Prisma Mini FiberLinX-II Installation Instructions

Overview

This document provides instructions for installing, configuring, and troubleshooting the Prisma® Mini FiberLinX-II media converter module.

These modules allow fiber network operators to connect to and manage remote network segments.

Purpose

This document provides product information and instructions for installing the Prisma Mini FiberLinX-II module.

Qualified Personnel

Only appropriately qualified and skilled service personnel should attempt to install, operate, maintain, and service this product.

WARNING:

Allow only qualified and skilled personnel to install, operate, maintain, and service this product. Otherwise, personal injury or equipment damage may occur.

In This Document

Important Safety Instructions

Read and Retain Instructions

Carefully read all safety and operating instructions before operating this equipment, and retain them for future reference.

Follow Instructions and Heed Warnings

Follow all operating and use instructions. Pay attention to all warnings and cautions in the operating instructions, as well as those that are affixed to this equipment.

Terminology

The terms defined below are used in this document. The definitions given are based on those found in safety standards.

Service Personnel - The term *service personnel* applies to trained and qualified individuals who are allowed to install, replace, or service electrical equipment. The service personnel are expected to use their experience and technical skills to avoid possible injury to themselves and others due to hazards that exist in service and restricted access areas.

User and Operator - The terms *user* and *operator* apply to persons other than service personnel.

Ground(ing) and Earth(ing) - The terms *ground(ing)* and *earth(ing)* are synonymous. This document uses ground(ing) for clarity, but it can be interpreted as having the same meaning as earth(ing).

Electric Shock Hazard

This equipment meets applicable safety standards.

WARNING:

To reduce risk of electric shock, perform only the instructions that are included in the operating instructions. Refer all servicing to qualified service personnel only.

Electric shock can cause personal injury or even death. Avoid direct contact with dangerous voltages at all times. The protective ground connection, where provided, is essential to safe operation and must be verified before connecting the power supply.

Know the following safety warnings and guidelines:

- Dangerous Voltages

- Only qualified service personnel are allowed to perform equipment installation or replacement.
- Only qualified service personnel are allowed to remove chassis covers and access any of the components inside the chassis.

- Grounding
  - Do not violate the protective grounding by using an extension cable, power cable, or autotransformer without a protective ground conductor.
  - Take care to maintain the protective grounding of this equipment during service or repair and to re-establish the protective grounding before putting this equipment back into operation.

Installation Site

When selecting the installation site, comply with the following:

- **Protective Ground** - The protective ground lead of the building's electrical installation should comply with national and local requirements.
- **Environmental Condition** – The installation site should be dry, clean, and ventilated. Do not use this equipment where it could be at risk of contact with water. Ensure that this equipment is operated in an environment that meets the requirements as stated in this equipment's technical specifications, which may be found on this equipment's data sheet.

Installation Requirements

WARNING:

Allow only qualified service personnel to install this equipment. The installation must conform to all local codes and regulations.

Equipment Placement

WARNING:

Avoid personal injury and damage to this equipment. An unstable mounting surface may cause this equipment to fall.

To protect against equipment damage or injury to personnel, comply with the following:

- Install this equipment in a restricted access location.
- Do not install near any heat sources such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.
- Place this equipment close enough to a mains AC outlet to accommodate the length of this equipment's power cord.

- Route all power cords so that people cannot walk on, place objects on, or lean objects against them. This may pinch or damage the power cords. Pay particular attention to power cords at plugs, outlets, and the points where the power cords exit this equipment.
- Use only with a cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with this equipment.
- Make sure the mounting surface or rack is stable and can support the size and weight of this equipment.
- The mounting surface or rack should be appropriately anchored according to manufacturer's specifications. Ensure this equipment is securely fastened to the mounting surface or rack where necessary to protect against damage due to any disturbance and subsequent fall.

Ventilation

This equipment has openings for ventilation to protect it from overheating. To ensure equipment reliability and safe operation, do not block or cover any of the ventilation openings. Install the equipment in accordance with the manufacturer's instructions.

Rack Mounting Safety Precautions

Mechanical Loading

Make sure that the rack is placed on a stable surface. If the rack has stabilizing devices, install these stabilizing devices before mounting any equipment in the rack.

WARNING:

Avoid personal injury and damage to this equipment. Mounting this equipment in the rack should be such that a hazardous condition is not caused due to uneven mechanical loading.

Reduced Airflow

When mounting this equipment in the rack, do not obstruct the cooling airflow through the rack. Be sure to mount the blanking plates to cover unused rack space. Additional components such as combiners and net strips should be mounted at the back of the rack, so that the free airflow is not restricted.

CAUTION:

Installation of this equipment in a rack should be such that the amount of airflow required for safe operation of this equipment is not compromised.

Elevated Operating Ambient Temperature

Only install this equipment in a humidity- and temperature-controlled environment that meets the requirements given in this equipment's technical specifications.

CAUTION:

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, install this equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.

Handling Precautions

When moving a cart that contains this equipment, check for any of the following possible hazards:

WARNING:

Avoid personal injury and damage to this equipment! Move any equipment and cart combination with care. Quick stops, excessive force, and uneven surfaces may cause this equipment and cart to overturn.

- Use caution when moving this equipment/cart combination to avoid injury from tip-over.
- If the cart does not move easily, this condition may indicate obstructions or cables that may need to be disconnected before moving this equipment to another location.
- Avoid quick stops and starts when moving the cart.
- Check for uneven floor surfaces such as cracks or cables and cords.

Grounding

This section provides instructions for verifying that the equipment is properly grounded.

Safety plugs (USA only)

This equipment is equipped with either a 3-terminal (grounding-type) safety plug or a 2-terminal (polarized) safety plug. The wide blade or the third terminal is provided for safety. Do not defeat the safety purpose of the grounding-type or polarized safety plug.

To properly ground this equipment, follow these safety guidelines:

- **Grounding-Type Plug** - For a 3-terminal plug (one terminal on this plug is a protective grounding pin), insert the plug into a grounded mains, 3-terminal outlet.

  Note: This plug fits only one way. If this plug cannot be fully inserted into the outlet, contact an electrician to replace the obsolete 3-terminal outlet.

- **Polarized Plug** - For a 2-terminal plug (a polarized plug with one wide blade and one narrow blade), insert the plug into a polarized mains, 2-terminal outlet in which one socket is wider than the other.

Note: If this plug cannot be fully inserted into the outlet, try reversing the plug. If the plug still fails to fit, contact an electrician to replace the obsolete 2-terminal outlet.

Grounding terminal

If this equipment is equipped with an external grounding terminal, attach one end of an 18-gauge wire (or larger) to the grounding terminal; then, attach the other end of the wire to a ground, such as a grounded equipment rack.

Safety plugs (European Union)

- **Class I Mains Powered Equipment –** Provided with a 3-terminal AC inlet and requires connection to a 3-terminal mains supply outlet via a 3-terminal power cord for proper connection to the protective ground.

  Note: The equipotential bonding terminal provided on some equipment is not designed to function as a protective ground connection.

- **Class II Mains Powered Equipment –** Provided with a 2-terminal AC inlet that may be connected by a 2-terminal power cord to the mains supply outlet. No connection to the protective ground is required as this class of equipment is provided with double or reinforced and/or supplementary insulation in addition to the basic insulation provided in Class I equipment.

Note: Class II equipment, which is subject to EN 50083-1, is provided with a chassis mounted equipotential bonding terminal. See the section titled **Equipotential Bonding** for connection instructions.

Equipotential Bonding

If this equipment is equipped with an external chassis terminal marked with the IEC 60417-5020 chassis icon (⏚), the installer should refer to CENELEC standard EN 50083-1 or IEC standard IEC 60728-11 for correct equipotential bonding connection instructions.

AC Power

Important: If this equipment is a Class I equipment, it must be grounded.

- If this equipment plugs into an outlet, the outlet must be near this equipment, and must be easily accessible.
- Connect this equipment only to the power sources that are identified on the equipment-rating label normally located close to the power inlet connector(s).
- This equipment may have two power sources. Be sure to disconnect all power sources before working on this equipment.
- If this equipment **does not** have a main power switch, the power cord connector serves as the disconnect device.

- Always pull on the plug or the connector to disconnect a cable. Never pull on the cable itself.
- Unplug this equipment when unused for long periods of time.

Connection to -48 V DC/-60 V DC Power Sources

If this equipment is DC-powered, refer to the specific installation instructions in this manual or in companion manuals in this series for information on connecting this equipment to nominal -48 V DC/-60 V DC power sources.

Circuit Overload

Know the effects of circuit overloading before connecting this equipment to the power supply.

CAUTION:

Consider the connection of this equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Refer to the information on the equipment-rating label when addressing this concern.

General Servicing Precautions

WARNING:

Avoid electric shock! Opening or removing this equipment's cover may expose you to dangerous voltages.

CAUTION:

These servicing precautions are for the guidance of qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so. Refer all servicing to qualified service personnel.

Be aware of the following general precautions and guidelines:

- **Servicing** - Servicing is required when this equipment has been damaged in any way, such as power supply cord or plug is damaged, liquid has been spilled or objects have fallen into this equipment, this equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
- **Wristwatch and Jewelry** - For personal safety and to avoid damage of this equipment during service and repair, do not wear electrically conducting objects such as a wristwatch or jewelry.
- **Lightning** - Do not work on this equipment, or connect or disconnect cables, during periods of lightning.
- **Labels** - Do not remove any warning labels. Replace damaged or illegible

warning labels with new ones.

- **Covers** - Do not open the cover of this equipment and attempt service unless instructed to do so in the instructions. Refer all servicing to qualified service personnel only.
- **Moisture** - Do not allow moisture to enter this equipment.
- **Cleaning** - Use a damp cloth for cleaning.
- **Safety Checks** - After service, assemble this equipment and perform safety checks to ensure it is safe to use before putting it back into operation.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the static electricity buildup on the human body and other objects. This static discharge can degrade components and cause failures.

Take the following precautions against electrostatic discharge:

- Use an anti-static bench mat and a wrist strap or ankle strap designed to safely ground ESD potentials through a resistive element.
- Keep components in their anti-static packaging until installed.
- Avoid touching electronic components when installing a module.

Fuse Replacement

To replace a fuse, comply with the following:

- Disconnect the power before changing fuses.
- Identify and clear the condition that caused the original fuse failure.
- Always use a fuse of the correct type and rating. The correct type and rating are indicated on this equipment.

Batteries

This product may contain batteries. Special instructions apply regarding the safe use and disposal of batteries:

Safety

- Insert batteries correctly. There may be a risk of explosion if the batteries are incorrectly inserted.
- Do not attempt to recharge ‘disposable’ or ‘non-reusable’ batteries.
- Please follow instructions provided for charging ‘rechargeable’ batteries.

- Replace batteries with the same or equivalent type recommended by manufacturer.
- Do not expose batteries to temperatures above 100°C (212°F).

Disposal

- The batteries may contain substances that could be harmful to the environment
- Recycle or dispose of batteries in accordance with the battery manufacturer's instructions and local/national disposal and recycling regulations.



- The batteries may contain perchlorate, a known hazardous substance, so special handling and disposal of this product might be necessary. For more information about perchlorate and best management practices for perchlorate-containing substance, see www.dtsc.ca.gov/hazardouswaste/perchlorate.

Modifications

This equipment has been designed and tested to comply with applicable safety, laser safety, and EMC regulations, codes, and standards to ensure safe operation in its intended environment. Refer to this equipment's data sheet for details about regulatory compliance approvals.

Do not make modifications to this equipment. Any changes or modifications could void the user's authority to operate this equipment.

Modifications have the potential to degrade the level of protection built into this equipment, putting people and property at risk of injury or damage. Those persons making any modifications expose themselves to the penalties arising from proven non-compliance with regulatory requirements and to civil litigation for compensation in respect of consequential damages or injury.

Accessories

Use only attachments or accessories specified by the manufacturer.

Electromagnetic Compatibility Regulatory Requirements

This equipment meets applicable electromagnetic compatibility (EMC) regulatory requirements. Refer to this equipment's data sheet for details about regulatory compliance approvals. EMC performance is dependent upon the use of correctly shielded cables of good quality for all external connections, except the power source, when installing this equipment.

- Ensure compliance with cable/connector specifications and associated installation instructions where given elsewhere in this manual.

Otherwise, comply with the following good practices:

- Multi-conductor cables should be of single-braided, shielded type and have conductive connector bodies and backshells with cable clamps that are conductively bonded to the backshell and capable of making 360° connection to the cable shielding. Exceptions from this general rule will be clearly stated in the connector description for the excepted connector in question.
- Ethernet cables should be of single-shielded or double-shielded type.
- Coaxial cables should be of the double-braided shielded type.

EMC Compliance Statements

Where this equipment is subject to USA FCC and/or Industry Canada rules, the following statements apply:

FCC Statement for Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this 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 instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case users will be required to correct the interference at their own expense.

Industry Canada - Industrie Canadienne Statement

This apparatus complies with Canadian ICES-003.
Cet appareil est confome à la norme NMB-003 du Canada.

CENELEC/CISPR Statement with Respect to Class A Information Technology Equipment

This is a Class A equipment. In a domestic environment this equipment may cause radio interference in which case the user may be required to take adequate measures.

Laser Safety

Introduction

This equipment contains an infrared laser that transmits intensity-modulated light and emits invisible radiation.

Warning: Radiation

WARNING:

- **Avoid personal injury! Use of controls, adjustments, or procedures other than those specified herein may result in hazardous radiation exposure.**
- **Avoid personal injury! The laser light source on this equipment (if a transmitter) or the fiber cables connected to this equipment emit invisible laser radiation. Avoid direct exposure to the laser light source.**
- **Avoid personal injury! Viewing the laser output (if a transmitter) or fiber cable with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.**

- Do not apply power to this equipment if the fiber is unmated or unterminated.
- Do not stare into an unmated fiber or at any mirror-like surface that could reflect light emitted from an unterminated fiber.
- Do not view an activated fiber with optical instruments (e.g., eye loupes, magnifiers, microscopes).
- Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.

Warning: Fiber Optic Cables

WARNING:

Avoid personal injury! Qualified service personnel may only perform the procedures in this manual. Wear safety glasses and use extreme caution when handling fiber optic cables, particularly during splicing or terminating operations. The thin glass fiber core at the center of the cable is fragile when exposed by the removal of cladding and buffer material. It easily fragments into glass splinters. Using tweezers, place splinters immediately in a sealed waste container and dispose of them safely in accordance with local regulations.

Safe Operation for Software Controlling Optical Transmission Equipment

If this manual discusses software, the software described is used to monitor and/or control ours and other vendors' electrical and optical equipment designed to transmit video, voice, or data signals. Certain safety precautions must be observed when operating equipment of this nature.

For equipment specific safety requirements, refer to the appropriate section of the equipment documentation.

For safe operation of this software, refer to the following warnings.

WARNING:

- **Ensure that all optical connections are complete or terminated before using this equipment to remotely control a laser device. An optical or laser device can pose a hazard to remotely located personnel when operated without their knowledge.**
- **Allow only personnel trained in laser safety to operate this software. Otherwise, injuries to personnel may occur.**
- **Restrict access of this software to authorized personnel only.**
- **Install this software in equipment that is located in a restricted access area.**

Laser Safety Information

This laser based multi-mode transceiver is an IEC 60825-1 Amend. 2 Class 1 laser product. It complies with FDA performance standards (21 CFR 1040.10 and 1040.11) for laser products except for deviations pursuant to Laser Notice No. 50, dated July 26, 2001.

