameters

Alarm	Description
LOS	The LOS defect is declared upon observing 175 +/- 75 contiguous pulse positions with no pulses of either positive or negative polarity. The LOS defect is terminated upon observing an average pulse density of at least 33% over a period of 175 +/- 75 contiguous pulse positions starting with the receipt of a pulse.
LOF	T3 Loss of Frame (LOF) failure is declared when the T3 OOF defect is consistent for 2 to 10 seconds. The T3 OOF defect ends when reframe occurs. The LOF failure is cleared when the OOF defect is absent for 10 to 20 seconds.
RAI	The Remote Alarm Indication (RAI) failure is declared after detecting the Yellow Alarm Signal on the alarm channel. The Remote Alarm Indication failure, in C-bit Parity T3 applications, is declared as soon as the presence of either one or two alarm signals are detected on the Far End Alarm Channel. The Remote Alarm Indication failure may also be declared after detecting the far-end SEF/AIS defect. The Remote Alarm Indication failure is cleared as soon as the presence of the any of the above alarms are removed. Also, the incoming failure state is declared when a defect persists for at least 2-10 seconds. The defects are the following: Loss of Signal (LOS), an Out of Frame (OOF) or an incoming Alarm Indication Signal (AIS). The failure state is cleared when the defect is absent for less than or equal to 20 seconds.
AIS	The AIS is framed with "stuck stuffing." This implies that it has a valid M-subframe alignments bits, M-frame alignment bits, and P bits. The information bits are set to a 1010 sequence, starting with a one (1) after each M-subframe alignment bit, M-frame alignment bit, X bit, P bit, and C bit. The C bits are all set to zero giving what is called "stuck stuffing." The X bits are set to one. The T3 AIS defect is declared after E3/T3 AIS is present in contiguous M-frames for a time equal to or greater than T, where 0.2 ms ≤ T ≤ 100 ms. The T3 AIS defect is terminated after AIS is absent in contiguous M-frames for a time equal to or greater than T. The T3 binary content of the AIS is nominally a continuous stream of ones. When receiving AIS, the SYNC LED turns off.
LES	Line Errored Second is a second in which one or more CV occurred or one or more LOS defects.
PES	P-bit Errored Seconds. An PES is a second with one or more PCVs OR one or more Out of Frame defects or a detected incoming AIS. This counter is not incremented when UASs are counted.
PSES	P-bit Severely Errored Seconds. PSES is a second with 44 or more PCVs or one or more Out of Frame defects or a detected incoming AIS. This counter is not incremented when UASs are counted.
CES	C-bit Errored Seconds. An CES is a second with one or more CCVs or one or more Out of Frame defects or a detected incoming AIS. This counter is not incremented when UASs are counted.
CSES	C-bit Severely Errored Seconds. CSES is a second with 44 or more CCVs OR one or more Out of Frame defects or a detected incoming AIS. This counter is not incremented when UASs are counted.
SEFS	Severely Errored Framing Seconds. A SEFS is a second with one or more Out of Frame defects or a detected incoming AIS. This counter is not incremented when UASs are counted.
UAS	Number of Unavailable Seconds in the current interval. The line becomes unavailable if 10 consecutive PSESs appear. The 10 PSESs are included in the UAS time. The link becomes available if 10 consecutive seconds pass with no PSESs. The 10 seconds with no PSESs are excluded from the UAS.

Displaying Bundle Connection Data

IPmux-8/16 allows viewing the following bundle connection data:

- Current connection status per bundle
- Bundle connection statistics per bundle and per interval.

Displaying Bundle Connection Status

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

Path: Main > Performance Monitoring > Bundle Connection Status.

➤ **To view the bundle connection status:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Bundle Connection Status.**
   The Bundle Connection Status screen appears (*Figure 6-6*).
3. From the Bundle Connection Status screen, select **Bundle Number** and enter the number of the bundle which connection status you intend to display.

   or

   Type **F** to view the status of the next open bundle.
4. Type **R** to reset the counters.

```
                        BUNDLE CONNECTION STATUS

 Next Hop MAC Address:                          |    Not Exist
 Connectivity Status:                           |    Not Exist
 Last Flip Cause:                               |    N/A
 FarEnd TDM Status                              |   O.K.
                                                |
                                                |
 Sequence Errors:                               |            0
 Jitter Buffer Underflows:                      |            0
 Jitter Buffer Overflows:                       |            0
 Redundancy Flips:                              |            0
-------------------------------------------------------------------------------
 1. Bundle Number            1

 ESC. Exit        F. Forward connection        R. Reset Counters
```

Figure 6-6. Bundle Connection Status

Table 6-6 lists the bundle connection status parameters.

Notes

- *For bundles cross-connected internally, the Next Hop MAC Address is set to N/A, and the Connectivity Status is OK – loop to the cross-connected bundle.*
- *If Connectivity Status is Disabled, there is no value for Next Hop Mac Address.*
- *There is a set of counters for each bundle separately. The counters count errors only when the bundle is active.*
  When a bundle changes state from active to stand-by, its "Redundancy Flips" counter is increased. This is true also in 1:1 box redundancy, where the single bundle in the box is "hushed" by the remote side.

Table 6-6. Bundle Connection Status Parameters

Parameter	Possible Values	Description
Next Hop MAC Address		In this screen Next Hop Mac Address displayed is in fact the resulting Mac Address of the ARP process for the destination IP address.
	N/A	Indicates that a cross connection was made and this field is irrelevant.
	FFFFFFFF	Indicates an unreachable bundle
Connectivity Status	O.K.	Ethernet frames are received on the local and remote IPmux-8/16
	OK-LOOP	Cross-connection has been successfully made
	Remote Fail	Ethernet frames are not received by the remote IPmux-8/16.
	Local Fail	Ethernet frames are not received by the local IPmux-8/16
	Disabled	Bundle connection is disabled
	Validation Fail	Configuration of the local and remote IPmux units are not compatible
	Unavailable	Remote unit is not identified as an IPmux (available when the OAM Connectivity is enabled)
Last Flip Cause	Cause for the last bundle redundancy flip	
FarEnd TDM Status		Status of the remote TDM port, to which the remote bundle belongs. This parameter is relevant only for the new TDMoIP format (V2).
	O.K.	Remote TDM port operates properly
	Fail	Remote TDM port failure is detected. E1/T1 failures: loss of synchronization (red alarm), loss of signal, AIS CT3 failures: loss of frame, AIS, loss of signal at internal (T1) or external (CT3) level
	Unknown	Status of the remote TDM port cannot be retrieved. This occurs when the current bundle is in Local Fail status or it is unavailable.
	N/A	The current bundle is configured to the old TDMoIP format (V1)

Table 6-6. Bundle Connection Status Parameters (Cont.)

Parameter	Description
Sequence Errors	Each packet transmitted by IPmux holds a sequence number. The receiving IPmux 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 traffic has sufficient bandwidth. See FAQ 2636 for throughput calculation. • Make sure Ethernet connection is functioning properly. • 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 FAQ 3107. • Make sure the network devices do not drop/lose/ignore packets.

Table 6-6. Bundle Connection Status Parameters (Cont.)

Parameter	Description
Jitter Buffer Underflow	The IPmux 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 at a constant rate, but the problem is that they are reaching the opposite IPmux 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. 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, the IPmux instantly flashes the jitter buffer, causing a forced underflow. Underflow events initiated by the device (after an overflow event) will not be enumerated in the jitter buffer underflow counter. 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 application, and that the "TDM bytes in frame" parameter is identical in both IPmux units. • 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 each IPmux "UDP destination Port" field.

Table 6-6. Bundle Connection Status Parameters (Cont.)

Parameter	Description
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 is not 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. Recommendations: • Check network devices and try increasing Jitter Buffer configuration. • Check system's clocking configuration • Make sure the same amount of timeslots for bundle is configured on each side of the IPmux application, and that the "TDM bytes in frame" parameter is identical in both IPmux units.
Redundancy Flips	Number of occurred bundle redundancy flips

Configuring Intervals for Bundle Statistics Collection

You can set the interval for the bundle statistics collection, as well the statistics threshold. The intervals can be set for the following bundle events:

- JIT BUF UFLOWS
- JIT BUF OFLOWS
- SN ERRORS.

Path: Main > System > Event Log > Update Bundle Connection Events or Bundle Connection Events Threshold.

➤ **To configure intervals for bundle statistic collection:**

- From the Event Log menu, 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.

  With the interval set to 1 minute, a new START event (such as SN ERRORS START SLOT1 PORT1 BNDL1) is stored in the event log if the number of errors has been above threshold during the last minute.

A new END event (such as SN ERRORS END SLOT1 PORT1 BNDL1) is stored in the event log if the number of errors has been below threshold during the last minute.

With the interval set to 1 second, an event specifying the number of errors that occurred during the last second is stored in the event log. The even is stored if a number of errors exceeded threshold. For example, SN ERRORS END SLOT1 PORT1 BNDL1 20 EV'S means that within the last second 20 sequence errors occurred. This event is logged only if the threshold has been configured to a value from 1 to 19.

Displaying Bundle Connection Statistics

Bundle Connection Statistics screen provides information on the sequence errors and jitter buffer underflow/overflow counters. Statistics are collected for 96 150-minute intervals for every open bundle.

Path: Main > Performance Monitoring > Bundle Connection Statistics.