Note: All adjustments have been made at the factory prior to shipment of the module. No maintenance or alteration of this device is required. No adjustments or controls provided.

Class 1 Laser Product

Avoid possible exposure to hazardous levels of invisible laser radiation; do not view laser aperture.

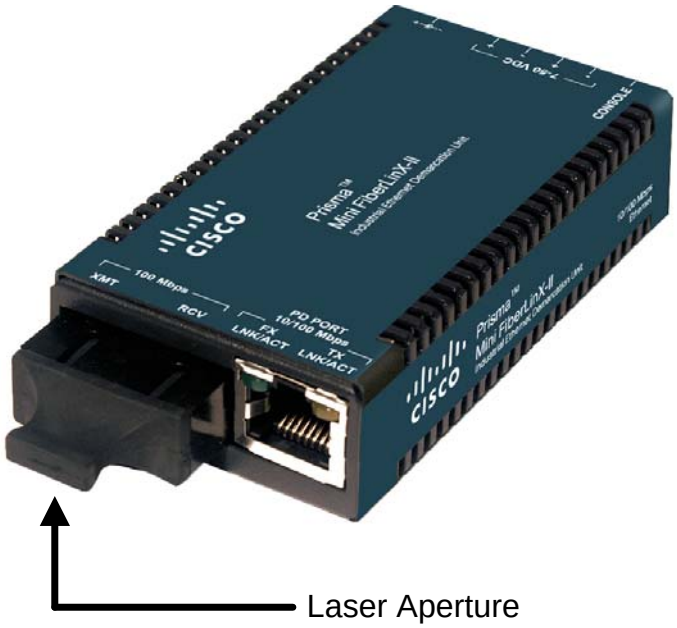
Warning Label

The following label applies to this module, but cannot be affixed due to space limitations.

Class 1 Laser product, Luokan 1 Laserlaite,
Laser Klasse 1, Appareil A'Laser de Classe 1

Product Laser Information

The following illustration displays the location of laser aperture on the module front panel.



About the Prisma Mini FiberLinX-II

The Prisma Mini FiberLinX-II is an optical demarcation network interface device that lets you connect to and manage remote network segments. Advanced networking capabilities enable you to view the end points of a network segment and the fiber link between them as a single management entity, rather than as a separate network. No host management traffic is visible to the remote or customer network, and no access to the customer network is required, guaranteeing end-to-end data integrity.

The Mini FiberLinX-II includes one 100 Mbps fiber port (OPTICS), one 10/100 twisted pair data port (DATA), and one auxiliary Craft port for serial configuration (with the included adapter). The twisted-pair port can auto-negotiate or be set manually for 10 or 100 Mbps and for half or full duplex mode. The optics port operates at 100 Mbps, full duplex only. Powering options include AC and DC power as well as power over Ethernet, functioning as a powered device (PD) compliant with IEEE 802.3af.

The Mini FiberLinX-II is IEEE 802.1Q VLAN compatible, supporting a full-range of VLAN IDs, and offering Q-in-Q tagging and a 2-tier queue for differential prioritization (IEEE 802.1p). The Mini FiberLinX-II also includes the LinkLoss and FiberAlert as well as LinkFault Pass Through (LFPT) features for troubleshooting, loopback testing functionality, bi-directional bandwidth control, and optional protection against Broadcast storms.

Single-strand fiber versions of the Mini FiberLinX-II allow two wavelengths to share one fiber strand. Full-duplex data travels on two different wavelengths, 1310 nm and 1550 nm, thereby doubling the capacity of fiber.

PrismaView™, a graphical element management system that runs on SNMP, is offered for use with this module.

PrismaView Management Software

PrismaView is a network management application for Prisma FiberLinX intelligent networking devices. It features a graphical user interface (GUI) that provides network managers the ability to monitor and control Prisma FiberLinX products. The application is available in several versions, and can also function as a snap-in module for HP OpenView Network Node Manager. Refer to the PrismaView help file for information regarding configuring and managing the Mini FiberLinX-II.

PrismaView supports the following platforms:

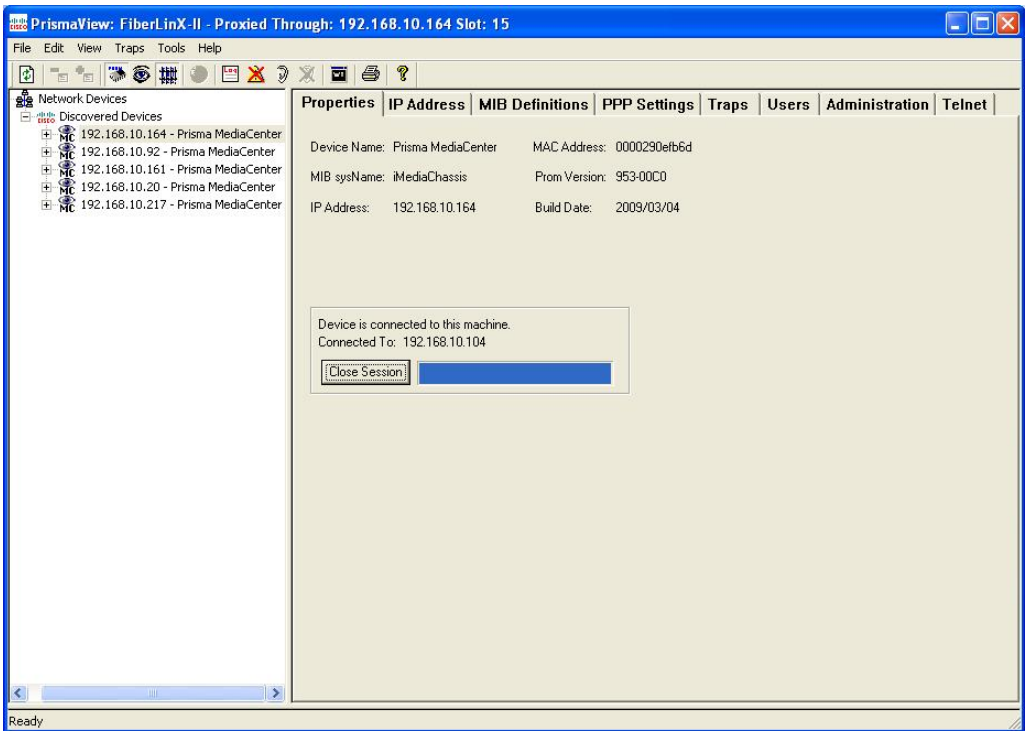
- Windows 98
- Windows NT
- Windows 2000
- Windows XP
- Windows Vista

iConfig Utility

iConfig is an in-band utility used for SNMP configuration for Prisma FiberLinX SNMP-manageable devices. iConfig allows you to set the following parameters for each device:

- IP address
- Subnet mask
- Default gateway
- Community strings
- SNMP traps

iConfig also includes an authorized IP address system and restricted access to MIB groups which are supported by Prisma FiberLinX manageable devices. These extra layers of security do not affect SNMP compatibility. iConfig can upload new versions of the system software and new MIB information. iConfig also includes diagnostic capabilities for faster resolution of technical support issues.



iConfig is also available as a standalone application. (Windows 98 users must use the standalone version of iConfig.) Both PrismaView and iConfig are included on the PrismaView CD. For information regarding the use of iConfig, refer to the PrismaView help menu.

Default Username/Password

The default user ID and password for both iConfig and Telnet are as follows:

- User ID: **admin**
- Password: **admin**

Installation

To install the Mini FiberLinX-II into a network environment, connect the proper twisted-pair and fiber cables. In a standalone configuration, or if direct management is desired, assign an IP address to the Mini FiberLinX-II after installation. Refer to ***Assigning IP Information*** (on page 27) for information on assigning an IP address.

Usage in Pairs

Single-strand fiber products use optics that transmit and receive on two different wavelengths. Therefore, these products must be used in pairs or connected with compatible single-strand fiber products.

For example, a Mini FiberLinX-II, TX/SSFX-SM1310-SC transmits on 1310 nm and receives on 1550 nm. It must be paired with a product which transmits on 1550 nm and receives on 1310 nm, such as a Prisma FiberLinX-II, TX/SSFX-SM1550-SC.

The two connected products must also have the same speed and distance capabilities. For example, both must be single-mode (20 km) or single/PLUS (40 km).

Autocross Feature for Twisted-Pair Connection

All twisted pair ports on the Mini FiberLinX-II include AutoCross, feature that automatically selects between a crossover workstation and a straight-through connection depending on the connected device.

Mini-Serial Port

Included with the Mini FiberLinX-II is a serial port adapter for configuration. A standard AC mini-jack on the Mini FiberLinX-II provides a local RS-232 craft interface for management. A special mini-jack to DF-9F cable is provided for direct connection to a PC serial port.

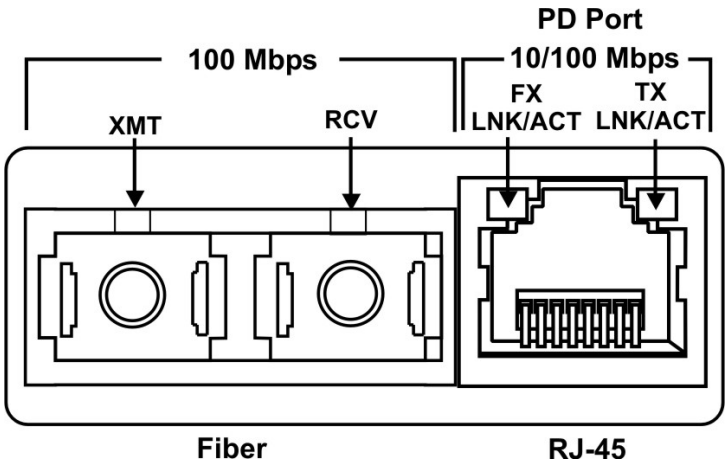
Using the Serial Port

To log on through the serial port, set the computer or terminal for VT-100 emulation and apply the following communication settings:

- 38.4K baud
- 8 data bits
- 1 stop bit
- No parity
- No FlowControl

LED Operation

The Mini FiberLinX-II features two diagnostic LEDs, labeled FX LINK/ACT and TX LINK/ACT.

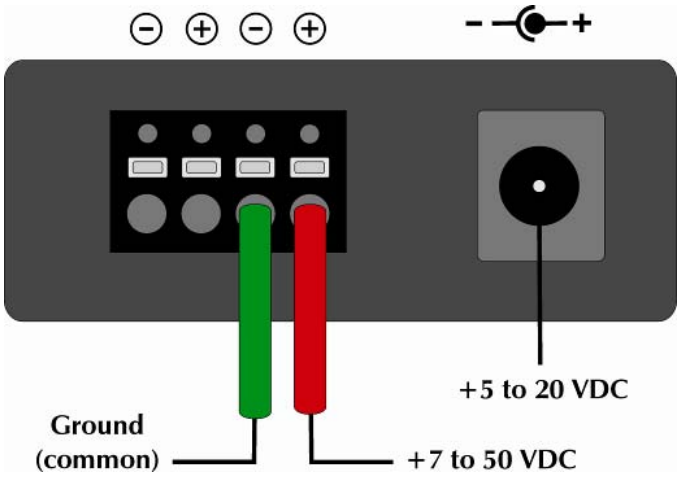


The following table describes the functions of these LEDs.

LED	Function
FX LNK/ACT	This LED is on when a FX Link exists and blinks when data passes through the fiber connection.
TX LNK/ACT	This LED is on when a TX Link exists and blinks when data passes through the twisted-pair connection.

Powering Options

Powering options for the Mini FiberLinX-II include AC and DC powering as well as power over Ethernet, functioning as an IEEE 802.3af-compliant powered-device (PD) module. The DC terminal block allows you to daisy-chain one Mini FiberLinX-II to another.



To use the DC terminal block, connect to any one positive and any one negative terminal from a power source. The illustration above shows the wiring configurations for the DC terminal block (7 to 50 VDC).

Features and Configuration

The Mini FiberLinX-II offers a full feature set including the following:

- Auto-Negotiation
- Selective Advertising
- FiberAlert
- AutoCross
- Read/write VLANs
- SNMP management
- Bandwidth control
- Loopback testing

The following sections of this guide provide additional information on these features.

Configuration

The features listed above can be configured through software or via a serial port, Telnet session, iConfig, or SNMP.

Additionally, software updates for the module can be downloaded through TFTP and iConfig.

Auto-Negotiation, Duplex Mode, and Speed

The twisted-pair port on the Mini FiberLinX-II auto-negotiates for speed and duplex mode, while also providing the option of selectively advertising or forcing the speed and duplex mode.

The optics port does not auto-negotiate, but instead, operates at 100 Mbps full duplex. Use the management software to configure the features on the twisted-pair ports.

The Mini FiberLinX-II ships from the factory with Auto-Negotiation enabled on the twisted-pair port. In this mode, the port automatically negotiates for speed and duplex.

The twisted-pair port on the Mini FiberLinX-II can also be manually set for 10 Mbps or 100 Mbps operation and for half or full duplex. These settings give the following possible combinations:

- 10 Mbps full duplex
- 10 Mbps half duplex
- 100 Mbps full duplex
- 100 Mbps half duplex

Selective Advertising, when used in combination with Auto-Negotiation, advertises only the configured speed and duplex mode for the twisted-pair port. If a specific speed or duplex mode is desired, use Selective Advertising rather than Force Mode when connecting to devices that only auto-negotiate.

Bandwidth Control

The Mini FiberLinX-II includes bi-directional bandwidth control, which can be independently set in 32 Kbps increments up to 100 Mbps. Bandwidth control can be configured through PrismaView2 or a console session. The device features an integrating algorithm with a 64 Kb buffer, allows traffic bursts, to prevent lost data. This allows operators to offer tiered services. See the PrismaView help file for configuration information.

FX/TX LinkLoss and FiberAlert

During normal operation, link integrity pulses are transmitted by all point-to-point Ethernet devices. When a Mini FiberLinX-II receives valid link pulses, it knows the device to which it is connected is up, and the copper or fiber cable coming from that device is intact. The appropriate LNK LED is lit to indicate this. For troubleshooting information using the LinkLoss and FiberAlert features of the Mini FiberLinX-II modules, refer to ***Troubleshooting*** (on page 58).

CAUTION:

The FiberAlert and LinkLoss features cause data interruptions designed to alert remote sites of line failures. These data interruptions can be misinterpreted as module failures when these features are enabled. Enable these features only when the resulting data interruptions and causes are well understood.

FX LinkLoss

FX LinkLoss is link integrity monitoring feature that forwards fiber link faults to the RJ-45 DATA port to indicate that a fiber link fault has occurred.

TX LinkLoss

TX LinkLoss is a link integrity monitoring feature that forwards an RJ-45 link fault to the fiber connected device to indicate that a link fault has occurred.

FiberAlert

FiberAlert minimizes the problems associated with the loss of one strand of fiber. Normally when a single strand of fiber is lost, the transmitting side of the connection is unaware that there is a fault. FiberAlert returns faults back on the fiber they came in on.

Using LinkLoss and FiberAlert

In a typical central site to remote site media conversion, it is recommended that you enable the LinkLoss and FiberAlert features as indicated in the following:

Feature	Enabled	Fault Location	Port Affected
FiberAlert	Remote side only	Fiber	Fiber
TX LinkLoss	Remote side (or both)	Twisted pair	Fiber
FX LinkLoss	Hot side (or both)	Fiber	Twisted pair

CAUTION:

Do not enable FiberAlert on both modules when using them in pairs. This will cause them to lock up when a fault occurs on the fiber. Only enable FiberAlert on the remote module.

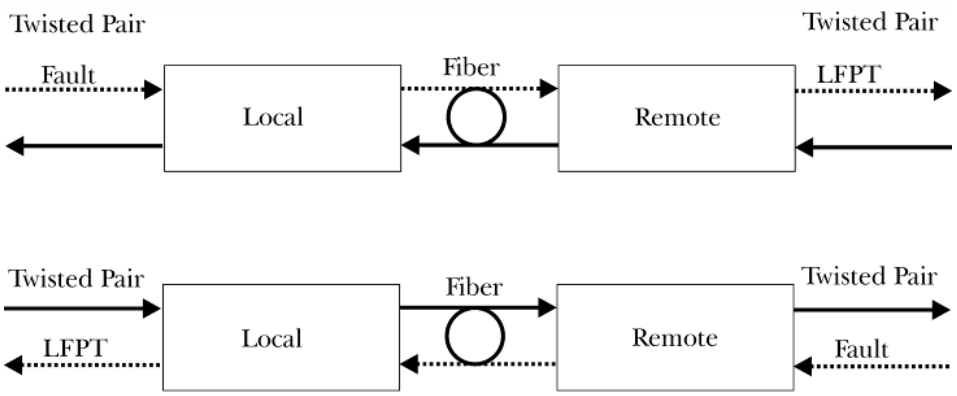
Link Fault Pass Through

Link Fault Pass Through (LFPT) is a troubleshooting feature that combines TX and FX LinkLoss from both the local and remote modules. You enable LFPT by turning on both FX and TX LinkLoss on both modules.

This feature allows either end of the conversion to detect a link fault occurring at the other end of the media conversion chain, as follows:

- A cable fault occurs on the remote twisted pair.
- TX LinkLoss detects the fault and disables the OPTICS (or UPLINK) port.
- FX LinkLoss detects the fiber loss and disables the DATA port.

The link fault is passed through the media conversion and is observed at each end. It acts just as it would if the devices were directly connected.



FX and TX LinkLoss enabled on both modules will enable LFPT

Note: FiberAlert can also be added to the remote side of the pair to further assist in locating a fault.

Loopback Testing

The Mini FiberLinX-II includes Loopback testing functionality, which loops back all frames arriving on the optics port (except for the device's management traffic). When in Loopback mode, the Mini FiberLinX-II drops the link on the twisted pair port.

Another form of Loopback testing, called Source/Destination (Src/Dest) Address Swap, swaps the frame's MAC Address. This test mode is set from the Unit screen in the serial/Telnet session or from PrismaView.

Note: This test mode can cause a frame with a multicast source address to be created, which violates the IEEE standard. Select only clear multicast bits.

For more information, see the **Unit Control Settings** section of ***Using the Main Configuration Screen*** (on page 30) or consult the PrismaView help file.

Assigning IP Information

To use SNMP management in a standalone environment, you must assign the Mini FiberLinX-II IP configuration information (IP address, subnet mask, etc.) by using either iConfig (from PrismaView), the module serial port, or DHCP.

These methods will also allow you to create community strings, assign access rights, configure traps, and more. iConfig offers more options than serial port configuration. After assigning the Mini FiberLinX-II an IP address, use PrismaView or another SNMP-compatible network management system (NMS) for remote configuration, monitoring, and management.

Note: You can access the remote Mini FiberLinX-II module (through iConfig, Telnet, etc.) for performance upgrades and management by using the IP address assigned to the Prisma FiberLinX-II host unit, or, when used in a standalone application, through the remote module's own unique IP address.

Configuration

The Mini FiberLinX-II includes many features that function automatically or are configurable via PrismaView, iConfig, or a serial/Telnet session.

To Configure Software

The following table presents port options configurable from PrismaView or from a serial/Telnet session. Refer to ***Using PrismaView*** (on page 47) or the PrismaView Help file for more information. For information on configuring VLANs, refer to **Serial Configuration/Telnet Session** in ***Using the Main Configuration Screen*** (on page 30).

Feature	PrismaView	Serial/Telnet
FX/TX LinkLoss	✓	✓
FiberAlert	✓	✓
Loopback	✓	✓
Auto-Negotiation	✓	✓
Selective Advertising	✓	✓
Force Mode	✓	✓
FlowControl	✓	✓
Bandwidth Control	✓	✓
VLANs		✓

The following table presents management options configurable via iConfig or a serial/Telnet session.

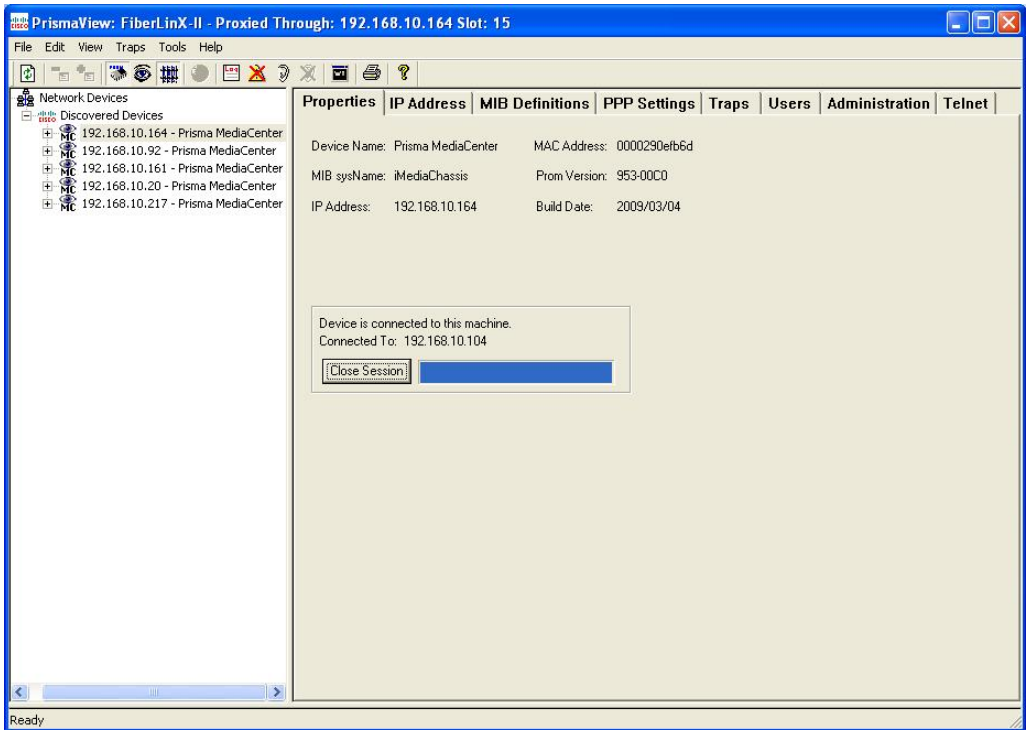
Feature	PrismaView	Serial/Telnet
PROM Software Download/Upload	✓	
Telnet Session	✓	
TFTP Trigger		✓
Software Download Setup (TFTP)		✓
DHCP		✓
Configuration File/Save Restore	✓	

The following options are configurable through both iConfig and Serial:

- IP address
- Subnet mask
- Default gateway
- MIB community
- Traps assignment
- Users
- Passwords
- Access level
- Reboot

Using the Main Configuration Screen

Press **Enter** at the prompt to display the main configuration screen.



The following displays are available:

Saved Values (displays changes made during current session)

- IP Address (must be assigned during initial configuration)
- Subnet Mask (must be assigned during initial configuration)
- Default Gateway (default router for IP traffic outside subnet)
- Server IP Addr (for the TFTP server)
- New Prom File (firmware file name)

Current Values (displays values currently in use)

- IP Address (IP address of SNMP agent)
- Subnet Mask (mask to define IP subnet)
- Default Gateway (default router for IP traffic outside subnet)
- Server IP Addr (for the TFTP server)
- New Prom File (firmware file name)

Note: Reboot the Mini FiberLinX-II for changes to take effect. To reboot, type **reboot** at the prompt on the main configuration screen, or press **Delete** or **F2** to power-cycle the chassis. Any changes to the configuration may result in a momentary loss of connection.

Command List

- I = Enter New Saved Parameter Values
- P = Change Password
- T = New Trap Destination
- K = Remove ALL Trap Destinations
- C = New Community String
- U = Delete ALL Community Strings
- E = End Session
- Reboot = Reboots the Mini FiberLinX-II
- D = Enable/disable DHCP
- Space = Device Specific Configuration Options

To Assign TCP/IP Information

Complete the following steps to modify the Saved Parameter Values (i.e., assign IP address and subnet mask).

1. Press **I**, type the IP address, and then press **Enter**. The cursor moves to the subnet mask field.
2. Type the subnet mask for the connected device, and then press **Enter**. The cursor moves to the default gateway field.
3. Type the default gateway, or press **Enter** to skip.
4. Press Enter, and then type **reboot** to reboot the module. The TCP/IP information changes goes into effect following reboot.

Note: The Current Values can only be saved and acted on after the Mini FiberLinX-II has been successfully rebooted.

To Password-Protect Serial Port Connections

Password protection is provided for the serial configuration process by pressing P on the main configuration screen. Enter a password, keeping in mind that passwords are case-sensitive and must not exceed eight characters or include spaces, and press Enter. This password will be requested whenever logging on. To remove password protection, select P and, instead of entering a password, press Enter. If a password becomes lost, contact Cisco Services for your area. See ***For Information*** (on page 62).

To Assign Trap Destinations

Traps are sent by the manageable device to a management PC when a certain event takes place. To enter a trap destination, press T. At the "Enter a New IP Address." prompt, enter the appropriate IP address and press Enter. Then, type the name of the community string (that the destination device has been configured to accept) and press Enter. This function enables ALL of the device traps. To individually activate and deactivate traps, use iConfig for configuration. Supported traps include: Link Down, Link Up, Cold Start, Warm Start and Authentication Failure.

To Remove Trap Destinations

To remove all trap destinations, press **K**, then press **Y** to continue to confirm (or **N** to abort), and then press **Enter**.

Note: To selectively remove community strings, use iConfig to configure the device.

To Create Community Strings

Community strings add a level of security to a network. The default community string is named "public" and has read/write access. You should replace "public" with custom community strings, such as one with read-only access (for general use), the other with read/write access (for the administrator).

Complete the following steps to create community strings:

1. Type **C** on the main configuration screen.
2. Type the name of the new community (up to 16 characters, no spaces), and then press **Enter**.
3. Type one of the following to assign the community string access rights:
   - **R** (for read-only access), and then press **Enter**.
   - **W** (for read/write access), and then press **Enter**.
   - **Enter** (to abort)
4. To finish, press **Enter**, and then reboot.

To Delete Community Strings

Complete the following steps to delete all community strings:

1. Press **U**. The "Are you sure you want to delete all future strings?" prompt appears.
2. Press **Y** to proceed, **N** to abort.
3. Press **Enter**.

Note: This function deletes ALL community strings. To selectively delete community strings, use iConfig to configure the device.

To End the Session

Be sure to press E to end a serial port or Telnet/HyperTerminal session, before disconnecting the cable. This will stop the continuous stream of data to the serial port.

To Reboot the Module

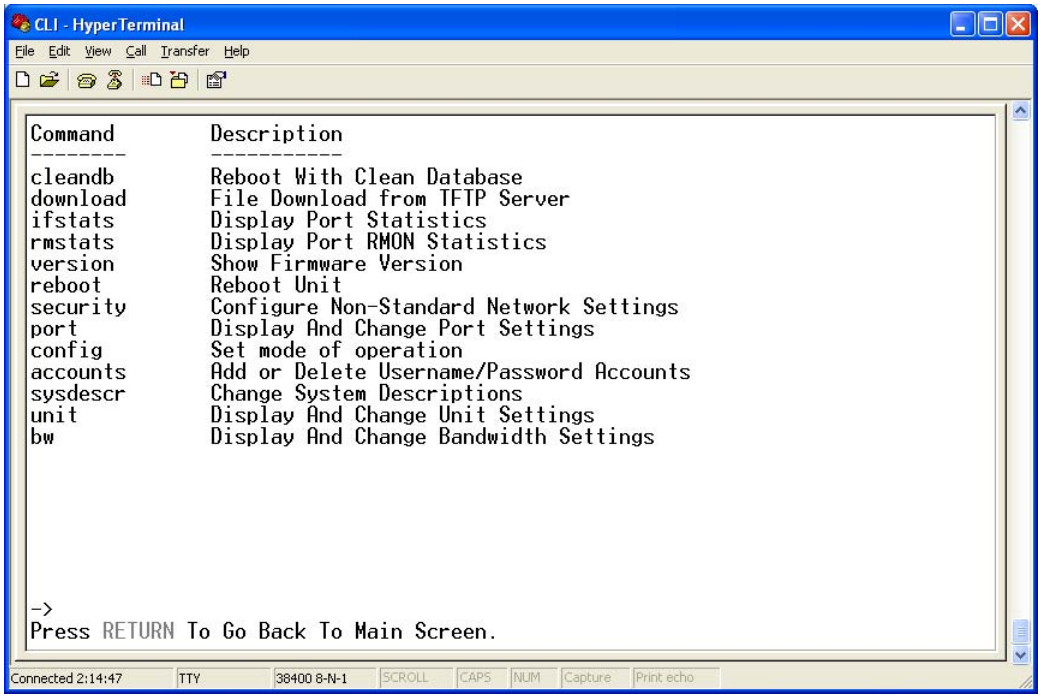
To reboot the Mini FiberLinX-II module, type **reboot**.

To Enable or Disable DHCP

To toggle DHCP on the Mini FiberLinX-II between enable and disable, press D.

Additional Device-Specific Commands

The Mini FiberLinX-II also includes the following device-specific options.



The following table summarizes these options. Additional details on each option are provided below.

Command	Description
cleandb	Reboots the unit with a clean database. This removes all information from the database and sets the unit to factory defaults.
download	Downloads firmware via the TFTP protocol.
ifStats	Displays Ethernet statistics.
rmStats	Displays RMON statistics.
version	Displays the unit's serial number and build date.
reboot	Reboots the unit and clears all internal counters.
security	Allows ARP request configuration. This setting is only for very unique configurations and should not be adjusted.
port	Displays and changes port settings, such as duplex status and speed.
config	Allows VLAN and transparency mode configurations.
accounts	Allows the addition of new users.
sysdescr	Allows the editing of sysName, sysDescr, and Port information text.
unit	Unit global setting.
bw	Bandwidth limiting controls.
spfstats	Provides information about the wavelength, serial number, output power, BER, and other useful information.

Cleandb

Entering cleandb reboots the unit with its database cleaned depending on the option selected. This command presents with two sequential options:

- First, to reset all SNMP settings.
- Second, to reset all module configuration to default.

Enabling the first option presents the second. Resetting the unit to factory default values (option two) deletes all custom IP and VLAN settings.