➤ **To view the bundle connection status:**

1. From the Main menu, select **Performance Monitoring**.
2. From the Performance Monitoring menu, select **Bundle Connection Statistics**.
   The Bundle Connection Statistics screen appears (*Figure 6-7*).
3. From the Bundle Connection Statistics screen, select **Bundle Number** and enter the number of the bundle which connection status you intend to display.

   or

   Type **F** to view the status of the next or previous open bundle.
4. From the Bundle Connection Statistics screen, select **Interval** and enter the number of the 15-minute, which statistics you intend to display (**1**–96**),** or type **N** or **P** to browse the stored interval statistics.

   Interval time indication is presented as follows:
   - Time Since – Time (in seconds) elapsed since the beginning of the currently active interval.
   - Start Time – Time and date of the beginning of the stored interval.

Note *The current active interval is always marked as interval 0, the previous interval is marked as 1 and so on. Whenever a new interval is started, the counters are reset to zero.*

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

```
                        BUNDLE CONNECTION STATISTICS

 Sequence Errors:                        |      empty
                                         |
 Jitter Buffer Underflows:               |      empty
 Jitter Buffer Overflows:                |      empty
                                         |
 Max Jitter Buffer Deviation:            |      empty
 Current MIN Jitter Buffer count:        |
 Current MAX Jitter Buffer count:        |
                                         |
-------------------------------------------------------------------------
Start Time: 2002-03-22 15:30:00                  Valid Intervals        26
 1. Interval Number           11
 2. Bundle Number             1

 ESC. Exit        F. Forward connection        P. Prev Inv        N. Next Inv
 Use <ESC>-key, Digit keys or Abc keys from menu
```

Figure 6-7. Bundle Connection Statistics

Table 6-6. Bundle Connection Statistics Parameters

Parameter	Possible Values / Remarks
Sequence Errors	The number of seconds a frame was dropped because frames were received from the network with SN fields not equal to the last SN+1 (or 2)
Jitter Buffer Underflows	The number of times frames were dropped because the receive buffer was in an underrun state. The buffer enters underflow state when: • Sequence errors occur • Flow underrun takes place due to PDV expiration • An overflow condition occurs.
Jitter Buffer Overflows	Number of times that frames were dropped because the receive buffer exceeded the maximum allowed depth
Max Jitter Buffer Deviation	Maximum deviation from the middle of the jitter buffer, in units of 10 μs.
Current MIN Jitter Buffer Count	Minimum jitter buffer usage registered during the last 1second. This value may be positive or negative, illustrating the overflow or underflow tendency.
Current MAX Jitter Buffer Count	Maximum jitter buffer usage registered during the last 1second. This value may be positive or negative, illustrating the overflow or underflow tendency.

6.2 Handling Alarms and Traps

IPmux-8/16 maintains an event log file that stores up to 2000 events. All events are time-stamped. The user can view the contents of the event log file via an ASCII terminal or a network management station. The user can also clear the contents of the log file.

Displaying Events

Path: Main > System > Event Log > Read LogFile.

➤ **To access the event log:**

1. From the Main menu, select System.
2. From the System menu, select **Event Log**.
3. From the Event Log menu, select **Read LogFile.**
   The Read Log File screen appears (see *Figure 6-8*).
4. In the Read Log File screen, type **N** to display the next page of the event log or **P** to display its previous page.

```
                              LOGFILE EVENTS
 Index                  Log entry
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 28
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 28
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 27
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 27
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 26
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 26
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 25
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 25
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 24
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 24
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 23
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 23
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 22
   2002-03-15 13:27:50 LOF END             Slt 3 Int DS1 22
   2002-03-15 13:27:50 AIS END             Slt 3 Int DS1 21


--------------------------------------------------------------------------------
   N. Next


   ESC. Exit
```

Figure 6-8. Read Log File

Clearing Events

Path: Main > System > Event Log > Clear LogFile.

➤ **To clear the event log:**

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

   IPmux-8/16 displays the following message:
   Logfile will be cleared. Continue ??? (Y/N)

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

Table 6-7 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-8/16 must be checked by the authorized technical support personnel.