Complete the following steps to access these options:

1. Press the **Space Bar** when in the Command List section of the Main Configuration screen (serial configuration/Telnet session).
2. Type the name of the action (shown below), and then press **Enter**.

Downloading Files

Firmware for the Mini FiberLinX-II can be downloaded from a central server via TFTP protocol. Initiate this download via serial configuration or Telnet session.

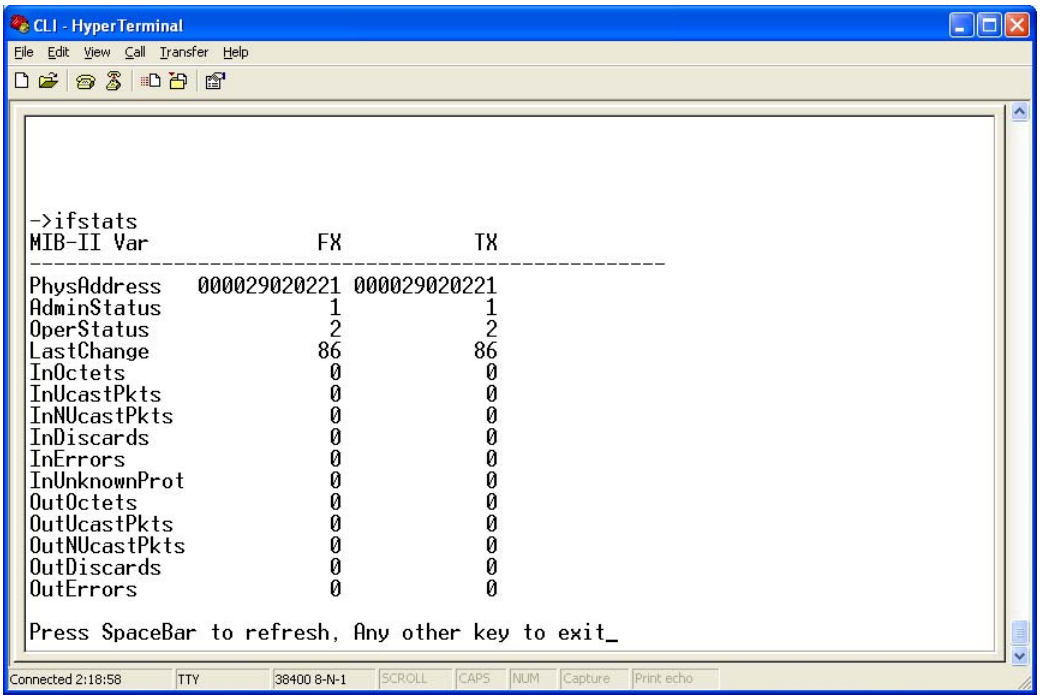
Complete the following steps to download a file.

1. Type **download** and then press **Enter**. The Download a File screen opens, displaying the IP address of the TFTP server and the name of the file to be downloaded.
2. Confirm that the TFTP server opens, and that the IP address and file name are correct in the Current Values section of the Main Configuration screen.
3. If necessary, change these values by entering **I** from the Main Configuration screen.
4. Press **Enter** to start downloading the file.

Viewing Port Statistics

To view port statistics on the Mini FiberLinX-II, type **ifstats** and then press **Enter**.

A screen opens displaying information on packets received and transmitted as defined by MIB-II standard RFC 1213.

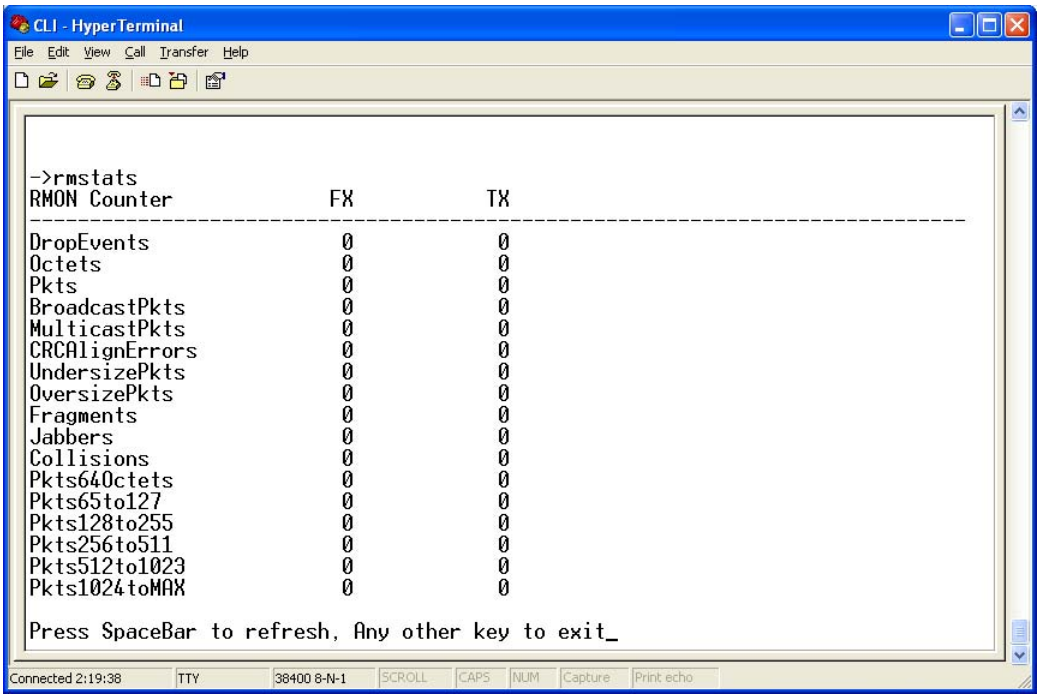


Note: If necessary, you can refresh the data on this screen by pressing the **Space Bar**.

Viewing Port RMON Statistics

To view port RMON (Remote MONitoring) statistics on the Mini FiberLinX-II, type **rmstats** and then press **Enter**.

A screen opens displaying RMON information on packets received as defined in RFC 2819 for RMON.



Note: If necessary, you can refresh the data on this screen by pressing the **Space Bar**.

Version

To display the current firmware version for the Mini FiberLinX-II, , type **version** and then press **Enter**.

Note: In the examples shown, ports are referred to as they appear on the module itself. Some screens may show TX and FX for the port titles, where TX = DATA port and FX = OPTICS port.

Reboot

To save the current settings and reboot the Mini FiberLinX-II, type **reboot** and then press **Enter**.

Setting Security

Security settings on the Mini FiberLinX-II are reserved for non-standard configurations. Use security configuration only when non-standard networking equipment is being employed.

Complete the following steps to define new security settings:

1. Type **Y** (or type any other key to abort). A screen appears allowing you to configure ARP settings, such as the destination address of ARP messages, along with Ethernet Types.
2. Enter the new data.
3. Type **S** to save the new security settings (or type **Q** to cancel).

Port Configuration

Serial/Telnet sessions display port status as well as allowing configuration of some port features. Type **Port** and press **Enter** to be taken to the Port screen. From this screen, you can view the port speed, duplex and link status.

The Port screen contains the following commands:

Command	Description
Port Enable	Enable/Disable the port. (Select Enable to enable the port.)
Admin Status	Set Administration level. (Select UP to enable the port.)
Port Speed Ctrl	Set the port manually or for auto-negotiation.
Advertise Ctrl	This is the Selective Advertising feature. Selective Advertising, when used in combination with Auto Negotiation, advertises the configured speed and duplex mode for the twisted pair ports. Auto Negotiation must be enabled for Selective Advertising. **Note:** Selective Advertising must be used when connecting to a device that Auto Negotiates and a specific speed and duplex mode is desired.
Advertise FlowC and Force FlowCtrl	This is the FlowControl feature. ■ When using FlowControl functionality on any port, enable Global FlowControl. Then, configure each port individually. ■ When using Auto Negotiation and FlowControl, set Advertise FlowC to Advertise Flow and set Force FlowCtrl to Flow Auto. ■ Set Advertise FlowC to No Flow to disable FlowControl on a given port. ■ When using FlowControl and Force Mode on a given port, set Advertise FlowC to Advertise Flow and set Force FlowCtrl to Frc FlowCt.
Unit FlowControl	This enables/disables FlowControl functionality on the unit and must be enabled for FlowControl to function on any port.

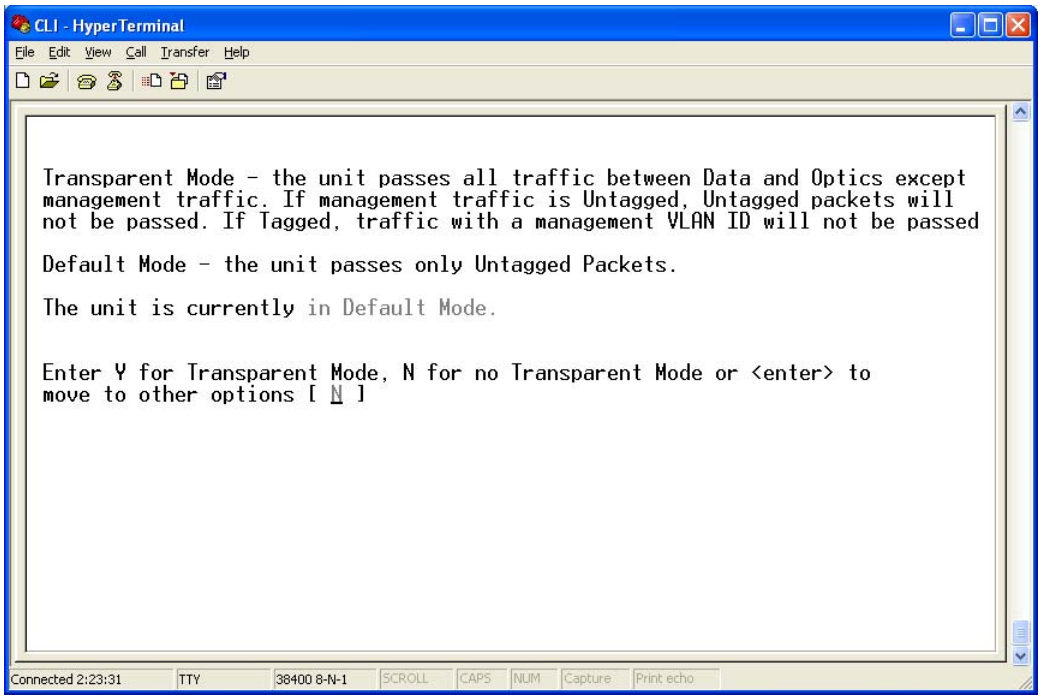
Operational Mode Configuration

As referenced in Product Applications, there are six modes of operation that can be configured through the Serial/Telnet session. All of the modes of operation will block management traffic on the Data port.

To access the configuration screen, type **config** and then press **Enter** from the Additional Commands screen.

Mode One – Default and Default Plus

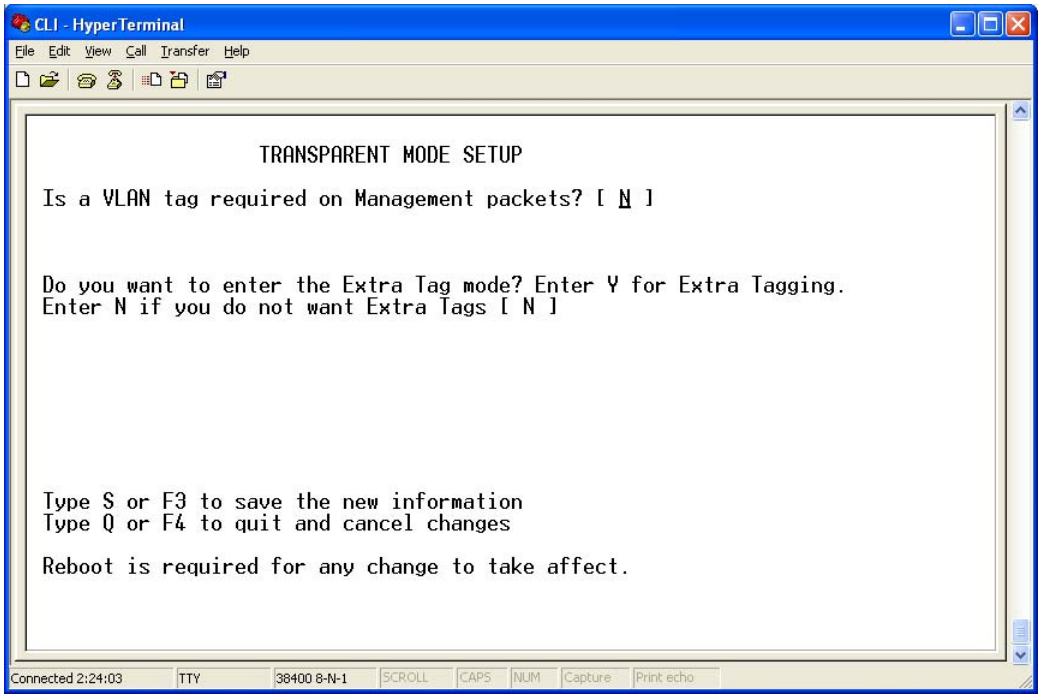
The default mode is designed to pass untagged traffic only. Press **F4** to return to the Additional Device-Specific Commands screen.



In Default Mode Plus, all tagged and untagged traffic passes between the data and optics ports. Management to the device must be untagged.

Mode Two - Transparency with Untagged Management

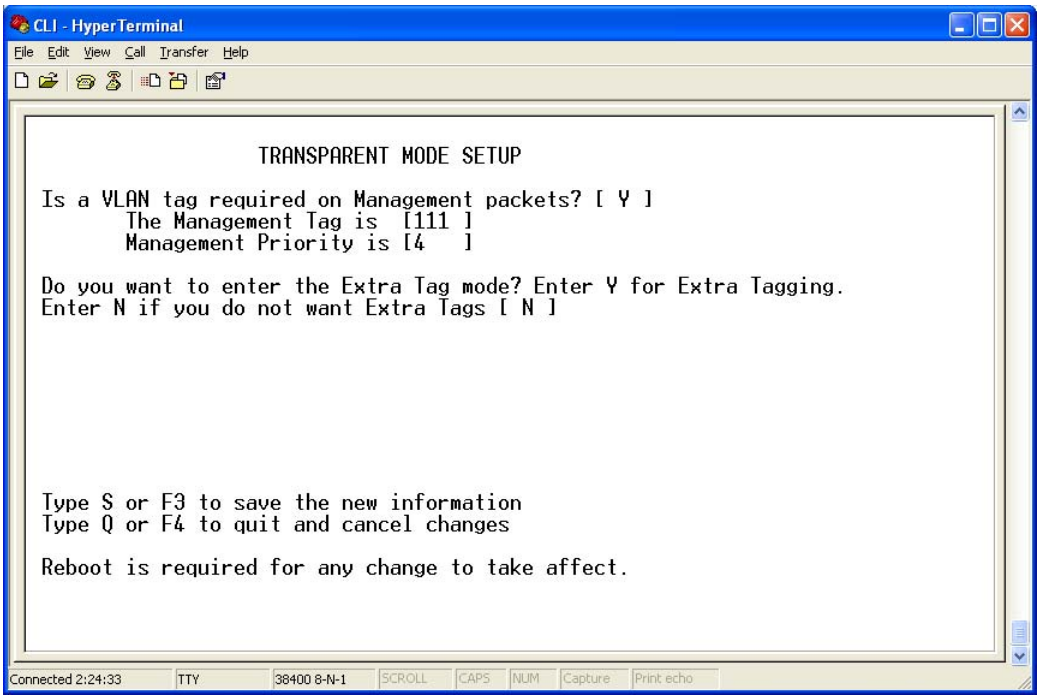
This mode is designed to pass all tagged and extra-tagged customer traffic unchanged and must be managed using untagged traffic only. It does not add or remove tags.



Select **Y** on the initial config screen, and from the Transparent Mode Setup screen, select **N** in the fields.

Mode Three - Transparency with Tagged Management

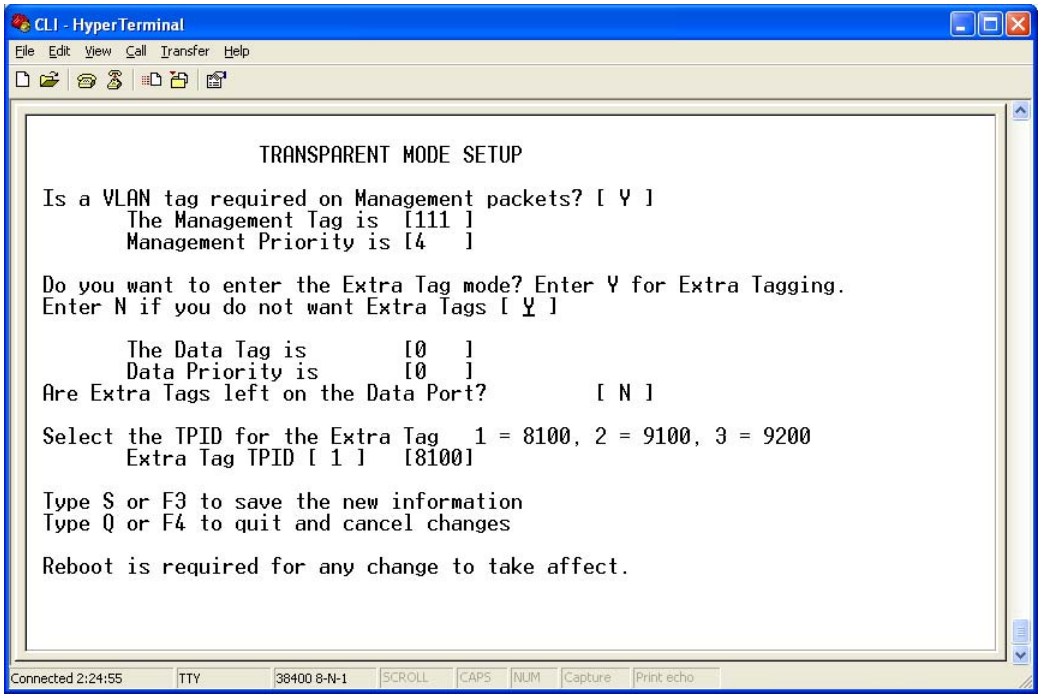
This mode will pass all tagged and untagged customer traffic. Management traffic must be tagged. It does not add or remove tags.



Select **Y** on the initial config screen, and from the Transparent Mode Setup screen, select **Y** and enter the Management Tag.

Mode Four - Transparency with Extra Tagging (or Q-in-Q)

This mode is designed to either pass all customer traffic with the defined extra tag (Q-in-Q) or add and remove the defined extra tag (Q-in-Q) on all customer traffic. Management traffic can be tagged or untagged.

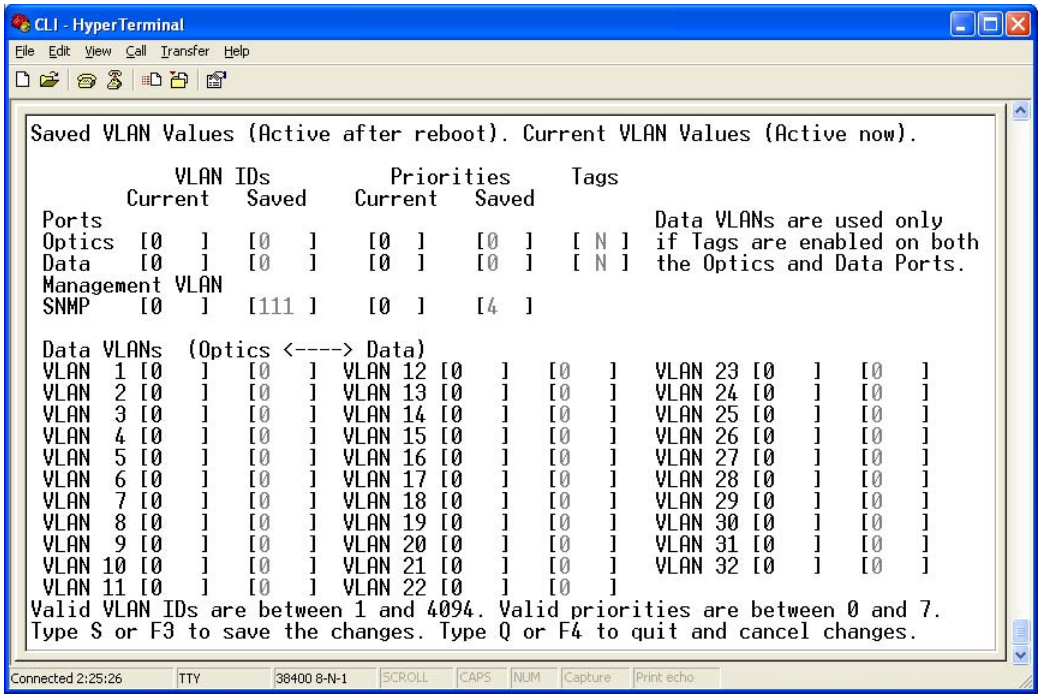


Select **Y** on the initial config screen, and then select **Y** when asked to select Extra Tags.

Note: When setting this operation mode, answer the question "Are Extra Tags left on the Data Port" **NO** for the remote Mini FiberLinX-II and **YES** for the host connection.

Mode Five - VLAN Filter

This mode is designed to only pass traffic with any of the 32 tags that have been identified in the user-defined table. No untagged traffic can pass and management traffic must be tagged. No tags are added or removed from the traffic.



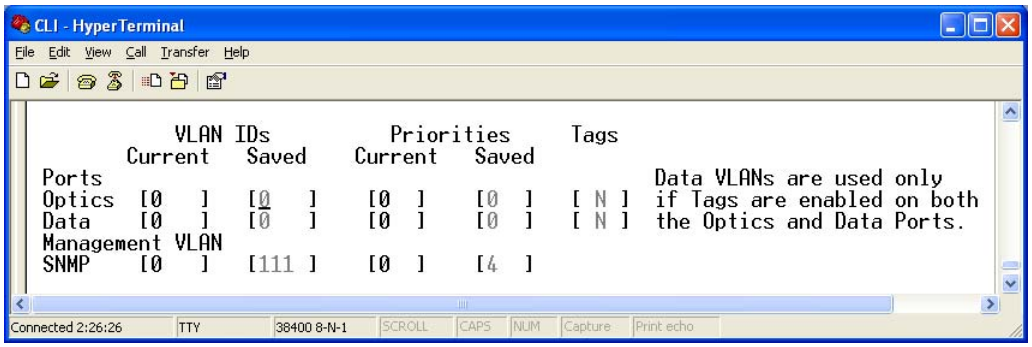
Select **N** on the initial config screen, and then set up the VLAN screen.

Note: VLAN IDs can be any number between 1 and 4,094.

Mode Six - Port VLAN

This mode tags all customer traffic received by the copper port going to the fiber port, untagging traffic conversely.

This tag is entered as the Data VLAN tag with the optical Tags selected as “YES” to indicate it is added at the egress of the optical port.



Select **N** on the initial config screen, and then set up the VLAN screen.

The following table shows how the settings are entered.

Setting	VLAN	Priority	Tags
Optical	-	-	Yes
Data	Tag2	4	No
Mgmt (SNMP)	Tag1	1	Yes

System Description (Sysdescr)

Sysdescr offers the options of assigning a system name, System Contact System Location, Unit Description, and individual Port names.

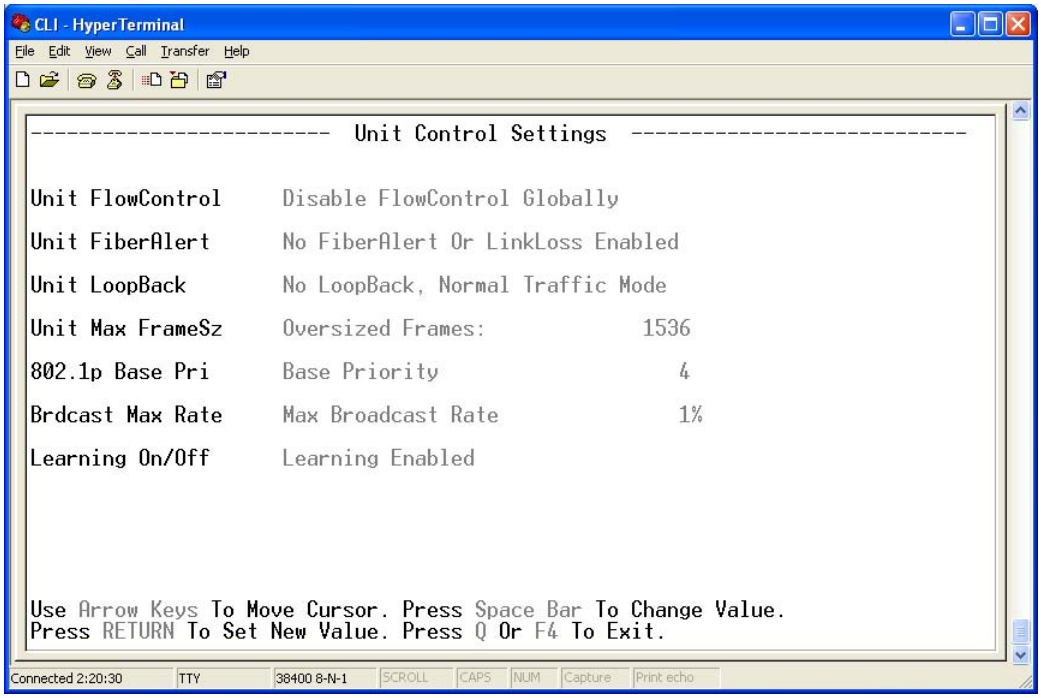
To assign each of these values, type the description or name, up to 32 characters per line, in the field provided. Press **Enter** key after each entry to complete the editing task.

To change the MIB name of the Mini FiberLinX-II as it appears on the network, type **sysname** and then press **Enter**. Enter a new name, not exceeding 16 characters in length.

Unit Control Settings

Serial/Telnet sessions display unit status as well as allowing configuration of some of the Mini FiberLinX-II features.

To access the Unit screen, type **unit** and then press **Enter**.



From this screen, view the settings for FlowControl, FiberAlert, LoopBack, Maximum Frame Size, and 802.1p Base Priority.

Note: This feature requires firmware version B2 or higher.

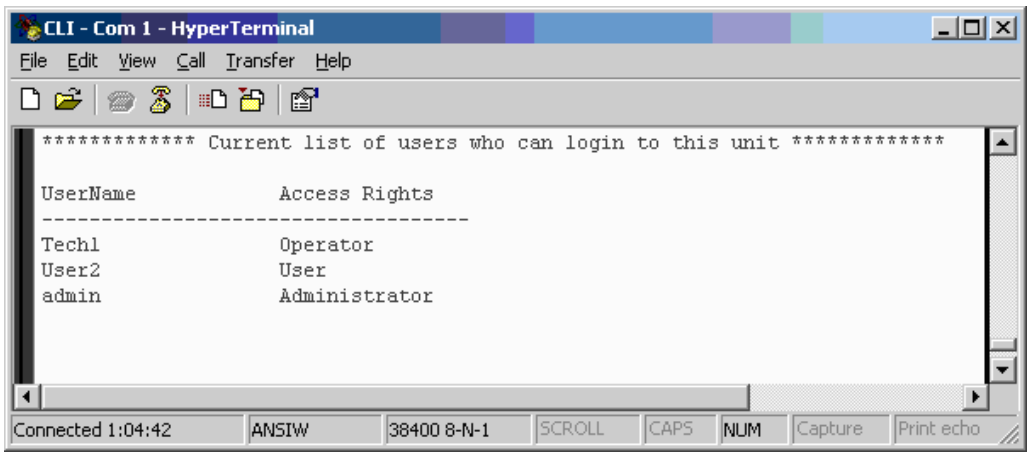
Use the **arrow keys** to navigate and the **Space Bar** to change the values on this screen.

The following table describes the settings available on this screen.

Setting	Description
Unit FlowControl	Enable/Disable FlowControl.
Unit FiberAlert	Enable/Disable FiberAlert.
Unit Loopback	Enable/Disable the various LoopBack testing modes.
Unit Max FrameSz	Set the maximum Frame Size to pass through the ports: 1518, 1522, 1536, or 1916.
802.1p Base Prj	Set the level of 802.1p base priority (3 or 4). The Mini FiberLinX-II has two outgoing queues: one for high priority traffic and one for low priority traffic. If the Base VLAN Priority is 4 for example, 0-3 are low priority and 4-7 are high priority. If the Base VLAN Priority is changed to 3, 0-2 are low priority and 3-7 are high priority.

Serial Configuration/Telnet Session

To manage access to the Mini FiberLinX-II, type **accounts** and then press **Enter** from the command screen. The following screen appears:



- To add a user, press **A**, and then enter the user information in the appropriate fields.
- To delete a user, press **D** for the user selected.
- To exit this screen, press any key other than A or D.

Note: User rights only allow viewing of status/settings but not changing of settings.

To log onto the unit through the serial port, connect a PC to the Mini FiberLinX-II using the included adapter. Set the computer or terminal for VT-100 emulation, and apply the following communication settings:

- 38.4K baud
- 8 data bits
- 1 stop bit
- No parity
- No FlowControl

Enter the User Name and Password as **admin** (the default setting) when connecting through Telnet/HyperTerminal. We recommend setting a new User Name and Password after signing on for the first time.

Assign the Mini FiberLinX-II an IP address before using a Telnet session (the default IP address is 10.10.10.10). All configurations performed using the serial port can also be performed using Telnet. Multiple accounts can be assigned with individual names and passwords.

Each account can be assigned one of the following authority roles:

Setting	Description
User	This role can only see status, change a password, and reboot.
Operator	This role can perform User role functions and change settings.
Administrator	This role can perform Operator role functions, add or delete accounts, and use the "cleandb" command. Account access through the serial port is at the Administrators level (default).

DHCP

Dynamic Host Control Protocol (DHCP) is disabled by default, but can be enabled to allow for the use of dynamic IP addresses.

DHCP Disable (Static IP Addressing)

DHCP is disabled in the default configuration. Initially, modules are assigned a static default IP address of 10.10.10.10. Changes to the static IP address can be added manually through iConfig, an RS-232 Serial session, or Telnet. The changes will be initiated following reboot of the module.