Table 6-7. Event List

Event	Description	Corrective Action
COLD_START	IPmux-8/16 is powered up	None
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 ERR	IPmux-8/16 has encountered an internal fatal error	IPmux-8/16 requires servicing
JIT BUF OFLOWS STRT SLOTx PORTy BNDLz	Jitter buffer overflow occurred on slot X port Y bundle Z	See Jitter Buffer Overflow in *Table 6-6*
JIT BUF OFLOWS END SLOTx PORTy BNDLz	Jitter buffer overflow state on slot X port Y bundle Z has ended	See Jitter Buffer Underflow in *Table 6-6*
JIT BUF UFLOWS STRT SLOTx PORTy BNDLz	Jitter buffer underflow occurred on slot X port Y bundle Z	See Jitter Buffer Overflow in *Table 6-6*
JIT BUF UFLOWS END SLOTx PORTy BNDLz	Jitter buffer underflow state on slot X port Y bundle Z has ended	See Jitter Buffer Underflow in *Table 6-6*
SN ERRORS START SLOTx PORTy BNDLz	Sequence errors have been detected on slot X port Y bundle Z	See Sequence Errors in *Table 6-6*
SN ERRORS END SLOTx PORTy BNDLz	Sequence errors on slot X port Y bundle Z have ended	See Sequence Errors in *Table 6-6*
JIT BUF UFLOWS SLOTx PORTy BNDLz n EV'S	The N number of jitter buffer underflow events have been detected on slot X port Y bundle Z	See Jitter Buffer Underflow in *Table 6-6*
JIT BUF OFLOWS SLOTx PORTy BNDLz n EV'S	The N number of jitter buffer overflow events have been detected on slot X port Y bundle Z	See Jitter Buffer Overflow in *Table 6-6*

Table 6-7. Event List (Cont.)

Event	Description	Corrective Action
SN ERRORS SLOTx PORTy BNDLz n EV'S	The N number of sequence errors have been detected on slot X port Y bundle Z	See Sequence Errors in *Table 6-6*
LINE AIS END	LINE AIS state detected has ended	None
LINE AIS START	IPmux-8/16 has AIS (alarm indicator signal) state on one of its E1/T1 channels	Check for a fault at the SDH network, on the receive direction
LINE FEBE END	LINE FEBE state detected has ended	None
LINE FEBE START (SDH module only)	IPmux-8/16 has LINE FEBE state on one of its E1/T1 channels	Check for errors in the E1/T1 connection on the transmit direction
LINE RDI END	LINE RDI state detected has ended	None
LINE RDI START	IPmux-8/16 has LINE RDI (remote defect indicator) state on one of its E1/T1 channels	Check for an E1/T1 connectivity fault on the transmit side
LOCAL FAIL	Ethernet frames are not received by the local IPmux-8/16 on the specified connection	Check Ethernet/IP path
LOF END	LOF state detected has ended	None
LOF START	IPmux-8/16 has a LOF (Loss of frame synchronization) state on one of its E1/T1 channels	Check port cable connection Check input signal
LOS END	LOS state detected has ended	
LOS START	IPmux-8/16 has a LOS (loss of signal) state on one of its E1/T1 channels	Check the port cable connection Check input signal
PS1_ACTIVE OR PS2_ACTIVE	One of the IPmux-8/16 power supply units is powered on	None
PS1_NOT_ACTIVE OR PS2_NOT_ACTIVE	One of the IPmux-8/16 power supply units is powered off	Check the external mains supply
REMOTE FAIL	Ethernet frames are not received by the remote IPmux-8/16 on the specified connection	Check Ethernet/IP path
SYS USER RESET	IPmux-8/16 was reset by the user	None

Note *Behavior of the Jitter Buffer Overflow, Jitter Buffer Underflow and Sequence Error depends on the setting of the interval and threshold setting. See explanation under Configuring Intervals for Bundle Statistics Collection below.*

Masking Alarm Traps

You can mask some IPmux-8/16 alarm to prevent their traps from being sent to the management stations.

Path: Main > Configuration > General Configuration > Management Configuration > Alarm Traps Mask.

➤ **To mask an alarm:**

1. Follow the path above to access the Alarm Traps Mask menu (*Figure 6-9*).

2. From the Alarm Traps Mask menu, select **Alarm ID** to choose alarm that you intend to mask. *Table 6-8* lists all traps supported by IPmux-8/16, traps which have alarm ID can be masked.
3. Select **Trap Status** to activate or mask alarm traps.

```
                              ALARM TRAPS MASK
1. Alarm ID <refer to Manual>            1
2. Trap status                           Masked
ACTIVE ALARM TRAPS: 2, 6, 8
ESC. Exit
Select item from the menu
```

Figure 6-9. Alarm Traps Mask Menu

Table 6-8. IPmux-8/16 Traps

Alarm ID	Alarm Description, Severity	Trap Sent to NMS
1	Loss of Signal (LOS Physical Layer), major	alarmLOS 1.3.6.1.4.1.164.6.1.3.0.7
2	Loss of Frame (LOF Physical Layer), major	alarmLOF 1.3.6.1.4.1.164.6.1.3.0.8
6	Alarm Indication Signal Received (AIS Line Physical Layer), major	alarmAIS 1.3.6.1.4.1.164.6.1.3.0.10
8	Remote Defect Indication Received (RDI Line Physical Layer), major	alarmRDI 1.3.6.1.4.1.164.6.1.3.0.11
21	Far End Block Error (FEBE Line Layer), major	alarmFEBE 1.3.6.1.4.1.164.6.1.3.0.12
23	External clock source has failed, minor	clkSrcChangeTrap 1.3.6.1.4.1.164.6.1.0.10
26	Bundle connectivity status, see *Displaying Bundle Connection Status* above. • O.K – major • Remote fail – minor • Local fail – major • Validation Fail – major • Unavailable – major	bundleConnectionStatusTrap 1.3.6.1.4.1.164.6.1.3.0.15
	IPmux-8/16 is powered up	rfc1215.coldStart 1.3.6.1.6.3.1.1.5.1
	Physical port (TDM or Ethernet) is down, major	rfc1215.linkDown 1.3.6.1.6.3.1.1.5.3
	Physical port (TDM or Ethernet) is up	rfc1215.linkUp 1.3.6.1.6.3.1.1.5.4

Table 6-8. IPmux-8/16 Traps (Cont.)

Alarm ID	Alarm Description, Severity	Trap Sent to NMS
	IPmux-8/16 SNMP agent received SNMP request with a wrong community name	rfc1215.authenticationFailure 1.3.6.1.6.3.1.1.5.5
	Used by TFTP application during file download	TftpStatusChangeTrap 1.3.6.1.4.1.164.6.1.0.1
	Used by RADview application for node status indication	AgnStatusChangeTrap 1.3.6.1.4.1.164.6.1.0.2
	Used by RADview application for path status indication	AgnCounterChange 1.3.6.1.4.1.164.6.1.0.6
	Generated for: • Power supply failure ▪ ps1NotActive(3), major ▪ ps1Active(4), minor ▪ ps2NotActive(5), major ▪ ps2Active(6), minor • Fan failure ▪ fan1Ok(17), minor ▪ fan1Fail(18), major ▪ fan2Ok(19), minor ▪ fan2Fail(20), major • Heat alarm ▪ heatAlarmOff(7), minor ▪ heatAlarmOn(8), major • General alarms. General alarms generated by an external circuit connected to the ALARMS connector.	SystemTrap 1.3.6.1.4.1.164.6.1.3.0.6

Working with Alarm Relay

IPmux-8/16 includes an alarm relay port which has two functions:

- Dry contact – a trigger for an external monitoring equipment when one of the alarms become active
- General purpose input port – it generates a system trap to the NMS when triggered from an external device.

Alarms are classified to 3 categories:

- Major alarm – all physical alarms, power supply and fan failures
- Minor alarm – alarms related to IP bundle status: ID 26, 27
- General alarm – a circuit between one of the four general-purpose discrete input pins and GND is closed.

All alarms are reported in the system Event Log.

Activating Minor/Major Alarms

The first step is to activate all relevant alarms in IPmux-8/16 via a terminal or an NMS. This is performed via the Management Configuration screen.

- Major alarm in IPmux-8/16 – a relay between pins 4 and 9 is closed.
- Minor alarm in IPmux-8/16 – a relay between pins 3 and 5 is closed.
- General alarm – used for generating traps towards the NMS and the IPmux-8/16 Event Log file, in case of external user equipment failure, such as air-conditioning failure. In order to enable this alarm, connect an external circuit to one of the general alarm pins: 1, 2, 6, 7 and to the ground pin= no.8. Upon circuit closure between 8 and 1, 2, 6 or 7, a general alarm is reported in the IPmux-8/16 Event Log file and a trap is sent to the NMS (set the **System Trap Option** in the **Manager List** window to **On).** A Log file entry is recorded regardless of the system trap option configuration.

Notes

- *A major alarm caused by a power supply or fan failure will always be activated in the dry contact; it cannot be masked.*
- *For general alarm there is no need to supply external voltage; the external equipment should only close the circuit.*

Warning

For minor or major alarms, the monitoring equipment should supply an input voltage that does not exceed 30 VDC or VAC 2A, or 60 VDC 1A.

6.3 Testing the Units

IPmux-8/16 diagnostic capabilities include loopbacks, ping test and route tracing utility.

Running Diagnostic Loopbacks

IPmux-8/16 supports activation of the internal and external loopbacks.

External Loopback

IPmux-8/16 can be set to an external loopback to test the connection between a TDM 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 6-10*).

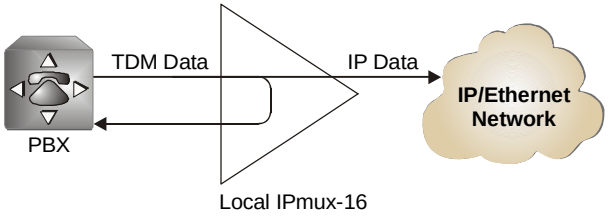


Figure 6-10. External Loopback

Internal Loopback

A TDM interface module can be set to an internal loop to test the connection between the TDM 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 remote PBX connected to the TDM port (see *Figure 6-11*).