DHCP Enable (Dynamic IP Addressing)

If a DHCP server is present on the network and DHCP is enabled, the DHCP client will initiate a dialogue with the server during the boot-up sequence. The server will then issue an IP address to the management card. Once the new IP address is received, the SNMP Management Module will reboot so that the new IP address will take effect.

When there is no DHCP server on the network, use iConfig or serial configuration to set the IP addresses manually.

When DHCP is enabled, the IP address (default 10.10.10.10 or user configured) is saved. When DHCP is disabled, the saved IP address will be reinstated and the device will reboot.

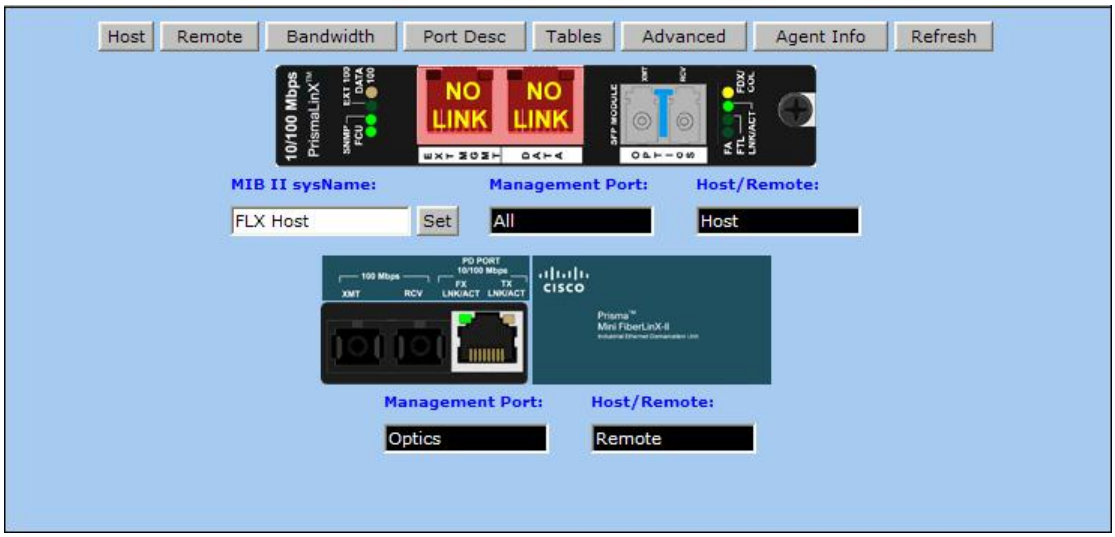
DHCP servers give out lease times, and devices renew their leases based on the administrator-specified time. If a device cannot renew its lease, and the lease expires, the device will be given the IP address 10.10.10.10, and will reboot.

Using PrismaView

PrismaView software provides network management in an easy-to-use GUI format.

After installing PrismaView on a network management PC using a Windows operating system, you can access PrismaView using the Windows Start menu.

Note: Windows SNMP services must be installed to receive traps.



The left side of the PrismaView screen displays the Prisma FiberLinX products on the network. To open the PrismaView screen for this module, click the connection for **Mini FiberLinX-II.**

The example above shows a connection to a FiberLinX, but this varies by configuration. When configuring the Mini FiberLinX-II as a standalone unit, only the Mini FiberLinX-II will appear.

A navigation bar on the top of the screen displays the options for configuring the Mini FiberLinX-II connection.

These options have the functions described below.

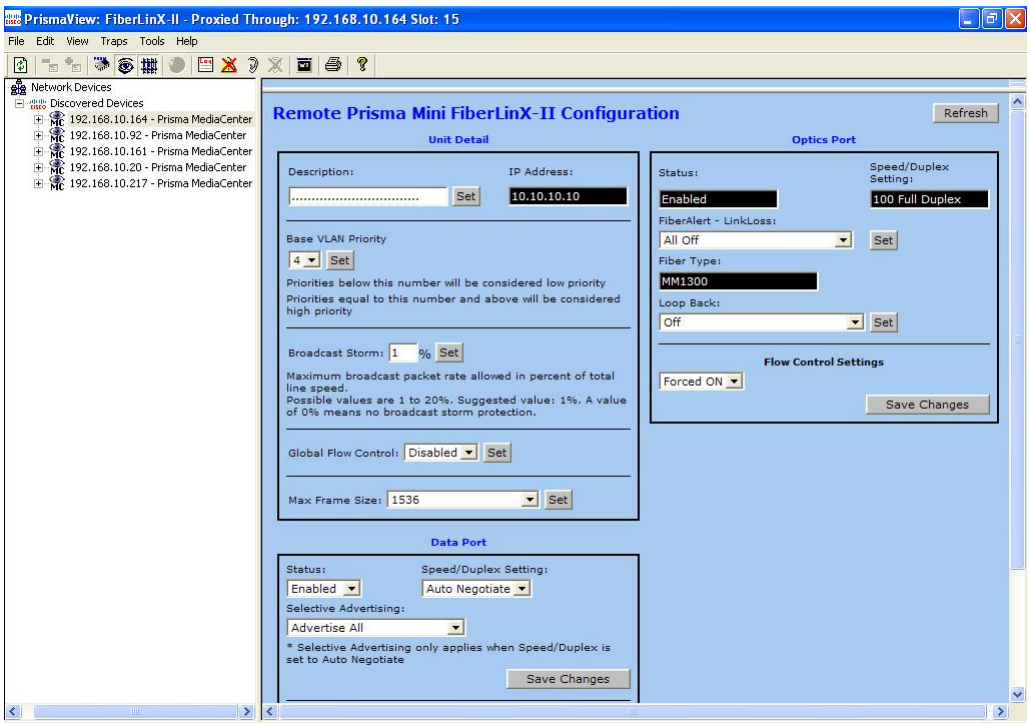
Option	Description
Host	Displays the configuration screen for the Host connection.
Remote	Displays the configuration screen for the Remote connection. This will show the Mini FiberLinX-II configuration information. Information on this screen is provided on the following page. **Note:** The Host and Remote buttons will not appear when configuring the Mini FiberLinX-II alone. In this setup, a Configuration button will appear with the same settings.

Option	Description
Bandwidth	Displays the Bandwidth Limitation Settings.
Port Desc	Displays a screen for setting port descriptions. Each name should not exceed 32 characters or include any spaces.
Tables	Displays a screen for viewing statistics tables regarding network performance.
Advanced	Displays the Mini FiberLinX-II advanced settings.
Agent Info	Information about the SNMP Management software is displayed here.
Refresh	To refresh the PrismaView settings on any screen, click this button.

The Configuration/Remote Screen

Depending on whether the Mini FiberLinX-II is being set up as a standalone or Host/Remote connection, the Configuration or Remote buttons will show a screen for configuring the Mini FiberLinX-II settings.

In addition to allowing setting changes on the Mini FiberLinX-II, settings on the ports can also be changed from the Configuration/Remote screen.



For information or instructions on the use of Unified Management Agent (UMA), refer to the *Prisma MediaCenter SNMP Management Module Installation Instructions*, part number 4027869.

Configuration File Save/Restore Function

The Configuration File Save/Restore function lets you back up all of the configuration settings of a unit. You can use this backup to restore settings to a unit if necessary or apply the same settings to a different unit.

Overview

All configurable managed objects are saved in a configuration file stored in the Large File Area of the module. This includes all configurable settings, such as VLAN configurations, IP Address configuration, and SNMP agent settings.

The configuration file can be transferred from the unit to a PC and saved to disk through the iConfig protocol. The configuration file can be transferred from a PC to a module of the same type through iConfig or TFTP into the Large File Area of the module. After the transfer is complete, the unit copies the configuration to flash and reboots.

The configuration file contents are specific to the device type, and can be identified by iConfig as a configuration file that is applicable to a specific type of device.

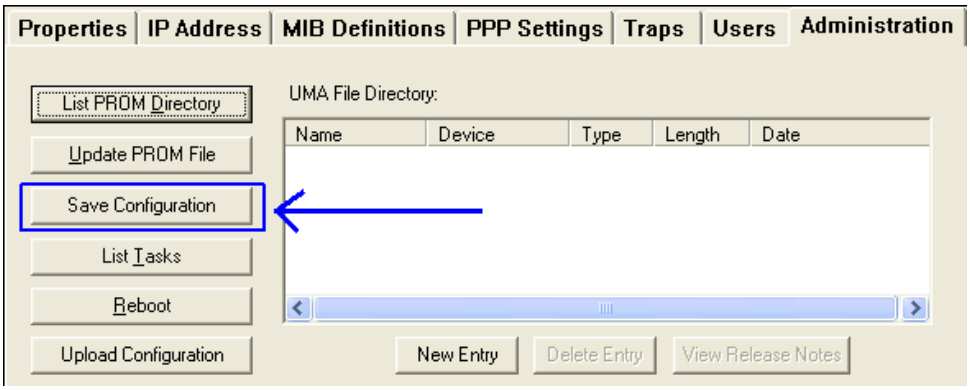
Requirements

The Configuration File Save/Restore function has two minimum requirements. FiberLinX-II family series products require Mini FiberLinX-II version B1 or higher, and PrismaView version: 1.8.4 or higher.

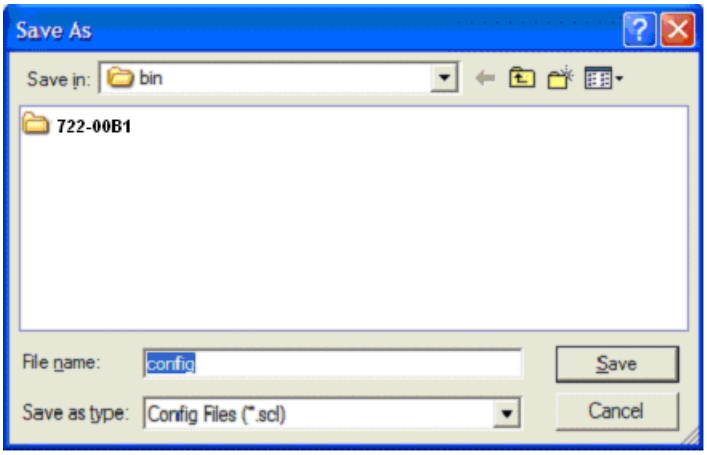
To Save a Configuration File

Complete the following steps to save a configuration file to disk.

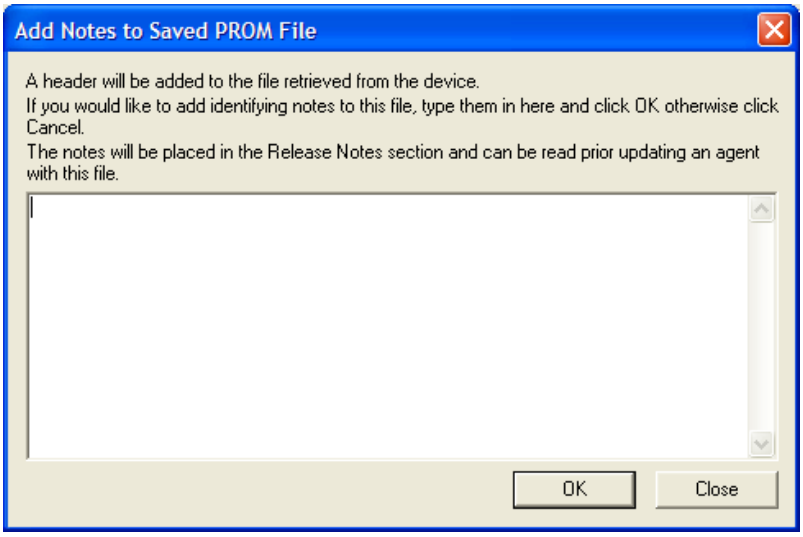
1. Log into the module through iConfig.
2. Navigate to the **iConfig Administration** tab.
3. From the iConfig Administration tab, click the **Save Configuration** button.



4 The Save As dialog window opens, prompting you for a file name.

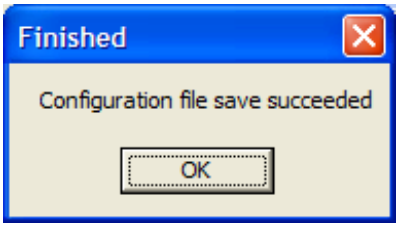


5 Type the file name, and then click **Save**. A new dialog prompts you for any notes to be added to the header of the saved file for future reference when uploading the file through iConfig.



6 Type any notes to be added to the header of the file, and then click **OK**.

After the file transfers from the module to disk, you are notified of the status.



Note: Once saved to disk, the file can be restored to the device or sent to another like device through iConfig or TFTP.

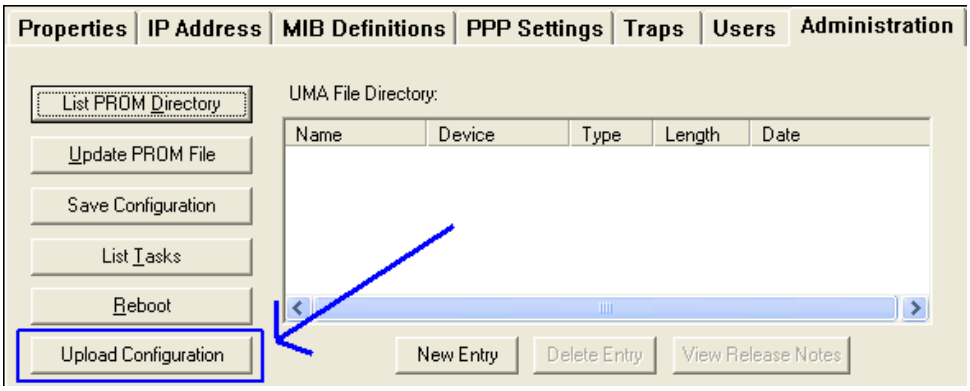
To Upload a Saved Configuration File Using iConfig

Complete the following steps to upload a saved configuration file using iConfig.

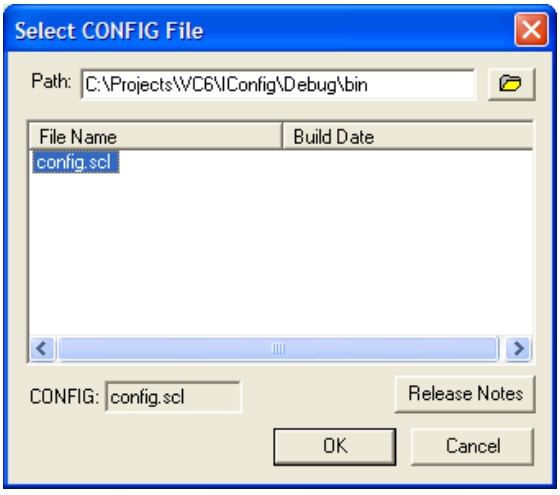
1 Log into the module through iConfig.

2 Select the **Administration** tab.

3 From the iConfig Administration tab, click **Upload Configuration**.



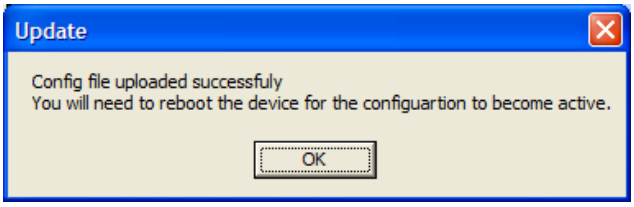
4 The Select Config File dialog window appears, prompting you to select a configuration file.