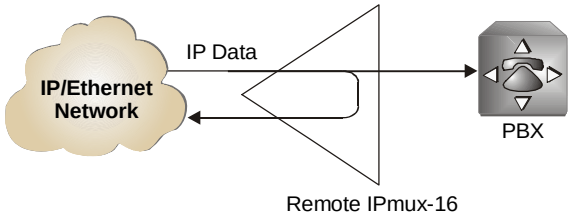


Figure 6-11. Internal Loopback

➤ **To run a loopback test:**

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

   The Configuration menu appears.

2. From the Configuration menu, select **Physical Layer Configuration**.

   The Physical Layer Configuration menu appears.

3. From the Physical Layer Configuration menu, select a TDM module slot to proceed to the E1, T1, E3, T3 or CT3 physical layer configuration:
   - E1, T1 module – select the channel (**1**–**4** or **1**–**8**)
   - E3, T3 module – the E3/T3 Physical Layer Configuration menu is displayed immediately after selecting E3/T3 module slot.
   - Channelized T3 – select **CT3 EXT**. from the Channelized T3 Physical Layer Configuration menu.

4. From the E1/E3/T3/CT3 Physical Layer Configuration menu, select **Loopback State**.

   For T1 interfaces, select **Loopback Configuration** from the Physical Layer Configuration menu, then select **Loopback State.**

5. Press the <**Spacebar**> to toggle between: **Internal**, **External**, **Disable**.

6. Press **<Enter>** when the desired loopback state value is displayed. Selecting **Disable** disables a running loopback.

Activating T1 Inband Loopbacks

T1 physical loopbacks can be activated by receiving a loopback activation code from TDM equipment connected to the T1 port. Loopback activation code is sent on a whole T1 frame.

When loopback activation code is received, IPmux-8/16 activates external or internal loopback, or transmits the code transparently to the remote TDM equipment.

➤ **To activate an inband loopback:**

- From the Loopback Configuration, perform the following:
  1. Select **Loopback State** and set it to Disable.
  2. Select **Loopback Location** and set it as follows:
     - Local System (External loopback is activated in the local IPmux-8/16)
     - Remote System (Internal loopback is activated in the remote IPmux-8/16)
     - Transparent (Loopback activation code is transmitted to the remote TDM device, which closes the loopback)
     - Disable (IPmux-8/16 ignores inband activation code).
  3. Define **Activate Loop Pattern** (8-bit code to be sent by the adjacent TDM device in order to activate a loopback)
  4. Define **Deactivate Loop Pattern** (8-bit code to be sent by the adjacent TDM device in order to deactivate a loopback).

```
                    T1 LOOPBACK CONFIGURATION

1. Loopback State                          Disable
2. Loopback Location                       Local System
3. Activate Loop Pattern                   10000
4. Deactivate Loop Pattern                 100

Select item from the menu.
```

Figure 6-12. T1 Loopback Configuration Menu

Running Ping Test

You can ping remote IP host to check the IPmux-8/16 IP connectivity.

➤ **To ping an IP host:**

1. From the Main menu, select **System**.
   The System menu is displayed.
2. From the System menu, select **Ping**.
   The Ping menu is displayed (see *Figure 6-13*).
3. From the Ping menu, enter IP address of the host that you intend to ping.
4. Press **<Spacebar>** to define the number of pings (**1**, **2**, **3**, **4** or **Endless Repeats**).
5. Press **<Enter>** to start pinging.

```
                                    PING
Enter Destination IP And Press Enter.
Destination IP: 14.12.13.15
Use Space Bar To Choose Ping Repetitions.
Ping Repetitions: 1

    |-------------------------------------------------------------------|
    | Ping Result: Host 14.12.13.15  Request Timed Out.                 |
    |-------------------------------------------------------------------|




Press Esc. to Exit, Or Any Other Key To Refresh The Screen

ESC. Exit
```

Figure 6-13. Ping Menu

Tracing the Route

This diagnostic utility traces the route through the network from IPmux-8/16 to the destination host.

➤ **To trace a route:**

1. From the System menu, select **Trace Route**.

   The Trace Route menu is displayed (see *Figure 6-14*).

2. From the Trace Route menu, enter an IP address of the host to which you intend to trace route, and press **<Enter>**.

   IPmux-8/16 starts tracing the route, displaying the IP addresses of all hop nodes.

3. Press **<Esc>** to stop the tracing.

```
                                 TRACE ROUTE
Enter Destination IP And Press Enter.
Destination IP: 12.12.12.12
Tracing route to 12.12.12.12 over a maximum of 30 hops
..............




ESC. Stop Tracing
```

Figure 6-14. Trace Route Menu

6.4 Troubleshooting

Table 6-9 lists faults and describes the actions required to correct the event (alarm) indication.

Table 6-9. Troubleshooting Chart

Fault	Probable Cause	Remedial Action
The E1/T1 equipment connected to IPmux-8/16 is not synchronized (E1/T1 level) with IPmux-8/16	Configuration problems	1. Check IPmux-8/16 port configuration and, if necessary, other IPmux-8/16 parameters. 2. Check E1/T1 physical connection (use loopbacks).
Slips and errors in E1/T1 equipment	• Ethernet port in switch and IPmux-8/16 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 – bundle connection status menu) • Network PDV or Lost Frames	1. Check E1/T1 physical connection (use loopbacks) and E1/T1 statistics. 2. Check timing settings according to explanation in this manual. 3. Check switch and IPmux-8/16 port configuration (negotiation, rate, duplex mode) and check Ethernet statistics. 4. Check PDV introduced by the network, and, if necessary, increase PDVT jitter buffer setting.
Echo in voice		1. Check network delay and try to decrease it. 2. Try to decrease PDVT (jitter) buffer.

6.5 Frequently Asked Questions

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

A: 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 timeslots (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 timeslots 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.

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

A: 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.

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

A: 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. PC 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, IPmux-11 up to 300 msec, IPmux-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.
- 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.

6.6 Technical Support

Technical support for this product can be obtained from the local distributor from whom it was purchased.

For further information, please contact the RAD distributor nearest you or one of RAD's offices worldwide. This information can be found at www.rad.com (offices – About RAD > Worldwide Offices; distributors – Where to Buy > End Users).

Appendix A
Interface Connector Specifications

A.1 E1 and T1 Connectors

The E1 and T1 interfaces of IPmux-8/16 terminate in an 8-pin RJ-45 connector, wired in accordance with *Table A-1*.

Table A-1. E1/T1 Connector Pinouts

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-8/16 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, wired in accordance with.

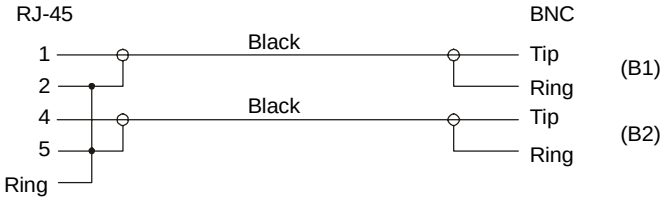


Figure A-1. CBL-RJ45/2BNC Cable Wiring Diagram

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+
6	Rx–
4, 5, 7, 8	Not used

A.3 CONTROL Connector

Control Port Connector Pinout

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

Table A-3. CONTROL Connector Pinout

Pin	Signal	Function
1	DCD	Data Carrier Detect
2	RXD	Receive data
3	TXD	Transmit data
4	DTR	Data Terminal Ready
5	GND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indicator

Cross Cable Wiring

Cross cable (CBL-DB-9/DB-9/NULL) is supplied with IPmux-8/16 for an ASCII terminal connection. The cable includes two 9-pin D-type male connectors. *Figure A-2* Illustrates the wiring of the cable. The following pins are connected to each other:

- DCD (pin 1), DTR (pin 4) and DSR (6) on each DB-9 connector
- RTS (pin 7) and CTS (pin 8) on each DB-9 connector.

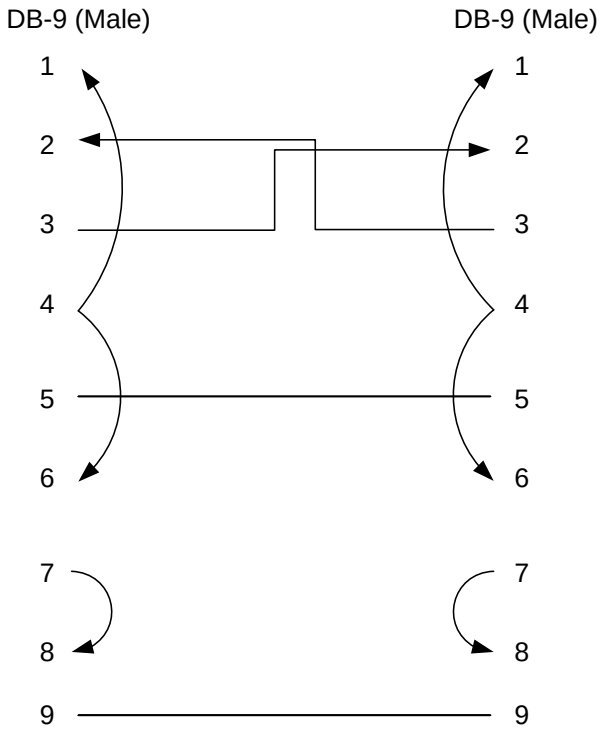


Figure A-2. CBL-DB-9/DB-9/NULL Cable Wiring

A.4 Alarm Connector

The dry contact alarm relay terminates in a 9-pin D-type female connector. *Table A-4* lists the connector wiring.