5 Select the appropriate configuration file, and then click **OK**. The file upload process begins.

Note: Once selected, you can view any notes that were added when the file was saved.

When the file upload process completes, you are notified of the status and reminded that a reboot is necessary for the new configuration to become active.

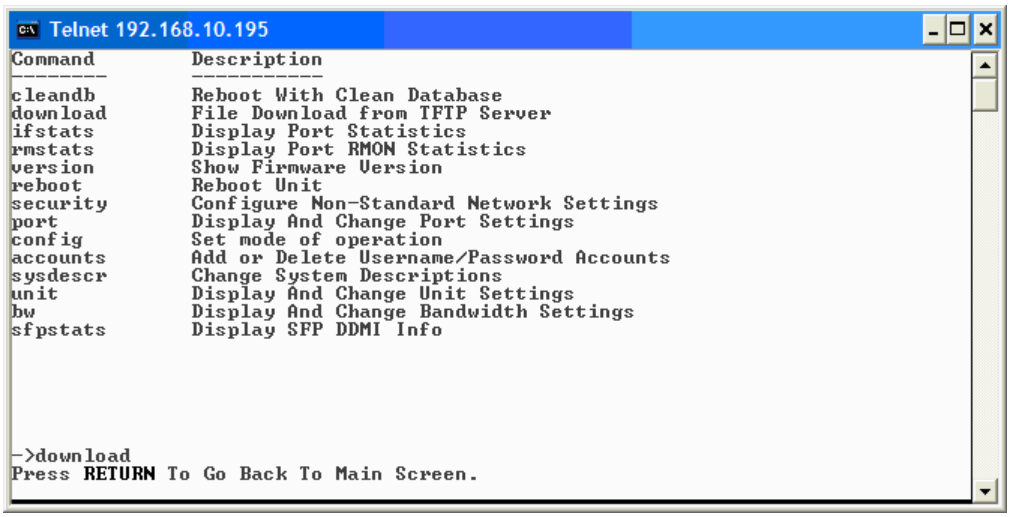


Note: By default, the new configuration file does not overwrite the current module IP address configuration.

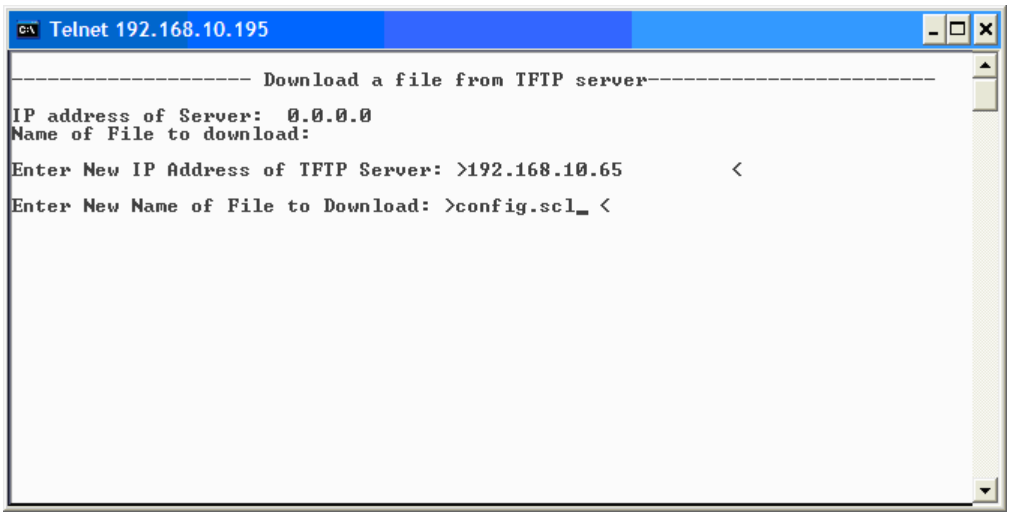
To Upload a Saved Configuration File Using TFTP

Complete the following steps to upload a saved configuration file using TFTP.

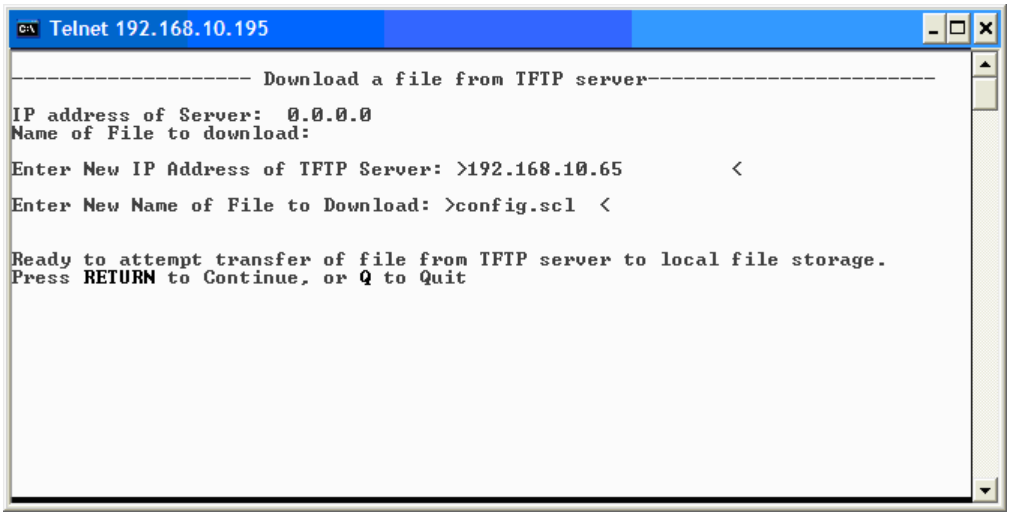
1 Log into the unit either through a serial port session or through Telnet. The CLI commands list appears.



2 Type **download** and then press **Enter** to run the Download command. The download command screen appears.

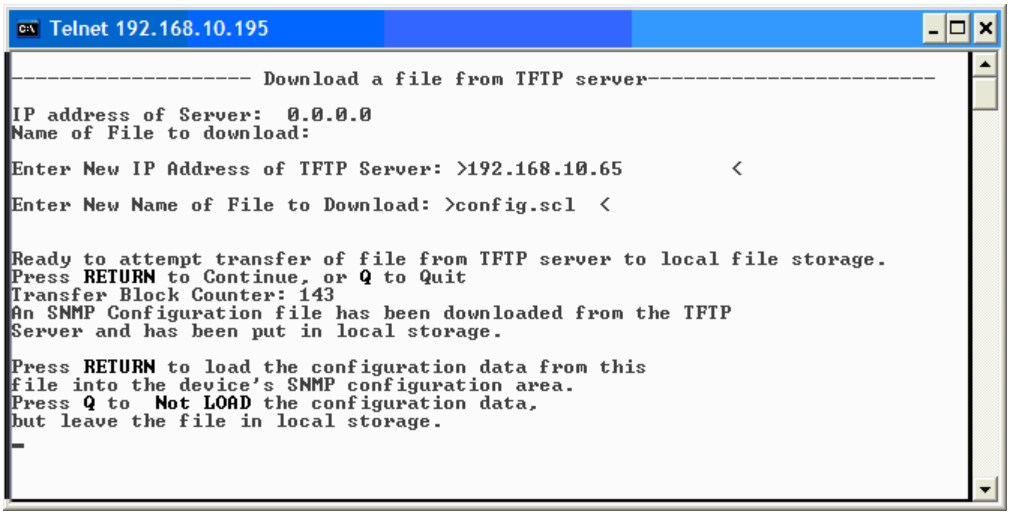


3 Type the IP address of the TFTP server and the name of the file to be retrieved, and then press **Enter**. A "ready" prompt appears.



4 Press **Enter** (or **Return**) to initiate the file transfer process (or press **Q** to cancel).

After the transfer process is complete, you are again prompted to press **Enter** (or **Return**) to load the configuration file.



5 Press **Enter** (or **Return**) to load the configuration file (or press **Q** to cancel).

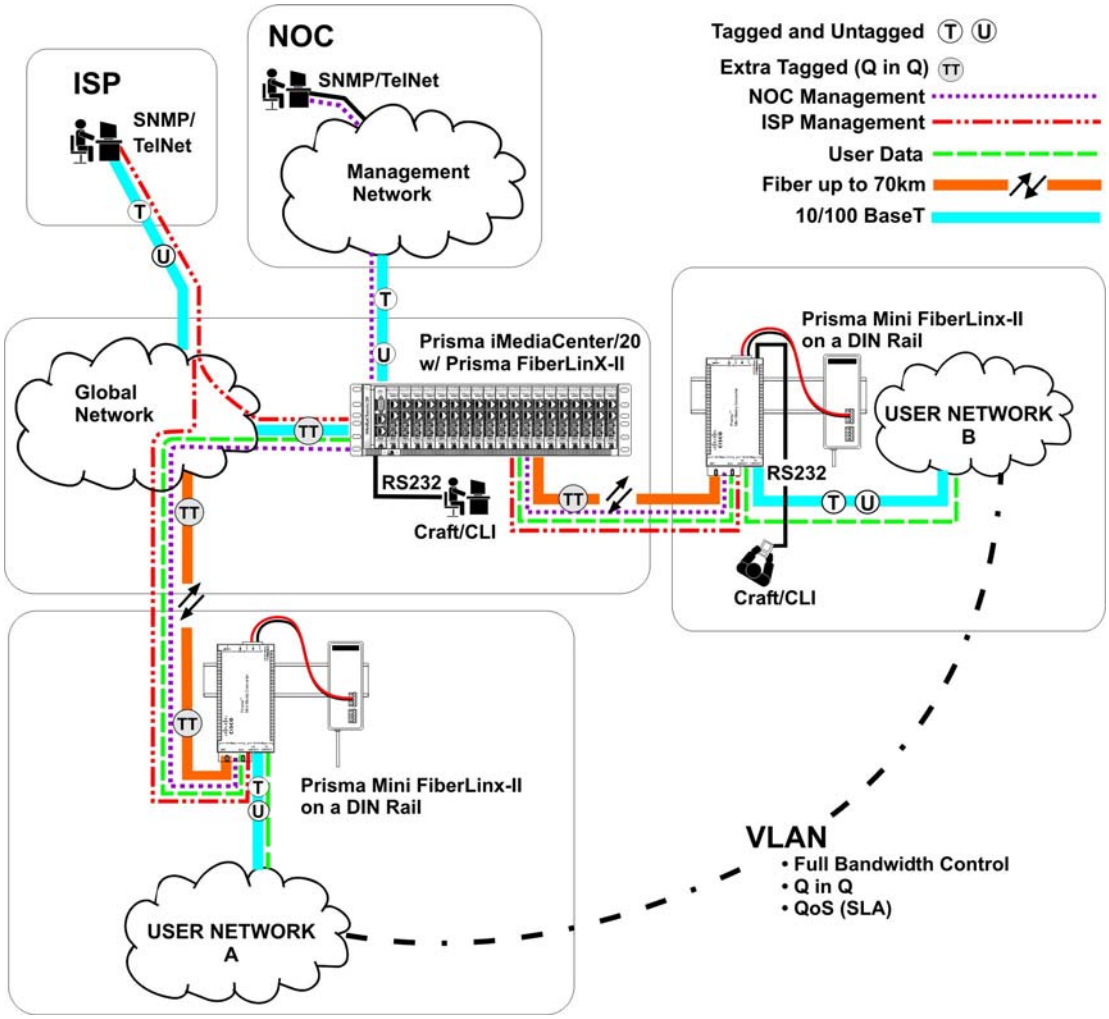
Once loaded into the module's SNMP memory area, you are prompted to reboot the module to make the new configuration active.

Note: By default, the new configuration file does not overwrite the current module IP address configuration.

Product Applications

The Mini FiberLinX-II comes with a variety of features for different network environments. When used with different types of IMC Products, some features can be enabled, such as extra tagging or "Q-in-Q," and different network setups come with different requirements.

The network setup example below shows one deployment scenario with a full range of management options.



The Mini FiberLinX-II module can be set up in one of two ways:

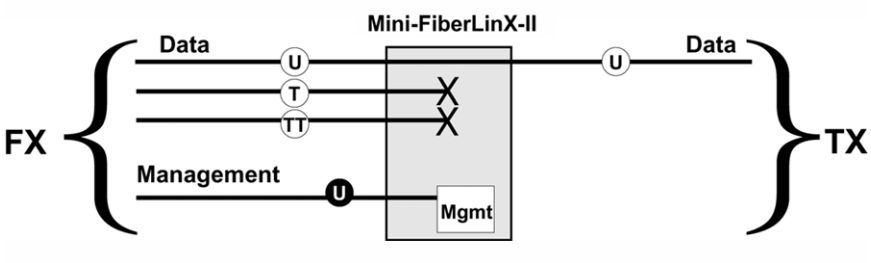
- One Mini FiberLinX-II and a FiberLinX-II for a Host/Remote application (one at each end)
- One Mini FiberLinX-II for a standalone application

Modes of Operation

The following are application examples of Operation Modes for the Mini FiberLinX-II. There are six modes of operation that can be configured through the Serial/Telnet session. All modes of operation block management traffic from the user network on the Data port.

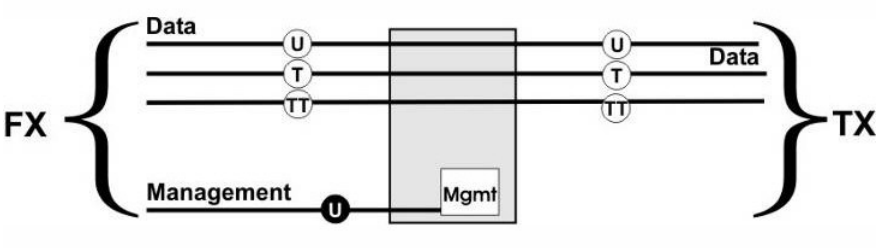
Mode One - Default

The default mode is provided to pass only untagged traffic.



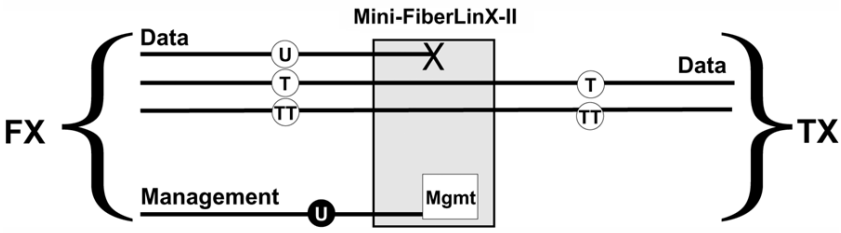
Default Plus

The Default Mode Plus allows tagged and untagged traffic to pass between the data and optics ports.



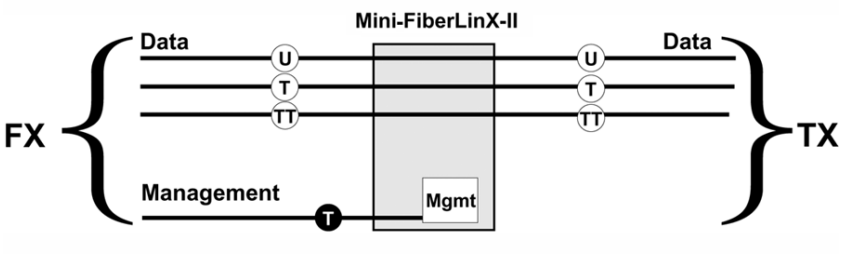
Mode Two - Transparency with Untagged Management

This mode is designed to pass all tagged and extra-tagged customer traffic unchanged and must be managed using untagged traffic only. It does not add or remove tags.