Table A-4. Alarm Relay Connector Pinout

Pin No.	Signal Name
1	General Alarm 1
2	General Alarm 2
3	Minor Alarm
4	Major Alarm
5	Minor Alarm
6	General Alarm 3
7	General Alarm 4
8	GND
9	Major Alarm

A.5 External Clock Connector

The external clock interface terminates in an 8-pin RJ-45 connector, wired in accordance with *Table A-5*.

Table A-5. External Clock Port Pin Assignment

Pin	Signal Name	Function
1	RRING	Rx
2	RTIP	Rx
3	GND	Usually not connected
4	TRING	Tx
5	TTIP	Tx
6	GND	Usually not connected
7, 8	–	Not connected

Appendix B

Boot Sequence for Downloading Software

This appendix provides a description of the IPmux-8/16 boot procedure.

The IPmux-8/16 software is stored in the flash memory in two sections, in the boot sector and in the file system. The boot sector holds a boot program that calls up the rest of the program from the file system.

The file system can hold two compressed copies of the IPmux-8/16 code. One copy is called the **operating file**, and the other is called the **backup file**. The operating file is the default-executable IPmux-8/16 code. The backup file is used whenever the operating file is absent or corrupted.

B.1 Booting IPmux-8/16

IPmux-8/16 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-8/16 configuration.

Figure B-1 shows the Boot menu.

```
                              BOOT MENU

The IPmux-8/16 File System can store two versions for each application file.
One is called Operating File and the Second is called Backup File.

    0. Exit
    1. Swap main CPU application File: Operating <-> Backup
    2. Download NEW Operating file (any application file)
       (existing Operating file will be saved as Backup)
    3. Delete main CPU Operating File
       (existing Backup file will be saved as Operating)
    4. Delete All Configuration files (CDB + CFG)
    5. Delete CDB file
    6. Delete CFG file
    7. Format File System (Delete all files: Software and Configuration files)

Type in one of the above option numbers (or <ESC> to exit): _
```

Figure B-1. Boot Screen

Boot Sequence

The IPmux-8/16 boot procedure comprises the following stages:

1. The boot program searches for the operating file in the file system:
   - If the file exists, a message appears on the screen and the program continues.
   - If the file does not exist, the boot program searches for the backup file, renames the file to **Operating file** (a message appears on the screen) and continues.
   - If there is no backup file, you must download a file via the out-of-band interface (XMODEM protocol). The received file is saved as the operating file in the file system.
2. Files in the file system are compressed and automatically decompressed into the RAM memory before execution begins. A message appears on the screen.

   After decompression, the IPmux-8/16 software starts to execute and the user can begin working.

If the system is working normally, the entire process is completed within two minutes.

Accessing the Boot Menu

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

If an operating file exists in the file system, there is a three-second delay. To access the boot menu, press <**Ctrl+A**> within this delay interval; the boot menu is displayed. (If you do not press <**Ctrl+A**> within three seconds, booting will continue normally.)

From the boot menu, you can:

- Exchange the operating and backup files
- Download a new operating file; the previous operating file is saved as the backup file
- Delete the operating file; the backup file becomes the operating file
- Delete the configuration file
- Delete all the software and configuration files.

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

Appendix C

SNMP Management

This appendix provides specific information for IPmux-8/16 management by SNMP (Simple Network Management Protocol).

The SNMP management functions of IPmux-8/16 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-8/16 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-8/16 SNMP agent are:

- rfc1213.mib (except the interfaces view which is supported via RFC 2233)
- ianaiftype.mib (defines the ifType)
- rfc2233.mib (IF-MIB)
- rfc1493.mib
- rfc2665.mib
- rfc1907.mib
- rfc2493.mib
- ces.mib
- rfc2495.mib (except Far End objects and RW configuration objects which are different for each configuration) – replaces RFC 1406, which is now obsolete.
- rfc2494.mib
- rfc2239.mib
- IP-MUX RAD private mib

The IPmux-8/16 object id is **iso (1).org(3).dod(6).internet(1).private(4).enterprises(1).rad(164).radGen(6). systems(1).radAce(3).radIPmux16(81)**

Enterprise-specific MIBs supported by RAD equipment, including IPmux-8/16, 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-8/16 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-8/16 SNMP agent stores the IP address of the Network Management Station (NMS) that is intended to manage it.

Index

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-8, IPmux-16

Publication Number: 118-200-07/06

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: _____

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

NORTH AMERICA 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. 118-200-07/06