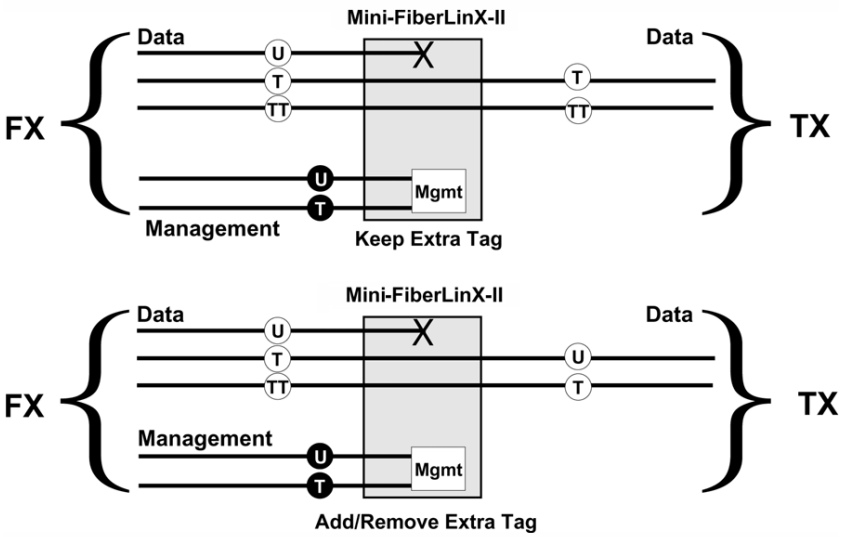
Mode Three - Transparency with Tagged Management

This mode will pass all tagged and untagged customer traffic. Management traffic must be tagged. It does not add or remove tags.



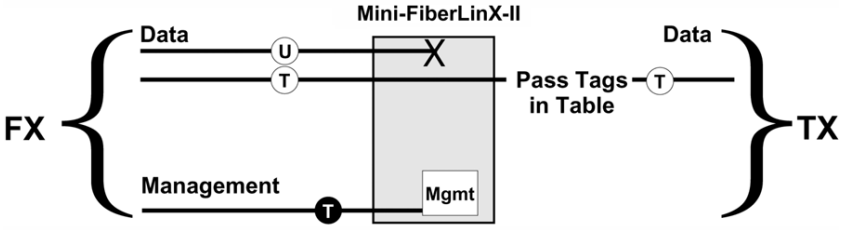
Mode Four - Transparency with Extra Tagging (or Q-in-Q)

This mode is designed to either pass all customer traffic with the defined extra tag (Q-in-Q) or add and remove the defined extra tag (Q-in-Q) on all customer traffic. Management traffic can be tagged or untagged.



Mode Five - VLAN Filter

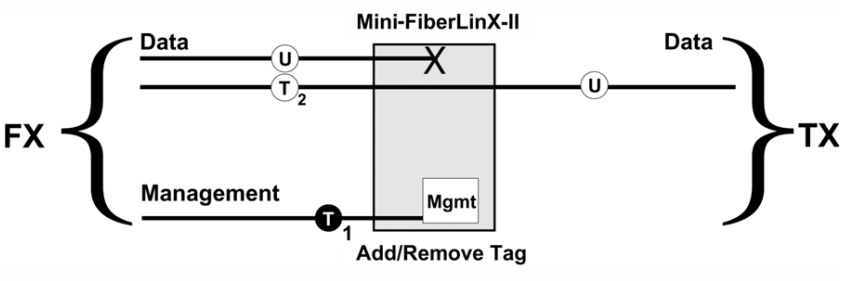
This mode is designed to only pass traffic with any of the 32 tags that have been identified in the user-defined table. No untagged traffic can pass and management traffic must be tagged. No tags are added or removed from the traffic.



Note: VLAN IDs can be any number between 1 and 4,094.

Mode Six - Port VLAN

This mode tags all customer traffic received by the copper port going to the fiber port, untagging traffic conversely. Management traffic must be tagged.



Troubleshooting

If a fiber connection cannot be established, perform the following steps to confirm that the fiber transceivers on the Mini FiberLinX-II are not over- or under-driving the fiber receivers:

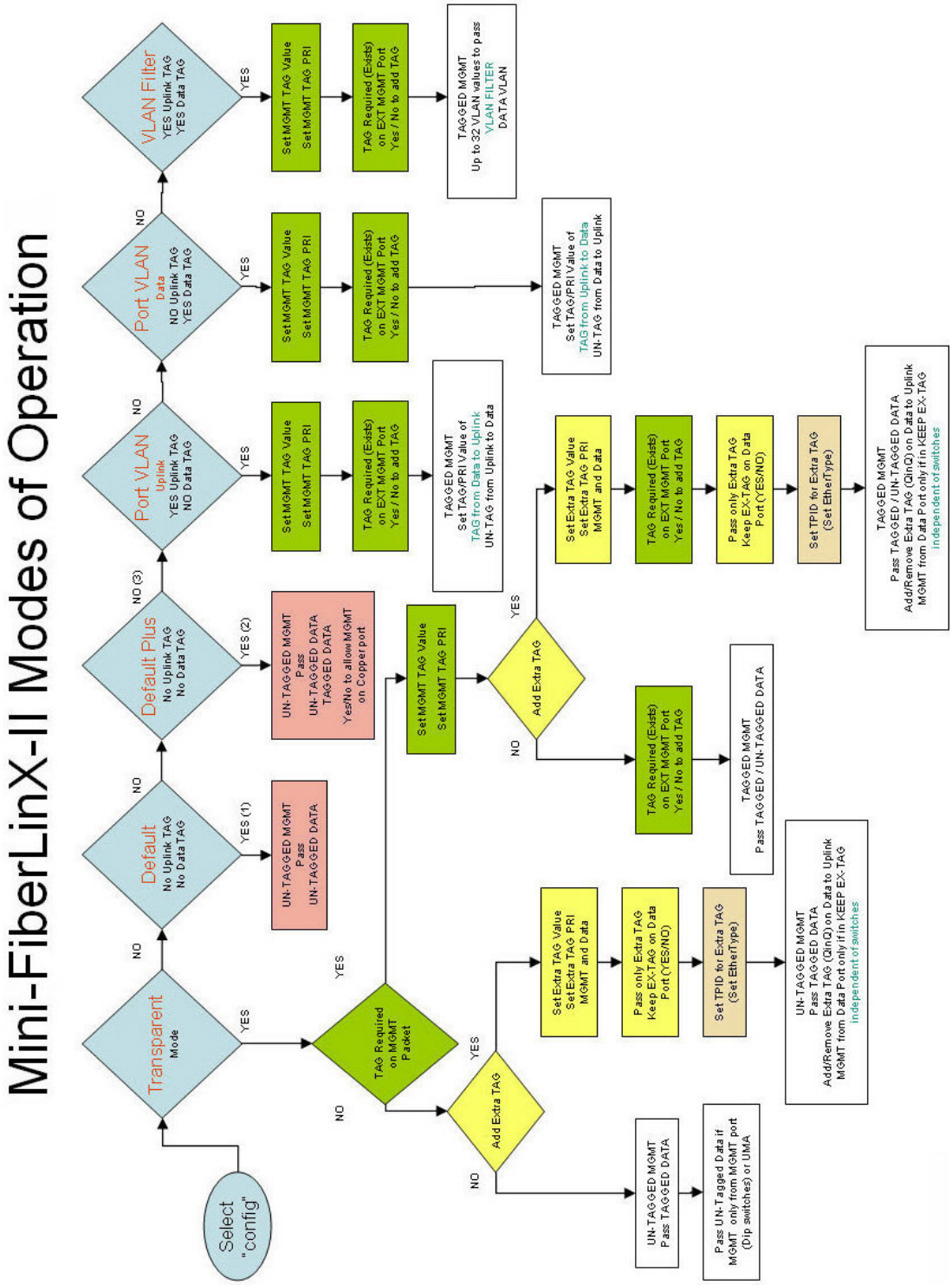
1. Make sure that the fiber wavelength on both connected devices match (i.e. both are 1310 nm single-mode fiber).
2. Make sure that FiberAlert is enabled on only one unit when connecting a Mini FiberLinX-II to another IMC Networks media converter with the FiberAlert feature.
3. Make sure that the twisted-pair port speed on the Mini FiberLinX-II matches that of the end devices connected to the Mini FiberLinX-II. Configure the Mini FiberLinX-II and its link partner to Auto-Negotiation or, if using Force mode, be sure that the speed and duplex match.
4. Management (VLAN tagged or Untagged) traffic will not be allowed to pass through the DATA port, and will only pass through the FIBER port.
5. When using the Mini FiberLinX-II as a powered device, establish power first, check the LEDs to confirm, and then connect the serial port to configure the device via a console session.

   Note: If you perform these steps in reverse order, the unit will appear non-functional. The same is true if connecting a DC terminal block.

To Restore Factory Defaults

To restore the unit to factory default settings, use the cleandb function from the serial port management feature.

Mini FiberLinX-II Modes of Operation



Fiber-Optic Cleaning Guidelines

CAUTION:

Proper operation of this equipment requires clean optical fibers. Dirty fibers will adversely affect performance. Proper cleaning is imperative.

The proper procedure for cleaning optical connectors depends on the connector type. The following describes general instructions for fiber-optic cleaning. Use your company's established procedures, if any, but also consider the following.

Cleaning fiber-optic connectors can help prevent interconnect problems and aid system performance. When optical connectors are disconnected or reconnected, the fiber surface can become dirty or scratched, reducing system performance.

Inspect connectors prior to mating, clean as needed, and then remove all residue. Inspect connectors after cleaning to confirm that they are clean and undamaged.

Recommended Equipment

- CLETOP or OPTIPOP ferrule cleaner (CLETOP Type A for SC, Type B for LC)
- Compressed air (also called “canned air”)
- Lint-free wipes moistened with optical-grade (99%) isopropyl alcohol
- Bulkhead swabs for LC or SC type connectors (choose appropriate type)
- Optical connector scope

Tips for Optimal Fiber-Optic Connector Performance

- Do not connect or disconnect optical connectors with optical power present.
- Always use compressed air before cleaning the fiber-optic connectors and when cleaning connector end caps.
- Always install or leave end caps on connectors when they are not in use.
- If you have any degraded signal problems, clean the fiber-optic connector.
- Advance a clean portion of the ferrule cleaner reel for each cleaning.
- Turn off optical power before making or breaking optical connections to avoid microscopic damage to fiber mating surfaces.

To Clean Optical Connectors

Warning:

- **Avoid personal injury! Use of controls, adjustments, or procedures other than those specified herein may result in hazardous radiation exposure.**
- **Avoid personal injury! The laser light source on this equipment (if a transmitter) or the fiber cables connected to this equipment emit invisible laser radiation.**
- **Avoid personal injury! Viewing the laser output (if a transmitter) or fiber cable with optical instruments (such as eye loupes, magnifiers, or microscopes) may pose an eye hazard.**

- Do not apply power to this equipment if the fiber is unmated or unterminated.
- Do not stare into an unmated fiber or at any mirror-like surface that could reflect light emitted from an unterminated fiber.
- Use safety-approved optical fiber cable to maintain compliance with applicable laser safety requirements.

Important: Ensure that no optical power is present prior to this procedure.

1. Turn optical power off to the connector.
2. Using an optical connector scope, inspect the connector for scratches, burns, or other signs of damage.

   Note: If the connector is damaged, replace the jumper.
3. If the connector requires cleaning, swipe it across the face of the appropriate ferrule cleaner several times. This will remove dust and some films.

   Note: You may hear a slight "squeak" while cleaning the connector, indicating that it is clean.
4. Inspect the connector again. If the connector requires further cleaning, clean it using 99% isopropyl alcohol and a lint-free wipe.
5. Swipe the connector across the face of the appropriate ferrule cleaner several more times to remove any film left by the alcohol.
6. Repeat all the steps above as needed until the connector is clean.

For Information

Support Telephone Numbers

This table lists the Technical Support and Customer Service numbers for your area.

Region	Centers	Telephone and Fax Numbers
North America	Cisco Services Atlanta, Georgia United States	For *Technical Support*, call: ▪ Toll-free: 1-800-722-2009 ▪ Local: 678-277-1120 (Press **2** at the prompt) For *Customer Service* or to request an RMA number, call: ▪ Toll-free: 1-800-722-2009 ▪ Local: 678-277-1120 (Press **3** at the prompt) ▪ Fax: 770-236-5477 ▪ E-mail: customer.service@sciatl.com
Europe, Middle East, Africa	Belgium	For *Technical Support*, call: ▪ Telephone: 32-56-445-197 or 32-56-445-155 ▪ Fax: 32-56-445-061 For *Customer Service* or to request an RMA number, call: ▪ Telephone: 32-56-445-444 ▪ Fax: 32-56-445-051 ▪ E-mail: elc.service@sciatl.com
Japan	Japan	▪ Telephone: 81-3-5908-2153 or +81-3-5908-2154 ▪ Fax: 81-3-5908-2155 ▪ E-mail: yuri.oguchi@sciatl.com
Korea	Korea	▪ Telephone: 82-2-3429-8800 ▪ Fax: 82-2-3452-9748 ▪ E-mail: kelly.song@sciatl.com
China (mainland)	China	▪ Telephone: 86-21-2401-4433 ▪ Fax: 86-21-2401-4455 ▪ E-mail: xiangyang.shan@sciatl.com
All other Asia-Pacific countries & Australia	Hong Kong	▪ Telephone: 852-2588-4746 ▪ Fax: 852-2588-3139 ▪ E-mail: support.apr@sciatl.com
Brazil	Brazil	For *Technical Support*, call: ▪ Telephone: 55-11-3845-9154 ext 230 ▪ Fax: 55-11-3845-2514 For *Customer Service* or to request an RMA number, call: ▪ Telephone: 55-11-3845-9154, ext 109 ▪ Fax: 55-11-3845-2514 ▪ E-mail: luiz.fattinger@sciatl.com

Region	Centers	Telephone and Fax Numbers
Mexico, Central America, Caribbean	Mexico	For *Technical Support*, call: ■ Telephone: 52-3515152599 ■ Fax: 52-3515152599 For *Customer Service* or to request an RMA number, call: ■ Telephone: 52-55-50-81-8425 ■ Fax: 52-55-52-61-0893 ■ E-mail: karla.lugo@sciatl.com
All other Latin America countries	Argentina	For *Technical Support*, call: ■ Telephone: 54-23-20-403340 ext 109 ■ Fax: 54-23-20-403340 ext 103 For *Customer Service* or to request an RMA number, call: ■ Telephone: 770-236-5662 ■ Fax: 770-236-5888 ■ E-mail: veda.keillor@sciatl.com

5030 Sugarloaf Parkway, Box 465447 678.277.1000
Lawrenceville, GA 30042

Printed in United States of America
March 2009 Part Number 4030542 Rev B